ISSN:0975-9646

Venugopal Gaddam et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2403-2407

Protection for Cloud Computing Using Level-Based Cryptography

Venugopal Gaddam[1], Srinivasulu Singaraju[2], M.Sundar babu[3], S.Sai Kumar[4]

[1,3,4]*Assistant Professor, Department of IT, PVP Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh*

[2]*Assistant Professor, Department of CSE, PACE Institute of Engineering and Technology, Ongole, Andhra Pradesh*

***Abstract*—Cloud computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Today most cloud computing system use asymmetric and traditional public key cryptography to provide data security and mutual authentication. Cloud computing providers have setup several data canters at different geographical locations over the internet in order to optimally serve needs of their customers around the world. Level-based cryptography has some attraction characteristics that seem to fit well the requirements of cloud computing. More companies begin to provide different kinds of cloud computing services for internet users at the same time these services also bring some security problems. Currently the majority of cloud computing systems provide digital identity for users to access their services. In this paper, by adopting federated identity management together with level-based cryptography, not only the key distribution but also the mutual authentication can be simplified in the cloud.**

***Keywords*— cloud computing, identity-based cryptography, authentication, level-based cryptography.**

I. INTRODUCTION

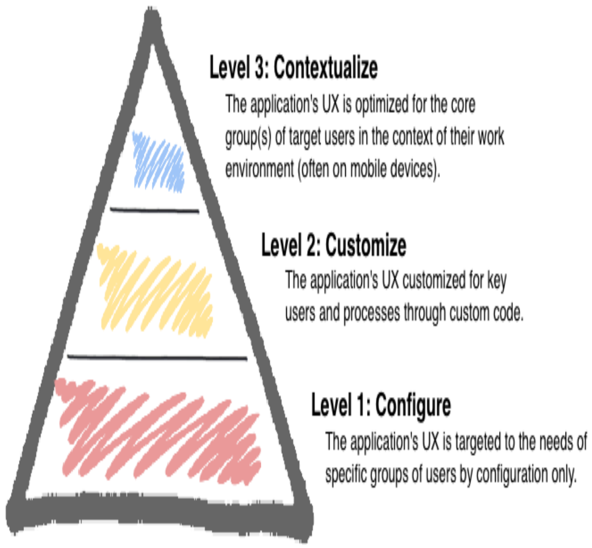
Each level represents a position in the hierarchy .For example; a time dimension might have a hierarchy that represents data at the month, quarter, and year levels. Each level above the base (or most detailed) level contain aggregate values for the levels below it. The members at different levels have a one-to-many parent-child relation .

Hierarchies and levels have a many-to-many relationship. A hierarchy typically contains several levels, and a single level can be included in more than one hierarchy. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs. It's called cloud computing, and it could change the entire computer industry. In a cloud computing system local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing systems interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.

II. IDENTITY-BASED HIERARCHICAL MODEL FOR CLOUD COMPUTING:

The new level-based static and dynamic hierarchies. Both dynamic hierarchies and static hierarchies can be level-based hierarchies. In a level-based hierarchy, you organize members into named levels. Each level is a list. You can use one or more lists for the hierarchy. In the cloud computing, it is frequent for the entities to communicate mutually. To achieve the security in the communication, it is important to propose an encryption and signature schemes.

Level-based cryptography is a public key technology that allows the use of a public identifier of a user as the user's public key. Hierarchy level-based cryptography is the development from it in order to solve the scalability problem. Recently identity-based cryptography and hierarchy identity-based cryptography have been proposed to provide security for some Internet applications.



Lower-level setup

1. Assume there are m nodes in the level-1. For each node, the root PKG acts as follows (let X be an arbitrary node in the m nodes):
2. Compute the public key of node.

3. Pick the secret point *X q ρ ∈Z for node X .X ρ is only known by node X and its parent node;
4. Set the secret key of node.
5. Define the Q-value is public.

After the above five steps are finished, all nodes in the level-1 get and securely keep their secret keys and the secret points. On the other hand, the public key and the Q-value are publicized.

III. Security in Cloud Computing

Cloud computing have many advantages in cost reduction, resource sharing, and timesaving for new service deployment. While in a cloud computing system, most data and software that users use reside on the Internet, which bring some new challenges for the system, especially security and privacy. Since each application may user source from multiple servers. The servers are potentially based at multiple locations and the services provided by the cloud may use different infrastructures across organizations. All these characteristics of cloud computing make it complicated to Provide security in cloud computing.

To ensure adequate security in cloud computing, various security issues, such as authentication, data confidentiality and integrity, and non-repudiation, all need to be taken into account. Currently, WS-Security service is wildly used in the cloud to provide security for the system. In WS-Security, XML encryption and XML signature are used to provide data confidentiality and integrity. Mutual authentication can be supported by adding X.509certificate and Kerberos stickers into SOAP message header. As mentioned earlier, there are three types of clouds in general: private cloud, public cloud and hybrid cloud. In a public cloud, resources are dynamically provisioned on a fine-grained, self-service basis over the Internet. Services in the cloud are provided by an off-site third-party provider who shares resources and bill son a fine-grained utility computing basis. While in most private clouds, with limited computing resources, it is difficult for a private cloud to provide all services for the risers, as some services may more resources than internal cloud can provide. Hybrid cloud is a potential solution for this issue since they can get the computing resources from external cloud computing providers.

Private clouds have their advantages incorporation governance and offer reliable services, as well as they allow more control than public clouds do. For the security concerns, when a cloud environment is created inside a firewall, it can provide its users with less exposure to Internet security risks. Also in the private cloud, all the services can be accessed through internal connection rather than public Internet connections, which make it easier to use existing security measures and standards. This can make private clouds more appropriate for services with sensitive data that must be protected. While in a hybrid cloud, it includes more than one domain, which will increase the difficulty of security provision, especially key management and mutual authentication.

The domains in a hybrid cloud can be heterogeneous networks, hence there may be gaps between these networks and between the different services providers. Even security can be well guaranteed in each of private/public cloud, while in a hybrid cloud with more than one kind of clouds that have different kinds of network conditions and different security Policies, how to provide efficient security protection is much more difficult. For example, cross domain authentication can be a problem in a hybrid cloud with different domains.

In a cloud, the cloud computing system needs to provide a strong and user-friendly way for users to access all kinds of services in the system. When a user wants to run an application in the cloud, the user is required to provide a digital identity. Normally, this identity is a set of bytes that related to the user. Based on the digital identity, a cloud system can know what right this user has and what the user is allowed to do in the system. Most of cloud platforms include an identity service since identity information is required for most distributed applications these cloud computing systems will provide a digital identity for every user.

IV. Level-Based Cryptography and Signature

The level-based hierarchy include root setup, lower-level setup, extraction, encryption, and decryption.

1. **Root setup:** root PKG will generate the root PKG system parameters and a root secret. The root secret will be used for private key generation for the lower-level PKGs. The root system parameters are made publicly available and will be used to generate public keys for lower-level PKGs and users.
2. **Lower-level setup:** Each lower-level PKG will get the root system parameters and generate its own lower-level secret. This lower-level secret will be used to generate private keys for the users in its domain.
3. **Extract:** When a user or PKG at level t with its identity ($ID_1 \ldots\ldots ID_t$) requests his private key from its upper-level PKG, where ($ID_1 \ldots\ldots ID_i$) is the identity of its ancestor at level i ($1 \leq i \leq t$), the upper-level PKG will use this identity, system parameters and its own private key to generate a private key for this user.

4. **Encryption:** User who wants to encrypt a message M can use the system parameters, receiver's identity and the message as input to generate the cipher text.

C = Encryption (parameters, receiver ID, M).

5. **Decryption:** Receiving a cipher text, receiver can use system parameters and his private key got from the PKG to decrypt the cipher text.

M = Decryption (parameters, k, C), k is the private key of the receiver

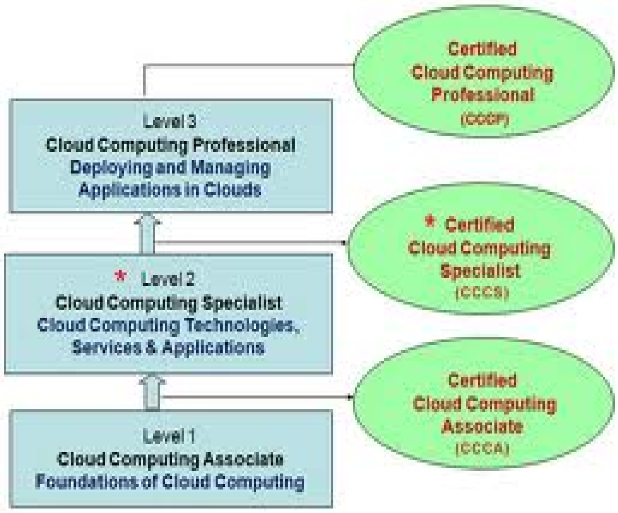
6. **Signing and verification:** A user can use parameters, its private key, and message M to generate a digital signature and sends to the receiver. Receiver and verify the signature using the parameters, message M, and the sender's ID.

Signature = Signing (parameters, k, M), k is the sender's private key.

Verification = (parameters, sender ID, M,Signature).

V. Level Management in the Cloud

Compared with centralized identity, which is used to deal with security problems within the same networks, federated identity is adopted to deal with the security problems that a user may want to access external networks or an external user may want to access internal networks. Federated identity is a standard-based mechanism for different organization to share identity between them and it can enable the portability of identity information to across different networks. One common use of federated identity is secure Internet single sign-on, where a user who logs in successfully at one organization can access all partner networks without having to log in again. Using identity federation can increase the security of network since it only requires a user to identify and authenticate him to the system for one time and this identity information can be used in different networks.



VI. Date Encryption and Digital Signature

In the cloud, one of the most important security problems are mutual authentication between users and servers, protection of data confidentiality and integrity during data transmission by encryption using secret keys. In a cloud using federated identity, any user and server has its unique identity and any user and server can get the identity of any other user/server by request with the PKGs. With HIBC, the public key distribution can be greatly simplified in the cloud. Users and servers do not need to ask a public key directory to get the public key of other users and servers as in traditional public key schemes. If any user or server wants to encrypt the data that transmitted in the cloud, the sender can acquire the identity of the receiver, then the sender can encrypt the data with receiver's identity.

VII. Functional levels of Cloud Computing

Conceptually, users acquire computing platforms or IT infrastructures from computing Clouds and then run their applications inside. Therefore, computing Clouds render users with services to access hardware, software and data resources, thereafter an integrated computing platform as a service, in a transparent way:

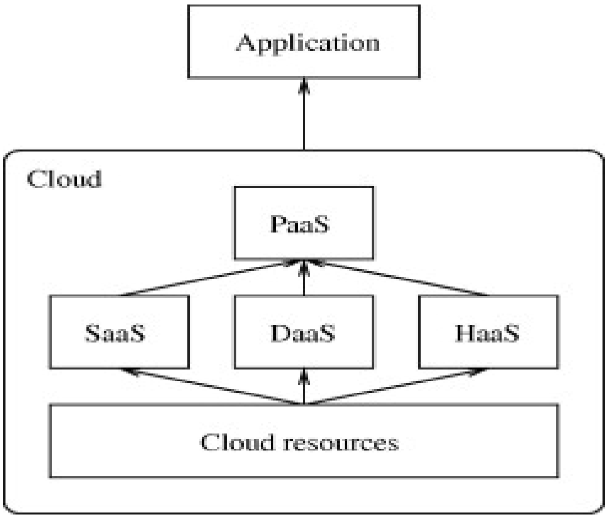
Hardware as a Service (HaaS): Hardware as a Service was coined possibly in 2006. As the result of rapid advances in hardware virtualization, IT automation and usage metering & pricing, users could buy IT hardware, or even an entire data canter, as a pay-as-you-go subscription service. The HaaS is flexible, scalable and manageable to meet your needs

Software as a Service (SaaS): Software or an application is hosted as a service and provided to customers across the Internet. This mode eliminates the need to install and run the application on the customer's local computers. SaaS therefore alleviates the customer's burden of software maintenance, and reduces the expense of software purchases by on-demand pricing.

Data as a Service (DaaS): Data in various formats and from multiple sources could be accessed via services by users on the network. Users could, for example, manipulate
the remote data just like operate on a local disk or access the data in a semantic way in the Internet. Amazon Simple Storage Service provides a simple Web services interface that can be used to store and retrieve, declared by Amazon, any amount of data, at any time, from anywhere on the Web. The DaaS could also be found at some popular IT services

Based on the support of the HaaS, SaaS and DaaS, the Cloud computing in addition can deliver the Infrastructure as a Service (IaaS) for users. Users thus can on-demand subscribe to their favorite computing infrastructures with requirements of hardware configuration, software installation and data access demands.

The below diagram shows relationship between the services



The Web Service Management layer(WSLA) also provides the security for cloud computing based on Level-based hierarchy. We describe three common WSLA services and some of their adaptations required in the cloud context.

1**. Measurement Services:** These services are responsible for measuring the runtime parameters of cloud providers resources. As discussed previously, service parameters like response time, throughput are constantly changed due to variability in service request from consumer side. In the context of the cloud however the usage and cost parameters are also dynamic. This is due to the pay-as-you-go nature and the elasticity of the cloud. Hence we identify 1) usage and 2) cost / price data as two major additional services that should be added to the set of measurement services in the context of clouds.

2. Condition Evaluation Service: This service is responsible of getting the results from measurement services and evaluating the Service Level Objectives. If there are violations the Management service will be contacted. We believe that due to the dynamic nature of the cloud, the condition evaluation needs to be performed more frequently than in a traditional service framework. Traditionally there is little attention on the complexity of conditions. In the cloud context, we propose that conditions be simpler for faster evaluation cycles. We add a dynamic scheduler that depends on a metric like the transaction rate. This ensures that when the load is high, the enforcement check runs more frequently since its most likely the violations happen during such transitions.

3. **Management Service:** This service is responsible for taking corrective actions on violation of the Service Level Objectives. We anticipate that since the cloud represents utility type computing resources, the management service would be primarily handling financial penalties similar to the real world utility industry practices.

VIII. CLOUD COMPUTING CHARACTERISTICS

Cloud computing provides several salient features that are different from traditional service computing, which we summarize below:

***Multi-tenancy*:** In a cloud environment, services owned by multiple providers are co-located in a single data canter. The performance and management issues of these services are shared among service providers and the infrastructure Provider. The layered architecture of cloud computing provides a natural division of responsibilities. The owner of each layer only needs to focus on the specific objectives associated with this layer. However, multi-tenancy also introduces difficulties in understanding and managing the interactions among various stakeholders.

***Shared resource pooling*:** The infrastructure provider offers a pool of computing resources that can be dynamically assigned to multiple resource consumers. Such dynamic resource assignment capability provides much flexibility to infrastructure providers for managing their own resource usage and operating costs. For instance, an IaaS provider can leverage VM migration technology to attain a high degree of server consolidation, hence maximizing resource utilization while minimizing cost such as power consumption and cooling.

***Geo-distribution and ubiquitous network access*:** Clouds are generally accessible through the Internet and use the Internet as a service delivery network. Hence any device with Internet connectivity, be it a mobile phone, a PDA or a laptop, is able to access cloud services. Additionally, to achieve high network performance and localization, many of today's clouds consist of data canters located at many locations around the globe. A service provider can easily leverage geo-diversity to achieve maximum service utility.

***Service oriented*:** As mentioned previously, cloud computing adopts a service-driven operating model. Hence it places a strong emphasis on service management. In a cloud, each IaaS, PaaS and SaaS provider offers its service according to the Service Level Agreement (SLA) negotiated with its customers. SLA assurance is therefore a critical objective of every provider.

***Dynamic resource provisioning*:** One of the key features of cloud computing is that computing resources can be obtained and released on the fly. Compared to the traditional model that provisions resources according to peak demand, dynamic resource provisioning allows service providers to acquire resources based on the current demand, which can considerably lower the operating cost.

***Self-organizing*:** Since resources can be allocated or deallocated on-demand, service providers are empowered to manage their resource consumption according to their own needs. Furthermore, the automated resource management feature yields high agility that enables service providers to respond quickly to rapid changes in service demand such as the flash crowd effect.

***Utility-based pricing*:** Cloud computing employs a pay per-use pricing model. The exact pricing scheme may vary from service to service. For example, a SaaS provider may rent a virtual machine from an IaaS provider on a per-hour basis. On the other hand, a SaaS provider that provides on-demand customer relationship management (CRM) may charge its customers based on the number of clients it serves (e.g., Sales force). Utility-based pricing lowers service operating cost as it charges customers on a per-use basis. However, it also introduces complexities in controlling the operating cost. In this perspective, companies like VKernel provide software to help cloud customers understand, analyze and cut down the unnecessary cost on resource consumption.

IX. TESTING FOR LEVEL-BASED COMPUTING

Conformance and interoperability testing involves checking that implementations follow their specifications and that they provide the intended functionality. In the following we use the term standard instead of specification, because we consider such a specification to be standardized and published by an organization like OGF, W3C or ETSI. In this section, we describe the details of conformance and interoperability testing, discuss related work on grid testing and describe the ETSI process for conformance and interoperability test development. Finally, we present an example that shows how the ETSI process can be used to define interoperability tests for grid systems. The example is based on the OGF OGSA-BES standard.

X. How to Assess

To prove the security and continuity risks associated with a cloud offering:

• How qualified are the policymakers, architects, coders and operators to understand and reduce the risks of their offering?

• What risk control processes and technical mechanisms are used?

• What level of testing has been done to verify that the service and control processes are functioning as designed and to identify unanticipated vulnerabilities?

In practice, there are only three ways to answer these questions and provide a risk assessment of a service:

1. Accept whatever assurances the service provider offers.
2. Evaluate the service provider in person.
3. Use a neutral third party to perform a security assessment.

The first method is obviously not the most rigorous or defensible, but it is the one most often used, and often for good reason. Many organizations have no ability in-house to adequately assess the security of a sophisticated offering, so they seek out suppliers that have more security and continuity expertise than they do. Unfortunately, many of today's cloud-computing products only come with the vaguest information about risk controls. Do not accept unsubstantiated claims, such as "we follow best practices," or vague assurances, such as "our employees are not reading your mail." Ask for specific evidence that answers questions on qualifications, controls and testing. Ultimately, you cannot expect any commercial organization to be totally objective about its weaknesses. To be fully transparent, a provider needs to be willing to undergo external reviews.

XI. CONCLUSION

Authentication is necessary in Cloud Computing. SSL Authentication Protocol is of low efficiency for Cloud services and users. In this paper, we presented an level based authentication for cloud computing, based on the level-based hierarchical model for cloud computing and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight than SAP, especially the more lightweight user side. This aligned well with the idea of cloud computing to allow the users with an average or low-end platform to outsource their computational tasks to more powerful servers.

REFERENCES

[1] Erdogmus, H.: Cloud Computing: Does Nirvana Hide behind the Nebula? IEEE Software 26(2), 4–6 (2009)

[2] Leavitt, N.: Is Cloud Computing Really Ready for Prime Time? Computer 42(1), 15–20 (2009) 166 H. Li et al.

[3] Freier, A.O., Karlton, P., Kocher, P.C.: The SSL Protocol, Version 3.0.INTERNET- DRAFT (November 1996), http://draft-freier-ssl-version3-02.txt

[4] Foster, I., Kesslman, C., Tsudik, G.: A Security Architecture for Computational Grids. In: ACM Conference on Computers and Security, pp. 83–90 (1998)

[5] Dai, Y.S., Pan, Y., Zou, X.K.: A hierarchical modelling and analysis for grid service reliability. IEEE Transactions on Computers 56(5), 681–691 (2007)

[6] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley (Feb 2009)

[7] Keller, A., Ludwig, H.: The wsla framework: Specifying and monitoring service level agreements for web services. J. Netw. Syst. Manage. 11(1) (2003) 57–81

[8] Ludwig, H., Keller, A., Dan, A., King, R., Franck, R.: Web service level agreement (WSLA) language specification. IBM Corporation (2003)

[9] Amazon: Service level agreement for ec2 [http://aws.amazon.com/ec2-sla/] (2008)

[10] He, C., Gu, L., Du, B., Li, Z.: A WSLA-based monitoring system for grid service-GSMon. In: 2004 IEEE International Conference on Services Computing, 2004.(SCC 2004). Proceedings. (2004) 596–599