

Application Level Security in Cloud Computing

Ankur Pandey, Kirtee Shevade, Roopali Soni
 Thakral College of Technology
 Bhopal, India.

ABSTRACT: Cloud Computing represents a new computing model that poses many demanding security issues at all levels, e.g., network, host, application, and data levels. The variety of the delivery models presents different security challenges depending on the model and consumers' Quality of Service(QoS) requirements. Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Infrastructure as a Service (IaaS) serves as the foundation layer for the other delivery models, and a lack of security in this layer affects the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. Information Technology (IT) Security Risk Management is a critical task for the organization to protect against the loss of confidentiality, integrity, and availability of IT resources and data. Due to system complexity and sophistication of attacks, it is increasingly difficult to manage IT security risk. So this paper deals with Security at the application level in cloud.

1. INTRODUCTION

The aim of this paper is to do research on security in Cloud Computing by authenticating a Blob by some secure algorithm like HMAC for an account [12]. First step of the research is to know about the security principle for designing a solution that was specified by NIST for Cloud Security policies and management. Next we must understand the concept of Authentication, Identification and Authorization. After that we must understand the concept of Storage Account which will be used for authentication purpose and then we need to know about Blob for which the access will be provided for certain duration of time. By applying algorithms like HMAC [10] [12] we are going to generate the access key which will be unique and the probability of generating the same key will be very rare and the key will be valid for only certain period of time and after that period the key will get expired.

2. MOTIVATION

The users of cloud computing work with application and data that is not located at their premise. So the organizations are also uncomfortable with this idea and there is also lack of knowledge about this. The goal of this research is to provide an authentication mechanism for the users of cloud services for limited period of time in a stepwise fashion

3. FUNCTIONALITY OF CLOUD COMPUTING

The concept of cloud was introduced by Amazon. Amazon was in the business of selling goods and gift items. In the peak season like Christmas, lots of people use to buy gift items and other goods, so the load on their server increases to great extent. In order to run their business smoothly, they increased their server capability. But what about off season, the servers were idle and they have to be kept running which in turn

consumes lots of power and at the same time power was consumed in cooling them. So the Amazon decided to rent out their servers in the off season to others, such that they can make money out of it. This is how the concept of cloud computing evolved as Infrastructure as a Service (IaaS). Later the concept of Platform as a service (PaaS) and Software as a Service (SaaS) evolved.

Software-as-a-Service(SaaS): The SaaS service model offers the services as applications to the consumer, using standardized interfaces. The services run on top of a cloud infrastructure, with cloud infrastructure being invisible for the consumer. The responsibility of the management the application, operating systems and underlying infrastructure lies within the domain of cloud provider. The consumer can only control some of the user-specific application configuration settings.

Platform-as-a-Service (PaaS): The PaaS service model offers the services as operation and development platforms to the consumer. The consumer can use the platform to develop and run his own applications, supported by a underlying cloud-based infrastructure. "The consumer does not manage or control the underlying cloud-based infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations". The cloud provider is responsible for the management of operating systems, network, servers and other computing resources.

Infrastructure-as-a-Service (IaaS): The IaaS service model is the lowest service model in the technology stack, offering infrastructure resources as a service, such as raw data storage, with processing power and increased network capacity. The consumer can the use IaaS based service offerings to deploy his own operating systems and applications, offering a wider variety of deployment possibilities for a consumer than the PaaS and SaaS models. It opens a new horizon for user for deployment of resources with greater flexibility. "The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components

4. DRAWBACKS OF CLOUD

4.1. SECURITY & PRIVACY

Users might not be comfortable handing over their data to a third party. This is an even greater concern when it comes to companies that wish to keep their sensitive information on cloud servers. Ensuring that a client's data is not accessed by any unauthorized users is of great importance for any cloud service. To make their servers more secure, cloud service vendors have

developed password protected accounts, security servers through which all data being transferred must pass and data encryption techniques.

4.2. *DEPENDENCY (LOSS OF CONTROL):*

Quality problems with CSP (Cloud Service Providers). No influence on maintenance levels and fix frequency when using cloud services from a CSP. No or little insight in CSP contingency procedures, especially backup, restore and disaster recovery. No easy migration to another CSP. Measurement of resource usage and end user activities lies in the hands of the CSP and tied to the financial health of another Company.

4.3. *COST*

While in the long run, cloud hosting is a lot cheaper than traditional technologies, the fact that it's currently new and has to be researched and improved actually makes it more expensive.

4.4. *DECREASED FLEXIBILITY*

This is only a temporary problem (as the others on this list), but current technologies are still in the testing stages, so they don't really offer the flexibility they promise. Of course, that'll change in the future, but some of the current users might have to deal with the facts that their cloud server is difficult or impossible to upgrade without losing some data.

4.5. *KNOWLEDGE AND INTEGRATION.*

More and deeper knowledge is required for implementing and managing SLA contracts with CSP's. Since all knowledge about the working of the cloud (e.g. hardware, software, virtualization, deployment) is concentrated at the CSP, it is hard to get grip on the CSP. Integration with equipment hosted in other data centers is difficult to achieve. Peripherals integration. (Bulk)Printers and local security IT equipment (e.g. access systems) is difficult to integrate. But also (personal) USB devices or smart phones or groupware and email systems are difficult to integrate.

5. RELATED WORK

There is a storage access key that is generated when we create a storage account and it is of 512 bits which may be used when the storage account is accessed and this is default one for the owner and our target in the research is to generate a different key each time who wanted to use the Blob and this key will be valid for certain amount of time only and after that it will get expired [3].

6. SECURITY IN CLOUD

There are four layers of security which can be implemented in cloud [9].

1. Physical security
2. Operating System/Database Security
3. Network security
4. Application Security

6.1. *PHYSICAL SECURITY*

Physical Security can be implemented by appointing a security guard on the premises where our servers and sensitive data is present. He will take

care and will be responsible of all kind of accesses and entry for that premises and a record can be maintained either in hard copy or in softcopy of the persons entering or leaving the premises with their names, address, phone number, purpose, time of entry and exit, so that the person responsible for any kind of future damage can be tracked down.

6.2. *OPERATING SYSTEM / DATABASE SECURITY*

Next level of security is the operating system and database security. The need for operating system based security is that any system can be globally accessible through a set of vast inter and intra-network connections [9]. Another reason is transition motivated by the need to work remotely, convenience in accessing personal records. Convenience and efficiency will increase security risks. The most important reason is that even a single security loophole in the OS design known to a malicious attacker could do serious damage [9]. For implementing operating system based security in azure "Windows Live Id" is provided. There are Security Descriptors that represent access rights of a logged-in user. There is Object Manager that reads the security descriptors and passes on the information to the Security Reference Monitor (SRM). SRM determines whether a user's action is legal or illegal. We can encrypt file system for providing security.

6.3. *NETWORK SECURITY*

Next level of security is network security where we can do the setup of a firewall which is going to monitor the incoming and outgoing traffic in our network. Now the question arises, that can be set up a firewall in azure? The answer is yes.

6.3.1. *CONTROLLING ACCESS TO YOUR DATA WITH THE FIREWALL IN AZURE*

The source IP address is checked against a list of allowed sources before an incoming connection. If the source address is not in this list, the connection is denied. There are no other rules supported, just the list of allowed addresses. The list is stored in the master database for your SQL Azure database server [4]. To manage your firewall rules through code, you can create a connection to the master database with your administrator account and use the provided stored procedures: `sp_set_firewall_rule` will create a firewall rule, and `sp_delete_firewall_rule` will remove a rule [4].

6.4. *APPLICATION SECURITY*

The final level of security is application security in which the application can only be accessed by providing some kind of credentials only and by providing the type of credentials we can further divide the application security in four types

1. Identity based access
2. Role based access
3. Key based access
4. Claim based access

6.4.1. *IDENTITY BASED ACCESS*

In identity based access a username and password is provided by the user and if they matches with the records in the database then only the access is provided otherwise the access is denied. Now the username can be of many types for example, name, email address, id proofs like driving license number, pan card number, ssn number in America, Uid number in India etc which will uniquely identify that person. In case of email id we have got additional advantage that in case of lost password we the issuing authority can send the new password to that email id. We can also enjoy the advantage of email id with other identity types if we take email id as an input at the time of registering.

6.4.2. ROLE BASED ACCESS

In role based identity a role is associated with the user like administrator, developer etc and the application changes the view according to the role of that user. Other credentials are also stored while issuing the role based identity to that user for security purpose.

6.4.3. KEY BASED ACCESS

In key based identity the end user is provided a key and by using that key only the end user can access the services. This key is also stored in the database for verification. This key is encrypted and is generally very long such that no one can guess it. The level of security is very high with key based identity. It is generally associated with a time stamp and the services can only be enjoyed generally for certain amount of time only like 1 day or 6 hours, 1 month etc.

6.4.4. CLAIM BASED ACCESS

In claim based identity a live id is created for a particular brand and all other services provided by that particular brand are accessed by that id. This is done because the end user or customer does not want to or does not prefer to create a new id and remembering the credentials each time for using the different services of that particular brand. The end user never likes filling the form each time for different services of that particular brand. So in order to attract customer to use their services without any pain and at the same time not compromising with the security claim based identity has been introduced and efforts and cost for maintain the data also reduce to great extent and at the same time we can track the data that how many services and what type of the services has been accessed by a particular type of person and this data can be used for data warehousing purpose. The example of claim based identity is Google id which is same for Gmail, Google+, Blogspot, Google search etc. Similarly Windows live id which is common for downloading all kinds of software provided for Windows. Similarly facebook id which is not only accepted by facebook but also accepted by websites of other brands also like Scribd as an additional type for login purpose.

7. ALGORITHM

- Step 1: Design a class
- Step 2: Declare private members for the endpoint of Blob, account name and access key
- Step 3: Create a container
- Step 4: Upload a blob in the Container
- Step 5: Create a shared access signature based on a Shared Access Policy
- Step 6: Specify that we want read access or write access on a blob for say 30 minutes.
- Step 7: Create a Shared Access Signature
- Step 8: Create a string to sign into the account with desired permissions with start and expiration time
- Step 9: Create an HMACSHA256 instance from the access key and by using it create an HMAC from the string to sign.
- Step 10: Use a shared access signature to initialize a Storage Credentials instance, which will be used to create a Cloud Blob Client. We use cloud blob client to construct the Cloud Blob Container and download the content of a blob.
- Step 11: By using Http Web Request and Http Web Response download of the content of a blob is made possible.

8. STORAGE ACCOUNT

Windows Azure which is an operating system for cloud environment has Blob, Table and Queue services and a Storage account provides access to the application stored in it. So we need a Storage Account to use Windows Azure storage [5]. The amount of data that can be stored in a storage account is up to 100 TB in the form of Blob, queue and table. A single user can create up to five storage accounts in Windows Azure. The cost of storage can be based on the percentage utilization of the storage as well as on the transactions required for reading, updating, adding and deleting the data stored. For billing average usage of the storage is calculated [5] [11]. There are different types of storage policies which are based on redundancy to overcome failure and for continuation of business in case if one of the system goes down. There is geo redundant storage (GRS) which are at the highest level of durability and like a dream replicating data at some other location [11]. Here redundancy is the key for fault tolerant system. If there is failure at primary location then secondary location which is 100 of miles away from the primary location is used for the continuation of the business. This feature can be turned on or off and it depends on the user requirement [11]. There is another storage policy called locally redundant storage which is highly durable and available in nature. All the redundant storages are available at the same location and data is replicated three times. Windows Azure is a locally redundant system and if we need GRS then additional cost has to be paid. We can group storage accounts in cloud service deployment in Windows Azure and this grouping is called affinity group [6]. We need to know about endpoints in storage account because they will be used while coding to represent the storage account and the default format of the endpoints are as follows [11]:

Blob service:

<http://Ankurstorageaccount.blob.core.windows.net>

Table service:

<http://Ankurstorageaccount.table.core.windows.net>

Queue service:

<http://Ankurstorageaccount.queue.core.windows.net>

There is a URL for accessing a storage account and is built by appending the location of object by its endpoint in the storage account. For example it may in the format of: <http://Ankurstorageaccount.blob.core.windows.net/mycontainer/myblob>.

8.1. BLOBS IN THE AZURE ECOSYSTEM

In Windows Azure system Blobs is the among the simplest storage technique available. Blob stores the file in binary format that is why they are named as binary large object. Blobs are further classified in two types page Blobs and block Blobs, we are going to use block Blobs in our research. Steaming is the purpose why these block Blobs are designed and read write is the purpose why the page Blobs were designed. The maximum size of block Blobs is 200 GB and that of page Blobs is 1 TB. Blobs are use to store images and videos where as in our local system we would have stored them in the files of some folder. In Azure System Blobs are stored in Containers. There can be any number of containers in a Windows Azure account [11].The permissions that can be

given to Blobs are public read or private and this access is done at container level. The size of metadata that a container can have is up to 8 KB. The maximum size of each Blob is up to 1 TB. Each blob is replicated minimum three times for the reason of scalability and protection of data. There are hot blobs also who are served from multiple servers. The Development storage Blobs can serve only 2 GB of data though a normal Blob can store 1 TB of data [11].

8.2. MODEL FOR DATA STORAGE IN BLOB

There are four components in Blob Storage model and these components are as follows:

- a. Storage account
- b. Containers
- c. Blobs
- d. Blocks or pages

We can think of a container as a folder holding some files and these files are Blobs. These Blobs contains one or more Blocks or pages of data [11]. We can get and set Access Control List (ACL) for containers. We can List all containers, create and delete containers, retrieve and set properties and metadata of all containers. Similarly we can create a Blob Container, access Blob Storage, upload Blobs to Containers, list the Files in a Blob Container, access Blobs and delete Blobs [11].

8.3. Basic Mechanism for accessing the Blob:

An application can be designed for uploading and then accessing the Blob. In Blobs we can store our data. But this data is not secure because it is public and anyone can access it. If we want to allow that certain person should only access that data then some security mechanism should be implemented in that application. We can also control the time of access by specifying the time in that application which will be common for all. For designing this application you should be aware of .net and programming in Windows Azure. For designing this application we have write a Web Role, Design.aspx and .cs file. Web Role is used to handle the clients reaching the front end, Design.aspx is used to provide the look and feel of the application and Event Handling is done to make the controls present on the front end fire the events. The cs file is used to write the business logic for providing the security token and time for which that token is valid.

9. RESULTS

We have suggested the levels at which we can apply security in cloud computing. This differentiation at different levels will simplify the approach for dealing with security issues in cloud and will help in developing a vision to work at which level for securing the cloud environment. There are two screenshots of the output of the two application are attached, in which 1st screenshot represent the output in which security is not applied and with the help of url generated we can download the Blob where as in 2nd screenshot after clicking the url a Secured access token is generated and now this is the only way through which we can access the Blob. We can also see in the 2nd screenshot that the image is not visible even at the time of generation of token, so the system is secure. The time for accessing the Blob is also limited which can be changes according to requirement but it will be common for all This ensures the Application level security in cloud by providing a token which is difficult to regenerate and remember.

10. FUTURE WORK

In Future we can work in AppFabric which is used to make changes in operating system and we can enhance the security of the Azure. Firewalls can also be used so we can suggest certain measures which can increase the security of our data in Azure. We can also do research to uncover the security loopholes of Azure and then we can suggest these loopholes to Microsoft, so that they can avoid future attacks on Azure by taking some remedy steps. For application level security we design application which are based on Claim based access and we can use Id of facebook as an additional login credentials for logging in the application.

11. CONCLUSION

We conclude with that we can implement Application level security in cloud by providing a shared access token. We have also talked about other levels of security that can be applied in cloud. We have also talked about different types of security available in Application level security in particular. We have also given the answer for implementing firewall in network level security in cloud. We have talked about some principles that should be kept in mind while proposing a solution for security in cloud. We have also talked about the size of data that can be stored in a blob. We have talked about the availability of blobs in case of any failure and the models for creating replicas to avoid the unavailability in case of any failure. In the end we have talked about secured as well as unsecured access of blob contents. So in total we have can make sure that our data is more secure in Azure cloud than at our premises but we must have confidence in Microsoft so that our interests are served.

REFERENCES

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines
2. The Cloud: Understanding the Security, Privacy and Trust Challenges, Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey (RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick)
3. Windows Aure step by Step, Roberto Brunneti
4. Azure in Action, , Chris Hey, Brain H Prince
5. Data Storage Security in Cloud S.Sajithabanu, Dr.E.George Prakash Raj
6. An Analysis of The Cloud Computing Security Problem, Mohamed Al Morsy, John Grundy and Ingo Müller Computer Science & Software Engineering, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia
7. Security and Privacy in Cloud Computing: A Survey Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou Software Engineering Institute, East China Normal University, Shanghai 200062, China. National Institute of Information and Communications Technology, Kyoto 619-0289, Japan
8. Cloud Computing Security Issues and Challenges, Kuyoro S. O, Ibikunle F, Awodele O.
9. Windows Azure™ Security Overview Charlie Kaufman and Ramanathan Venkatapathy
10. Hmac Vs Mac, Layron Walker Master of Information Technology and Internet Security June 2010.
11. Introducing the Azure Services Platform, David Chappell October 2008.
12. The Keyed-Hash Message Authentication Code (HMAC), Donald L. Evans, Secretary U.S. Department of Commerce Technology

Administration Philip J. Bond, Under Secretary National Institute of Standards and Technology Arden L. Bement, Jr., Director

13. Cloud Security Challenges and Solutions, Balraj S Boparai CISSP.
14. Security in Cloud Computing by HMAC Algorithm Ankur Pandey (Mtech Scholar CSE) Thakral College of Technology Bhopal
15. IBM point of view: security and cloud computing.

Containers:

myblobstorage x
 test x
 wad-control-container x

Name of the Container, after clicking Container the blobs stored in Container appears

test

http://127.0.0.1:10000/devstoreaccount1/test/Chrysanthemum.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Desert.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Hydrangeas.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Jellyfish.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Koala.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Lighthouse.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Penguins.jpg x
 http://127.0.0.1:10000/devstoreaccount1/test/Tulips.jpg x

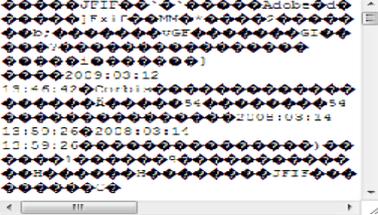
This url is used to download the Blob and is open for all

Upload blob:

File: No file chosen



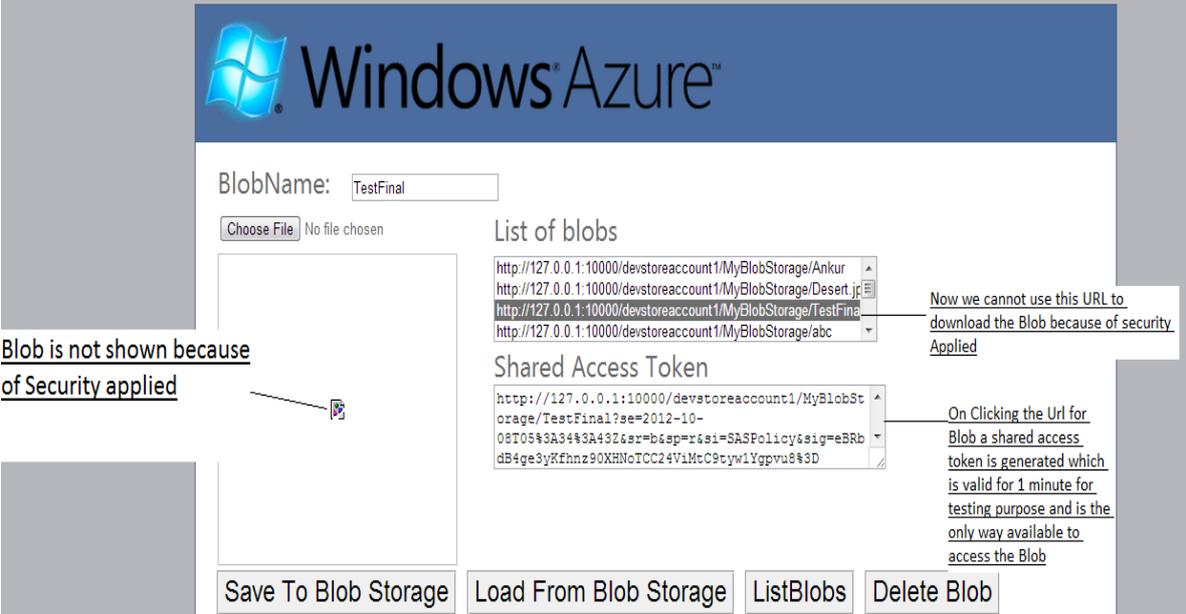
Contents of Blob



Default functionality without security

SCREEN SHOT - 1

← → C 127.0.0.2:81/BlobPage.aspx



Blob is not shown because of Security applied

Now we cannot use this URL to download the Blob because of security Applied

On Clicking the Url for Blob a shared access token is generated which is valid for 1 minute for testing purpose and is the only way available to access the Blob

SCREEN SHOT - 2