International Journal of Research in Advent Technology, Vol.2, No.7, July 2014
E-ISSN: 2321-9637

Security as a Service: Cryptology on Demand

Venkatesh Ranga[1], M.S.V. Sashi kumar[2], Dr. C.R.K.Reddy[3]
M.Tech CSE[1] , Assistant Professor CSE[2], Professor CSE[3], Osmania University[1,2,3]
venkuranga@gmail.com[1], sashi.mamidanna@gmail.com[2], crkreddy@gmail.com

Abstract- Cloud Computing is becoming more and more popular today and is ever increasing in popularity with large organizations as they sharing valuable resources in a cost effective way. By doing like this increasing demand for more clouds there is an ever growing threat of security becoming a major issue. Achieving strong security would often require large IT resource and also result in difficulty of usage. To increase security while reducing the spending on IT & improving the ease of use, we require a security technique which can configure itself, as requested, for services offered in a Cloud environment. This paper mainly focus on by the usage of less resources how can we provide security to the end user. The security architecture is driven by security policies based on these inputs into consideration.

1. Network Access Risk
2. User Data.
3. Key size

With these inputs in place, the security policies can generate security parameters which in turn are used to configure mechanisms to alter security (including algorithms and protocols) at every domain for protection of specific security services. Security requirements from users and services in cloud computing in turn building trust for the end users via Security at their ease & also data control.
Key words: Cloud; Encryption; Security.

1. INTRODUCTION

Cloud computing has been defined by NIST as a model for enabling ubiquitous, on- demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction . In simple words cloud computing is a accessing some one's software in some one' hardware in some one's data centre .Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. The term itself is often used today with a range of meanings and interpretations.

Three referenced service models have evolved:

Software-as-a-Service (SaaS): Is a way of delivering applications over the Internet. Instead of installing and maintaining software, you simply access it via the Internet. SaaS applications are sometimes called Web-based software or hosted software. Whatever name we can call it as, SaaS applications run on a SaaS provider's servers. The provider manages the access to the application, includes security, availability, and performance. It can reduce the total cost of hardware and software development and operations.

Platform-as-a-Service (PaaS): Platform as a Service (PaaS) is a way to use some one's hardware, operating systems, storage and network capacity over the Internet. The service delivery models are allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones. It can reduce the cost and managing hardware and software components of the platform.

Infrastructure-as-a-Service (IaaS): Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers. The service provider maintains the equipment and is responsible for housing, running and managing it. The client typically pays on a how much they are use that much amount customers will pay to service providers pay per use basis.

The most popular cloud types are namely private, public and hybrid clouds. In a private cloud, total infrastructure for implementing the cloud is controlled completely by the enterprise. Typically, private clouds are maintained and implemented in the enterprise data centre and managed by internal resources. A private cloud maintains all data in resources under the control of the legal and contractual umbrella of the organization. This eliminates the regulatory and legal security concerns represented with information being processed on third party computing resources. In a public cloud, external organization provides the infrastructure and management required to implement the cloud. Public clouds orderly simplify implementation and are typically billed based on usage of resources. This transfers the cost from a capital expenditure to an operational expense and can quickly be scaled to meet the organization's needs.

Security has been and is the biggest challenge to cloud computing. It is hard for the users

to believe in cloud computing due to invisibility of the user's data storage and how are they protected. Research says that as of now there is no way to know if the cloud providers properly remove a client's data, or whether they have saved it for some unidentified reason. Currently, the study on cloud security still lies in the preliminary study. For data storage, a TPA (Third Party Auditor) is proposed to verify the integrity of the dynamic data stored in the cloud.

In trust management field, some experts considered that multiple security policies should be used in user's authentication and identity management, and those policies must be able to avoid intrusion of data by unauthorized users.

2. PROBLEM DESCRIPTION:

Security parameters even differ for a specific service for two different users depending on the sensitivity of the information. The solution for these issues can simply be the usage of a highly complicated and secure algorithm popularly used to safeguard all services in the network. Potentially, this might not be effective way for cloud service providers to use the same security mechanism throughout the services since it consumes a lot of IT resources every time. It would not be a solution to consume resources for security itself, as we counteract the advantage of cloud computing platform wasting the available resources.

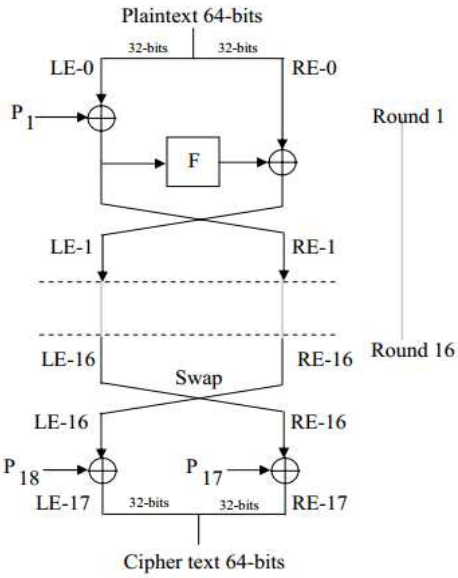
By considering all the applications in the cloud environment, all the applications are using Sha1 for authentication.AES and DES security algorithms to secure the data. Most of the applications are using same symmetric key algorithm for encrypting the any amount data and providing security to the user's data.

By using same variable key length for the any amount of data it will take more time for encryption/decryption and processing of the data .Using the same key for encryption/ decryption take same time when the data size is differ. If the data size is small then it will take same time and increases the data size. In our approach we can change the algorithm key size. When the size of the data changes If we uploading large data we can use large for foe security. If transferring data is small than we can go for small key to encrypt the data. Depending on the size of the file we can change the algorithm key size. By doing like this we can boost the performance of the CPU.

3. CRYPTOGRAPHIC ALGORITHM:

As far we are saying that every application is using same encryption key for encrypting the data. Most of the applications are using SHA1 for providing the security for the user authentication and some symmetric key algorithm for the encrypting the users data. In this paper we are using other symmetric algorithm called Blowfish. As per Researches Blowfish has been shown better results compare to other encryption algorithms. So In my Application we are using blowfish algorithm for encrypting the data. Blowfish algorithm is a symmetric block cipher that can be effectively used for both encryption and safeguarding of data. Blowfish algorithm is a Feistel Network and 64-bit block size and a variable key length from 32 bits to 448 bits in length, to calculate sub keys, which are used in the actual encryption and decryption. The P-array consists of 18 32-bit values while the 4 s-boxes consist of 256 32-bit values. The P-array is initialized first and followed by the S-boxes. It is a 16-round Feistel network for encryption and decryption. The algorithm was developed to 64-bit plaintext into 64 bit cipher securely.

ENCRYPTION:



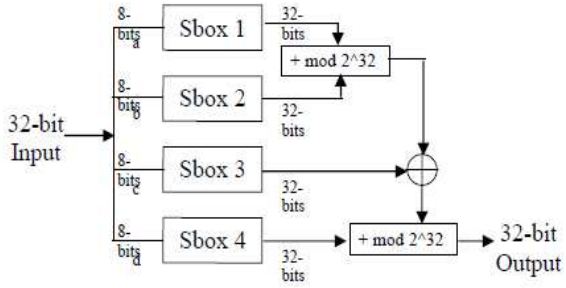
Blowfish has 16 rounds.
The input is a 64-bit data element, X
Divide x into 32-bit halves, XL, XR;
Then i= 1 to 16;
XL = XL XOR Pi
XR = F (XL) XOR XR;
Swap XL and XR;
After the 16th round, swap XL and XR again to undo the last swap.

Then, XR = XR XOR P17 and XL =XL XOR P18, Finally, recombine XL and XR to get the cipher.

Decryption same as encryption, except that P1, P2, P3, P4…... and P18 are used in the reverse order.

Blow fish is incorporated a bitwise exclusive-operation to be performed on the left 32 – bits before modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation.

F- Function:



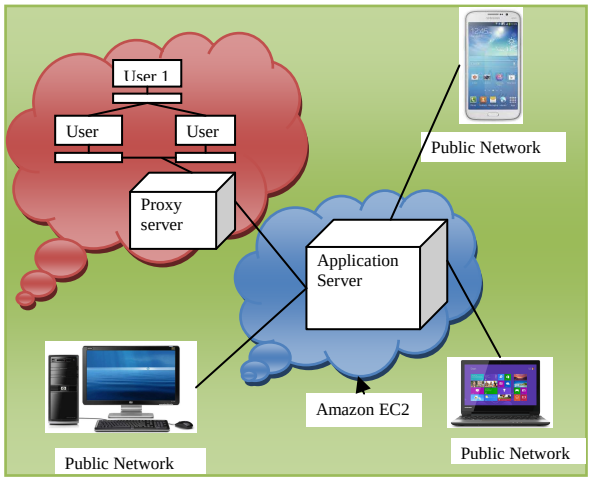
All the applications are using same encryption algorithm and same key large key for protecting the data. For providing the security to the users the application developers are using large key. By using the large key it will more computation and time. So In my approach we are differentiating the users considering the network from where the user is accessing the application and user computation. By considering these two factors we can provide security to the users. We can differentiate the user's security type by writing the policies in the application."

4. APPLICATION SCENARIO:

In this paper am trying to show the application which it is self configure the security by taking the above parameters into the consideration. As per my knowledge all the existing applications are using same security mechanism in the applications for all the users. So by this there is a chance of wastage of resources. As we already know in the cloud security is the biggest challenge. For transmitting the data between the two users we can not the transfer the data directly. We are using some encryption mechanism to transfer the data. For that we have to choose best encryption algorithm to give better results. If the conversation between the two friends i.e. normal information there is no need usage of large bit key .Whenever we are transmitting secret information (confidential) then we need more security so there we can use large key to encrypt the data. By considering the user's network we can change the algorithm key bit length. If the two user's are from same network then we can use small encryption key to transfer the data and if the user's are from different and untrusted network then we can increase the bit size. By using same key for everytime the system is more computation for encrypting and decrypting the data. So differcting the key lenth we can reduce the usage of computation in the system and time as well as we can also reduce the power.

For Example:

In an Enterprise the users are connected to each other then they are considered to be internal network. From the figure we can observe that User1, User2 and User3 are in same private ntework acessing the application hosted some where in the cloud environment, User4 and User5(mobile user) with different processing power devices are from public network and accessing the same application from the outside other than the office network. Whenever User1 is tranferring the data to the User2 then we can provide security with 128-bit(small) key.



In the internal network the users can access the application through the proxy server which is mainted in the internal network. The internal network users are access the application which is loacated in the cloud with the help of proxy server(which maitains the cloud application) . If the users are intrating in the public network users then increse the algorithm bit size to 256-bit key for encrypting the data. If the user is trying to access the application from the public network then we can increase the algorithm bit size i.e to 448-bit key to encrypt the data to incearse the security. In our approach we are tested our application with two symmetric encryption algorithms i.e blowfish and AES. Most of the application developers are using AES for encrypting the data . In our approach we are replacing the AES with Blowfish.We use blowfish for encryption/decryption of data.From the study learnt that blowfish performance is better when compare to other algorithms. So we can change the encryption algorithm according to the user requirement. We are tested two algorithms with different files size of data by using changing the algorithm key sizes . We got below results when tested with different algorithm key sizes.

5. RESULTS:

Table 1 Encryption and decryption times(in milli sec) using with 128 –bit key

Input in KB	Encryption time for blowfish with 128-bit key	Encryption time for AES with 128-bit key	Decryption times for Blowfish 128-bit key	Decryption time for AES with 128 -bit key
312	46.46	146.544	405.75	1316.767
512	47.187	147.921	433	1776
1536	128.288	212.455	413.253	1152.631
2048	194.824	284.029	440.054	1133.744
5120	401.911	698.02	389.548	1412.936
10240	686.988	671.422	674.928	1277.063

Table 2 Encryption and decryption times(in milli sec) using with 192 –bit key

Input In KB	Encryption time for blowfish with 192-bit key	Encryption time for AES with 192-bit key	Decryption times for Blowfish 192-bit key	Decryption times for AES 192-bit key
312	46.87	147.995	436.715	1594.123
512	60.087	156.341	447.156	1900.74
1536	142.58	283.82	423.55	1237.054
2048	184.984	391.643	440.152	1429.581
5120	409.484	761.41	417.677	1215.91
10240	725.4906	748.392	721.291	1194.154

Table 3 Encryption and decryption times(in milli sec) using with 256 –bit key

Input in KB	Encryption time for blowfish with 256-bit key	Encryption time for AES with 256-bit key	Decryption times for Blowfish 256-bit key	Decryption times for AES 256-bit key
312	47.187	160.1749	450.955	1966.08
512	58.975	176.32	428.948	1646.9
1536	136.563	301.1285	425.802	1254.111
2048	183.296	435.471	424.453	1418.943
5120	401.911	759.309	389.548	1117.111
10240	752.497	717.192	784.397	958.822

Table 4. Encryption and decryption times(in milli sec) using AES 256-bit key and 448-bit key

Input In KB	Encryption time for AES 256-bit key	Encryption time for Blowfish 448-bit key	Decryption time for AES 256-bit key	Decryption time for Blowfish 448-bit key
512	176.32	64.608	1646.9	771.544
1536	301.1285	143.8252	1254.111	846.725
2048	435.471	196.234	1418.943	465.208
5120	759.309	414.739	117.111	738.094
10240	717.192	808.402	958.822	717.601

Figure :1 Encryption and Decryption times for Blowfish and AES with 128-bit Key

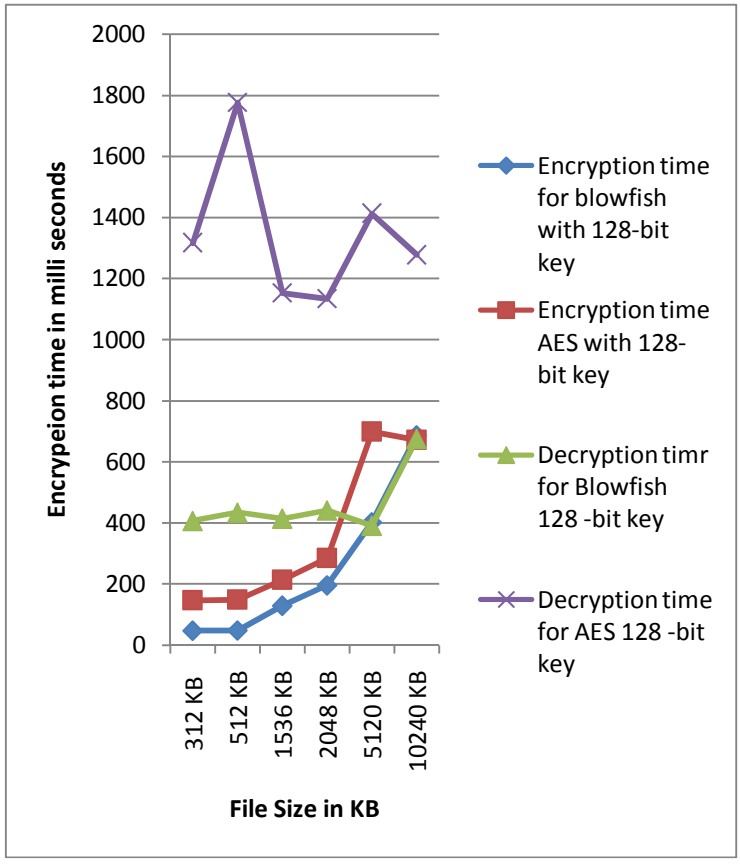


Figure 2. Encryption and Decryption times for Blowfish and AES with 192-bit Key

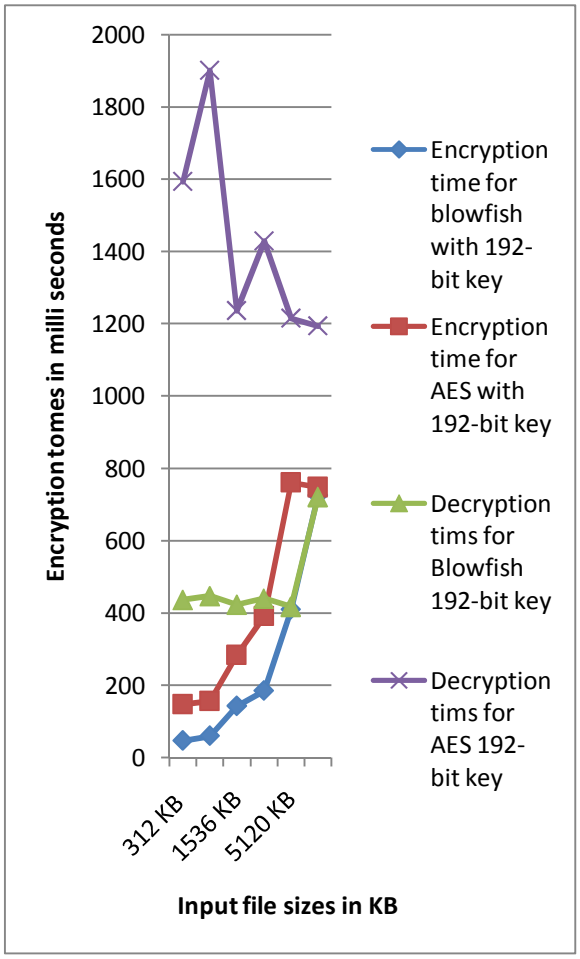


Figure 3. Encryption and Decryption times for Blowfish and AES with 256-bit Key

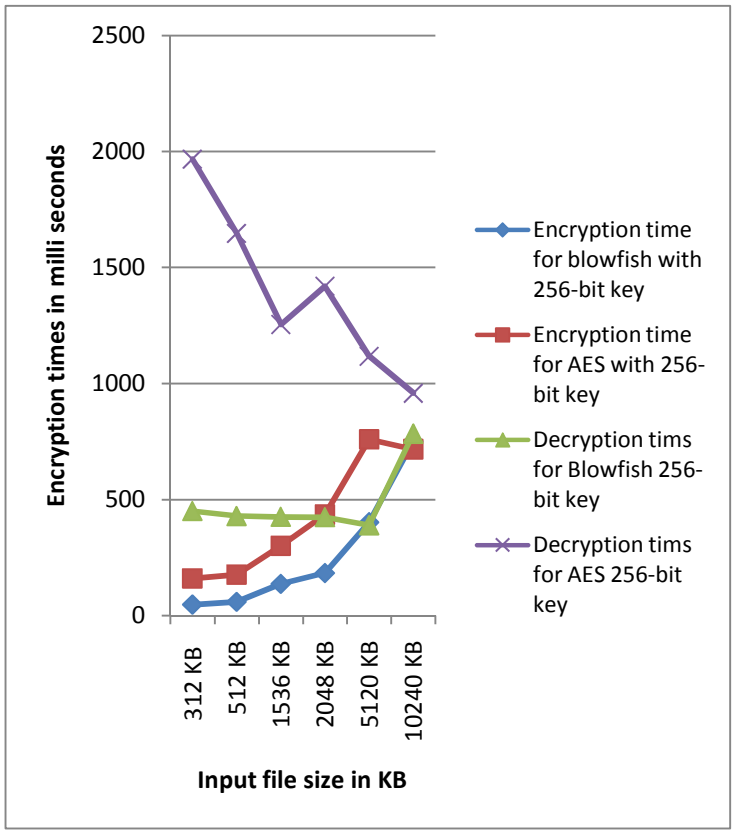
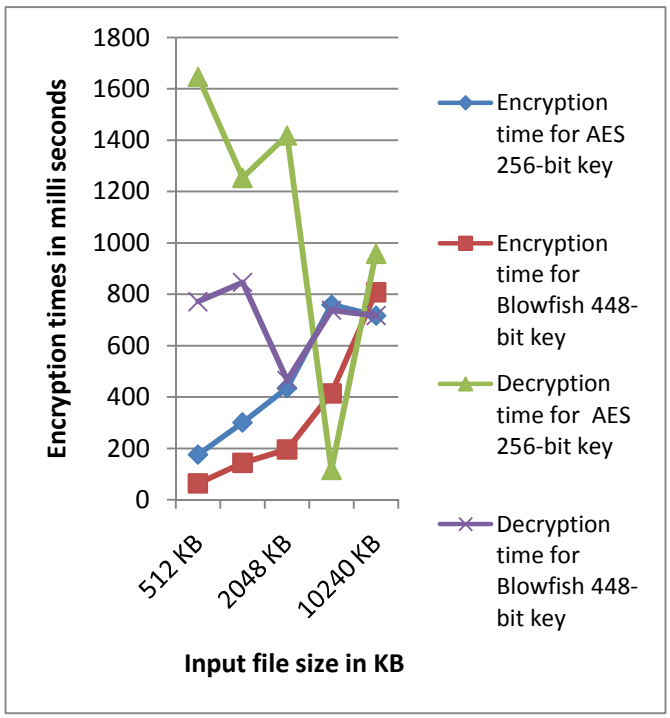


Figure 4 Comparision Between the Encryption and Decryption Times with AES 256 and Blowfish 448- bit



6. CONCLUSION :

In this paper we conclude that depending on the network users are being a part of, type of the application working on & the compute system used, we can provide the required security strengh by using best suited algorithm and varied key size. Transferring files from one network to another can be provided with on demand security level by increasing the bit size of the key. This feature can be provided on varied applications and deploying right security policy, the performance of the systems can be improved. From the comparision of two algorithms we found that blowfish performs well in all situations, but the key establishment still remains the concern. In traditional applications for encrypting any size of data, developers are using same key size for cryptography. In our scenario , we have varied the key size of the algorithm and the chosen algorithm depends on file size, user requirement and type of network. Usage of same key for encrypting and decrypting any amount of data, the allocation time for encryption and decryption taken more resouces in hardware and more time for processing the data will decrease the performance of the CPU. Applying right algorithm in the requirement will boost the performence of the CPU, reduce the usage hardware inturn reduce the processing time.

REFERENCES:

[1] P. Mell, T. Grance (2009), The NIST Definition of Cloud Computing, Version 15, National Institute of Standards and Technology.

[2] Jianyong Chen, Yang Wang, Xiaomin Wang (2011), On demand security architecture for Cloud Computing, Dept.of Computer science and Technology, China.

[3]M. Anand Kumar and Dr.S.Karthikeyan (2012), “Investigating the Efficiency Blowfish and Rejineal (AES)Algorithms”, I.J computer network and Information Technology.

[4] Pratap Chandra Mandal (2012),”Superiority of Blowfish Algorithm” IJARCSSE, WestBengal,India.

[5]http://docs.aws.amazon.com/gettingstarted/latest/Compute basis/web-app-hosting-intro.html

[6] http://en.wikipedia.org/wiki/Blowfish (cipher).