ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Securing Cloud Resource Allocation Requests with Tls Connections Mandate and Improving DH Key Exchange with Additional Security Factor

[1] Kulvinder Singh, [2] Dr. Ajit Singh
[1][2] Department of Computer Science
[1] Doon Institute of Engineering & Technology, Uttrakhand, India, [3] BTKIT, Dwarhat, Uttrakhand, India

***Abstract* - Today cloud computing is seen as the feature of IT industry. Use of IAAS, PAAS and SAAS is transforming capital expenses (CapEx) into operational expenses (OpEx) without sacrificing performance of communication and without compromising security and even streamlines workload with maximum profits. As organization look to build up modern IT architecture that scales rapidly and globally while supporting numerous digital channels and a variety of devices, the cloud is nothing less than critical. This paper, on one hand, exaggerates cloud feature like SSO with its underlying implementation details using SAML, improves communication security at TLS level and uses improved DH as "DH with an ASCII digit" to secure (handshake) public and private key shared on the network, on the other hand. These two additional security factors make cloud users more immune & secure and cloud security invincible for eavesdroppers/ attackers.**

Index Terms — DH, SSO, SAML, LDAP, TLS, SSL, IAM, CSP

INTRODUCTION

Now a day's every individual internet user, Service providers, small and medium businesses and huge enterprises all are shifting towards cloud computing model because of its immense benefits which includes enormous scalability, on demand service, rapid elasticity, pay as you go, self provisioning of resources, high availability, very low cost as compared to capital investments etc. While availing all these technological facilities user are prone to network attacks like fabrication attacks, masquerade, eavesdropping, identity spoofing, man in middle etc. and security of cloud users, networks and CSP's become severe issue. Although IAM software made a substantial advancement in authentication process over the internet and SSO which is enabled by LDAP to access different directories or databases to verify and validate users for websites, apps or API has revolutionized the use of different applications and accounts with a single identity. Considering the directory or database as a resource which is to be accessed to validate users using their username, password and security codes etc. to provide SSO over various related accounts of apps, websites or API's, there is a need to secure such a resource allocation within cloud. This is achieved through proposed model of TLS mandate and Diffie Hellman Key Exchange with additional ASCII digit in this paper.

IDENTITY AND ACCESS MANAGEMENT

Identity and access management (IAM) is a set of rules and technologies used for security purposes which controls access to the critical data within an enterprise. When a number of applications are being accessed using cloud computing framework, it becomes crucial to verify authentication properly and accurately. It provides a framework which can authenticate individuals for having the suitable permission and check the rights to access the information/ services/ applications.

SINGLE SIGN ON

SSO- Single Sign On enables user to login once and use or access all the related web applications/services with a single click. With a view to its vast application domain and easy to implement protocols, SSO becomes crucial and an integrated part of any cloud service provider. There is no need to login again and again to use other related applications or services from same service provider. This eliminates password fatigue and risks of security. Users can use application software (IAM's) like OneLogin for SSO (Single Sign-On) to secure and safe their enterprise customers accounts more efficiently, instead of using huge number of IT administrators and improves regulatory compliance.

OneLogin is an identity management solution that can guarantee the security and sort the trust issues for the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

leading worldwide organization by making authentication centralized, get rid of repeated logins/passwords and makes web applications access convenient and easier for an organization and individuals.

Bringing in ONELOGIN for any enterprise to get any single sign-on within a few minutes via security assertion Mark-up language (SAML). It saves huge amount of time and money as well.

Main advantage of OneLogin secure single sign on integration saves lot of time and money of an organization as well as extends the security of data in the cloud .It is an easy approach that fascinates both client and server. Now days many well known organization like Amazon, Myntra uses OneLogin sign on security system.

SECURITY ASSERTION MARKUP LANGUAGE

Security Assertion Markup Language (SAML) is an important XML based framework protocol which manages and authorization in a network allowing single sign on ability to provide web services by exchange of digitally sign XML documents. Now a day's SAML becomes so popular because it is secure and standardized. Working of SAML is described in the following diagram-

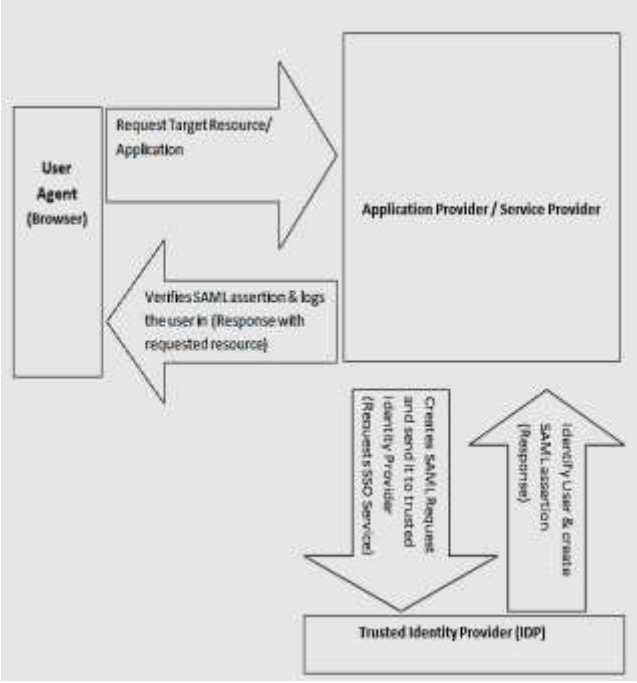


Fig.1.1 SAML authentication cycle

Firstly, user authentication is done by identity provider using a single-sign-on .This is authentication request to determine whether or not a person has been authenticated. SAML token is provided or issued by identity provider with user's identity. It sends SAML assertion to the server that actually provides services for security issues assertion may be encrypted. Identity provider redirects to users browsers of service provider. Work of service provider is to check and validate the SAML token. After successful verification and validation, service provider gives access to the applications.

SAML increases the security by eliminating extra and additionally credentials .It also eliminates phishing attack by eliminating the number of times password entry. It also increases number of access by eliminates barriers to usage by giving passwords. It reduces admin time and cost by eliminate or handling duplicates credentials.

SAML completely eliminates all passwords and deploy applications much faster. SAML use security assertion and encrypted message with a establish trust relationships. TLS-communication security between user and server over the internet is the main role of transport layer security. Main function of TLS is integrating privacy and protection.TLS and SSL gives a way to encrypt a communication channel between two computers.

It is necessary for the client to indicate to the server the setup of a TLS connection, as applications can communicate either with or without TLS (or SSL).
a) One way to achieve this is to use a different port number for TLS(other than HTTPS-443 port)
b) Another way is that the client can make a protocol specific request to the server to switch the connection to TLS. Example – by making a "STARTTLS" request when using the mail and USENET protocols (IMAP, POP3, SMTP, NNTP), "AUTH TLS" request for FTP and "OID" request for LDAP we can convert protocol specific request into private connection.

LDAP- Active directory is a directory service, implemented by Microsoft and supports LDAP. Light weight directory access protocol is a software protocol and a part of x.500.LDAP provides a secure way to store user name and password centrally so that user can be authenticated and allow to access different applications and services over the network. LDAPv3 is the latest specification of LDAP.
PROPOSED MODEL

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

This model is capable of converting all consumer connection requests into TLS connection. It makes a mandate for the cloud servers to run the commands like STARTLS, AUTH TLS and OID etc. which would be embedded in a small script in some scripting language like PERL or Shell scripting that supports Linux Kernel (OS) running on the server.

Shell Script	Perl Script
$ cat myscript.sh	$ cat myscript.sh
#!/bin/sh	#!/usr/bin/perl
	STARTTLS
STARTTLS	AUTH TLS
	OID
AUTH TLS	.
	.
OID	ctrl+d
.	
.	
ctrl+d	

Table 1.1

Any number of commands can be invoked through such a script written in shell or perl scripting language, marked by dots in the table. Script can be run from bin/bash shell after making it executable as follows:

$ chmod ugo+x myscript.sh
$ ./myscript.sh

Running this script will redirect the connection from normal port to SSL port and the further communication will be secured essentially. The port configuration is shown for each protocol with corresponding secure ports used in SSL in below figure

Protocol	Purpose	Normal Port	SSL variant	SSL port
SMTP	Send mail	25/587	SMTPS	465
POP3	Retrieve mail	110	POP3S	995
IMAP	Read mail	143	IMAPS	993
NNTP	News	119/433	NNTPS	563
	reader			
LDAP	Directory access	389	LDAPS	636
FTP	File transfer	21	FTPS	990

Table 1.2

DIFFIE HELLMAN WITH ADDITIONAL ASCII DIGIT

Diffie Hellman Key Exchange/Agreement is a protocol which assures the exchange of private key securely over the network. First of all DH must not be confused with encryption/decryption algorithms, as it is a pure key exchange algorithm. DH gets its security from the difficulty of calculating discrete logarithms in a finite field rather than calculating exponential in the same field, which is comparatively easy. Diffie Hellman is more secure because the secret key doesn't transmit across the network, but some random prime numbers are transmitted.

In our proposed model "Diffie Hellman With Additional ASCII Digit" an ASCII code ranging from small alphabet a to z will be shared on the public network along with an integer such that the summation of shared integer with ASCII code(ASCII value of letter ranging a-z) is a prime number. This combination is shared on the network and is seldom prone to be understood by eavesdroppers who are tracing the communication networks.

Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m
ASCII Value	097	098	099	100	101	102	103	104	105	106	107	108	109

n	o	p	q	r	s	t	u	v	w	x	y	z
110	111	112	113	114	115	116	117	118	119	120	121	122

Table 1.3

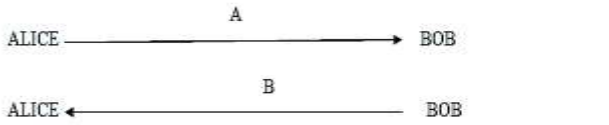
We assume a prime number g and then assuming an ASCII digit say'd'. In this example large prime number to be transmitted is 107, but rather sending 107 over the network we send the addition operation as '7+d' over the network, that gives illusion of sending 7 over the network to the eavesdropper as 7 is a prime but original prime is evaluated at receiver end as 107 because ASCII value of 'd' is 100. Then according to Diffie Hellman key sharing algorithm

Large prime number: q=7+d=107
Primitive root of 107: p=2

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

ALICE	BOB
Random prime selected: a=3	Random prime selected: b=5
$A = p^a \bmod q = 2^3 \bmod 107$	$B = p^b \bmod q = 2^5 \bmod 107$
$A = 8 \bmod 107$	$B = 32 \bmod 107$
$A = 8$	$B = 32$
Public Key of ALICE is 8 bit	Public key of BOB is 32 bit



Alice sends her public key generator to Bob and Bob sends her public key generator to Alice.

Secret Key of Alice	Bob's Secret Key
$S = B^a \bmod q$	$S = A^b \bmod q$
$= 32^3 \bmod 107$	$= 8^5 \bmod 107$
$= 32768 \bmod 107$	$= 32768 \bmod 107$
$= 26$	$= 26$

For the above assumed values public key for Alice is of 8 bit and Bob's public key is of 32 bit both are shared on the network. While both of them agrees on a private key of 26 bit and this is not shared over the network. An encryption key of up to 1024 bit can be used with current cryptography techniques available and current internet infrastructure, however security experts are looking for possibilities of 2048 bit size keys to be used for encryption in near future.

Traditional attackers are habitual of computing discrete logarithm problem which is though computationally infeasible for large prime number. But still attackers are in practice to attempt such a computational to obtain secret key, but inclusion of additional factor of ASCII code will make it unpredictable for attackers that what is the actual prime number and the attempt to compute public or private key will be automatically fail, hence adding one more security factor to DH key exchange algorithm to make it invincible. Use of Ephemeral Diffie Hellman Key exchange algorithm is also desirable to provide Forward Secrecy to any key exchange and hence to the communication.

Method- First we take any prime number q and its primitive root p then pick a secret key a and b for each party. After that, compute qa mod p and pb mod q respectively. Exchange the result (public key) with each other. For compute the secret key does same operation ba mod p and ab mod p for getting the same result which is a shared key for both parties.

CONCLUSION

Firstly, the proposed model successfully achieves secure handshake using " DH with ASCII digit "which makes it infeasible for eavesdroppers to track or find prime number sent on network and hence disable item to compute secret key(private key).
Secondly, it secure the session by converting a normal connection request into TLS request at server level with the help of a shell script running at the server for service requests received.
This model is a little rigorous but it invokes pretty good security for cloud connection and provides operational agility .Further scope of this model is implementation of such security measures in cloud resource allocation systems using Banker's or RAG algorithms.

FUTURE SCOPE

It is a persistent challenge to run a shell script for each HTTP request and to decide which kind of request it is. It is difficult to run all possible commands as shell script every time to convert ordinary HTTP request into TLS connection. Although there could be faster way do this, if we are able to identify what kind of request it is and then to execute single corresponding command to ensure security by creating a private connection.

REFERENCES

1. https://www.teneo.net/wp content/ uploads/ 2017/ 09/ riverbed -stages -cloud -adoption -design-ebook. Pdf

2. Cloud Computing Market Maturity Study Results, CSA Cloud Security Alliance, 2012.

3. "Amazon elastic compute cloud (Amazon EC2)," http://aws. amazon.com/ec2/, 2012.

4. Wailly, M. Lacoste, and H. Debar. Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources. In Workshop on Crytography and Security in Clouds (CSC), 2011.

5. Kulvinder Singh, Sarita Negi "Service Model Specific Security Requirements and Threats in Cloud

Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 7, July 2015.

6. Mohammed A.Alzain,Ben Soh and Eric Pardede, "A survey on data security in cloud Computing,"Journal of software, May 2013.

7. Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing". IEEE. 2010. 978-1-4244-549.

8. Kulvinder Singh, Tanshu Gairola "Cloud Security Issues: Counter DDOS Attack by Integrating IP Monitoring and Routing Protocol" IJARCSSE, Volume 6, Issue 7, July 2016.

9. Toma´s Jirsk, Martin Husak, Pavel Celeda, Zdenek Eichler, "Cloud-based Security Research Testbed: A DDoS Use Case", IEEE, 2014.

10. Kulvinder Singh, Tanshu Gairola "A Review on DOS and DDOS Attacks in Cloud Environment &Security Solutions" International Journal of Computer Science and Mobile Computing,Vol. 5, Issue. 7, July 2016, pg.136 – 141.

11. Virtual Organization Managment Service. http://www.globus.org/ grid_software/security/voms.php.

12. S. Kent, and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, November 1998.

13. Rajkumar Buyya, Rajiv Ranjan and Rodrigo N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", Springer 2010

14. Kulvinder Singh*, Dr. Ajit Singh "An insight into service model specific security in cloud computing" January, 2018 in Global Journal of Engineering Science and Research Management ISSN 2349-4506, Impact Factor: 3.799.

15. Mayank Aggarwal " Cloud Computing a new perspective" presented in National Conference "ETES-2013″ held at GKV,Haridwar, 9-10,Nov,2013.

16. Mayank Aggarwal " Introduction of Cloud Computing and Survey of Simulation Software for Cloud" published in International Journal Research Journal Of Science & IT Management,Vol 2, No. 12, Oct, 13, pp 15-23.ISSN : 2251-1563.

17. Mayank Aggarwal "Virtualization: A concept implementation for Cloud" published in IJETR.Vol 2 , Issue 3,March,2014,pp 52-55.ISSN : 2321-0869

18. Tim Mather, Subra Kumaraswamy, Shahed Latif "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O Rielly Publication