Implementation of Single Sign-On Authentication for Multiple Clouds

Pushpendra Singh[1], Nitin Rathore[2]
[1]M.E. Pursuing, Indore Institute of Science and Technology, Indore, M.P, India
[2]Assistant Professor, Indore Institute of Science and Technology, Indore, M.P, India
Department of Computer Science & Engineering.

Abstract- The information and data security concerns still need to network security and confidentiality fully addressed. Cloud allows customers to avoid hardware and software, flexibility, and investment cooperation with others, and to take advantage of sophisticated services.. In this paper, we consider a scenario where two servers cooperate to authenticate a client and if one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server. The proposed work continues the line of research on the two-server paradigm in, extend the model by imposing different levels of trust upon the two servers, and adopt a very different method at the technical level in the protocol design. The proposed scheme is a password-only system in the sense that it requires no public key cryptosystem and, no PKI. The paper work, generalize the basic two-server model to architecture of a single back-end server supporting multiple frontend servers and envision interesting applications in federated enterprises.

Keywords- Cloud computing security, Data security, Open Key Framework (PKI), Kerberos as an administration, Administration Level Assertion (SLA).

I. INTRODUCTION

Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture, as shown in fig.. The services offered through cloud computing usually include IT services referred as to SaaS (Software-as-a-Service) which is shown on top of the stack. SaaS allows users to run applications remotely from the cloud[1][2].

Infrastructure-as-a-Service (IaaS) refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access.

The data-Storage-as-a-service (dSaaS) provides storage that the consumer is used including bandwidth requirements for the storage.

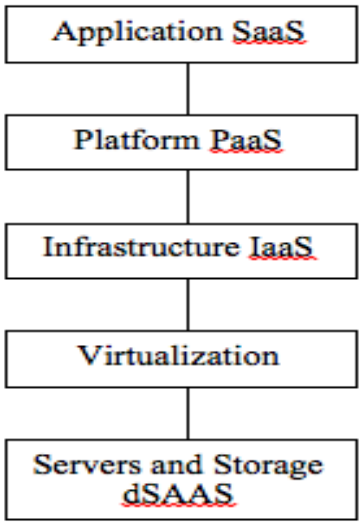
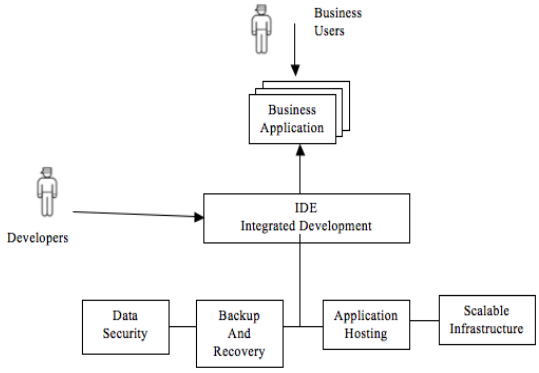


Fig.1: Layered architecture of cloud computing

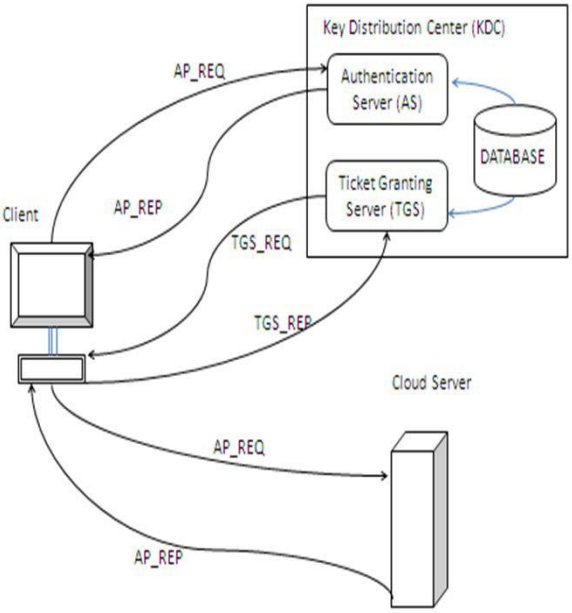
An example of platform-as-aService (Paas) cloud computing is shown in fig. the PaaS provides integrated development environment (IDE) including data security[3], backup and recovery, application hosting and scalable architecture.



.

Fig.2: The concept of Platform-as-a-Service.

Figure 2 illustrates another types of cloud service, where the application runs on the client; however it accesses useful function and services provided in the cloud. An example of this type of cloud services on the desktop is apple's iTunes[4][5].



.

Fig.3: Kerberos authentication System

II. RELATED WORK

This is matter of fact that in any research activity the exploration and deep study of existing approaches plays a significant role, therefore consideration this factor in mind the author of this thesis has performed a deep rooted survey for the role based access control mechanism and specially the access control approaches to be employed for cloud environment [4]. The study made on existing systems provides the well-defined and crisp knowledge about the strength as well as the weakness of the existing approaches and thus the new optimum system can be built. The literature survey conducted for role based access control and its allied processes has been given in this section, as follows:

Lan Zhou et al [6] addressed trusted administration and enforcement of role-based access control policies on data stored in the cloud. Role-based access control (RBAC) simplifies the management of access control policies by creating two mappings; roles to permissions and clients to roles. Recently crypto-based RBAC (C-RBAC) schemes have been developed which combine cryptographic techniques and access control to secured data in an outsourced environment [7]. In such schemes, data is encrypted before outsourcing it and the cipher text data is stored in the untrusted cloud. Those clients who satisfy the role-based access control policies can only decrypt this cipher text. However such schemes assume the existence of a trusted administrator managing all the clients and roles in the system. Such an assumption is not realistic in large-scale systems as it is impractical for a single administrator to manage the entire system.

Though administrative models for RBAC systems have been proposed decentralize the administration tasks associated with the roles, these administrative models cannot be used in the C RBAC schemes, as the administrative policies cannot be enforced in an untrusted distributed cloud environment.

In this paper, the researchers proposed a trusted administrative model ADC-RBAC to manage and enforce role-based access policies for C-RBAC schemes in large-scale cloud systems. The ADC-RBAC model uses cryptographic techniques to ensure that the administrative tasks such as client, permission and role management are performed only by authorized administrative roles. Their proposed model uses role based encryption techniques to ensure that only administrators who have the permissions to manage a role can add/revoke clients to/from the role and owner- can verify that a role is created by qualified administrators before giving out their data. We show how the proposed model can be used in an untrusted cloud while guaranteeing its security using cryptographic and trusted access control enforcement techniques [8][9].

III. EXISTING SYSTEM

A. Diffie-Hellman

Diffie-Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. To implement Diffie- Hellman [3], the two end users Alice and Bob, at the same time as communicating under a channel they mutually agree on two positive whole numbers q and g, such that q is a prime number and g is a generator of q. The generator g is a number to facilitate, when raised to constructive whole-number powers less than q, never produces the same result for any two such whole numbers. The value of q may be large but the value of g is usually small. DiffieHellman key exchange (DH)[nb 1] is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The DiffieHellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

B. ElGamal Encryption Scheme

Alice				*Bob*		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		p, g			b
a	p, g, A	$g^a \bmod p = A$	A		p, g	b
a	p, g, A		B	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, s

In cryptography, the ElGamal encryption system [6] is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It was described by TaherElgamal in 1984. It consists of key creation encryption, and decryption all the steps (Algorithms) as followsKey generation:-
The key generator works as follows:

1. Alice generates an efficient description of a multiplicative cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
2. Alice chooses a random x from 1, , q-1.
3. Alice computes
   $h = g^x$:
   Eqn(2.5)
4. Alice publishes h, along with the description of G,q,g as her public key. Alice retains x as her private key which must be kept secret.

C. Encryption:-

The following is the encryption algorithm to encrypt a message m to Alice under her public key (G, g, q, h)

1. Bob chooses a random y from 1, , q-1, then calculates
   $c1 = gy$
   Eqn (2.6)
2. Bob calculates the shared secret
   $s = hy$
   Eqn (2.7)
3. Bob converts his secret message into an element m of G.
4. Bob calculates
   $c2 = m0 :s$
   Eqn (2.8)
5. Bob sends the cipher text
   $(c1; c2) = (gy; m0 ; (gx)y)$
   Eqn (2.9)
   to Alice.

D. Decryption:-

The following is the decryption algorithm to decrypt a cipher text (c1,c2) with her private key x

1. Alice calculates the shared secret
   $s = c1x$
   Eqn (2.10)
2. And then computes
   $m0 = c2:s(1)$
   Eqn (2.11)
   which she then converts back into the plain text message m, where 1 inverse of sin the group G.

The decryption algorithm produces the intended communication, since

$c2:s(1) = m0 :hy:(gxy)(1) = m0 :gxy:g(xy) = m0 :$

Eqn (2.12)

ElGamal encryption scheme is a probabilistic encryption system. If encrypting the similar message using ElGamal encryption technique several times, it will, in general, yield different cipher texts. Tsiounis and Yung proved ElGamal encryption scheme to be semantically secure under the DDH assumption.

IV. PROPOSED SYSTEM

Our security analysis focuses on the adversary model as defined. We also evaluate the efficiency of our scheme via implementation of both file distribution preparation and verification token precipitation. In our scheme, servers are required to operate on specified rows in each correctness, verification for the calculation of requested token. We will show that this "sampling" strategy on selected rows instead of all can greatly reduce the computational overhead on the server, while maintaining the detection of the data corruption with high probability. Suppose servers are misbehaving due to the possible compromise or Byzantine failure.

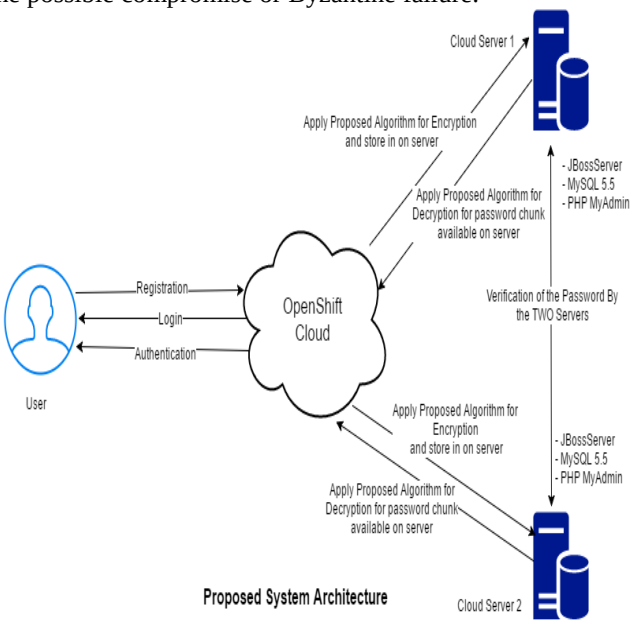


Fig.2: Proposed System

V. RESULT ANALYSIS

Proposed System has been implemented with the help of public cloud (Red hat-Open Shift).Following step we performed for create cloud:

- Create account on open shift
- Create an application using Openshift Dashboard. Application include
- JBOSS application Server
- MYSQL 5.5 Database Server
- Php my admin 4.0
- Mapping this Application with Eclipse (Kepler)

- After Mapping we perform all the functionality of proposed system
- Encryption
- Password Fragmentation,
- Managing Index
- SHA

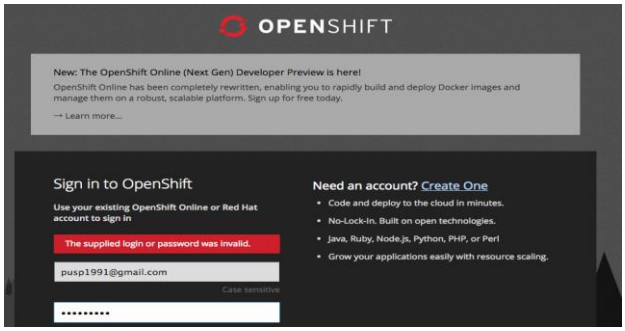


Fig.3: Openshift cloud Dashboard

Figure 3 describe application details of cloud which is created by us. Reaming functionality perform using language JAVA/JSP/Servlet.

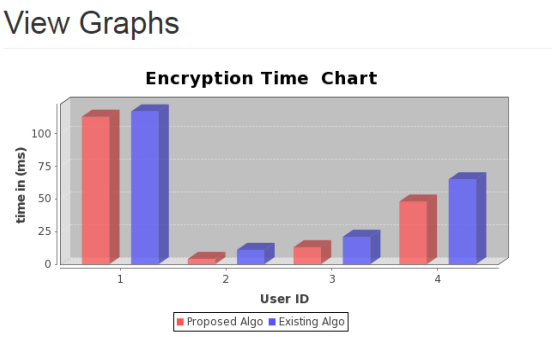


Fig.4: Encryption time chart for proposed and existing Algorithm

In Above Figure 4 shown graph which compare existing and proposed algorithm comparison through time . it show that proposed algorithm taken less time compare to existing Algorithm

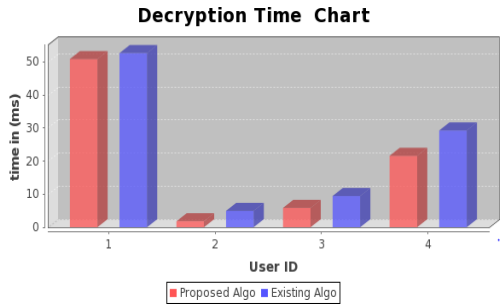


Fig.5: Decryption time chart for proposed and existing Algorithm

In Above Figure 5 shown graph which compare existing and proposed algorithm comparison through time it show that proposed algorithm taken less time compare to existing Algorithm

VI. CONCLUSION

In this system, we have accessible a symmetric protocol for two-server password-only authentication and key exchange.Security analysis has shown that our protocol is secure against passive and active attacks just in case that one between the two servers is compromised. Performance analysis has shown that our protocol is a lot of economical than existing system.

For the future enhancement any one can implement the projected system with private cloud. The proposed system sometime affect when any single server has gone in downlink. So, the cloud server will provide assurance both server will available on each transaction.

These rules out the utilization of Kerberos as a single sign-on framework for distributed applications that may reside in the internet or the cloud. Furthermore, Kerberos relies solely on unproven symmetric encryption mechanisms to authenticate users and maintain session state. It may also be possible to impersonate users and steal authentication tickets through simple network based attacks.

VII. REFERENCES

[1]. Sweta Jain* and DrVineetRichhariya "Kerberos based Enhanced Authentication Protocol for Cloud Computing Environment" International Journal of Theoretical & Applied Sciences, 9(2): 25-30(2017)

[2]. YaserFuad Al-Dubai & Dr. Khamitkar S. D, "Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control", Global Journals Inc. 2014.

[3]. YaserFuad Al-Dubai and Dr. Khamitkar S.D, "A Proposed Model For Data Storage Security In Cloudcomputing Using Kerberos Authentication Service", ISSN 0976 – 6367(Print) ISSN 0976 – 6375(Online) Volume 4, Issue 6, November - December (2013), pp. 62-69.

[4]. ANIESH KRISHNA K, BALAGOPALAN A S, "Authentication Model For Cloud Computing Usingsingle Sign-On", Proceedings of 10th IRF International Conference, 04th October-2014, Bengaluru, India, ISBN: 978-93-84209-56-8.

[5]. Raja Shree S., "Secure Substantiation in Cloud Computing Environment",International Journal of Modern Engineering Research (IJMER) 2014.

[6]. Abhishek P, Mayank Kumar, **"**A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module **",**Volume 3, Issue 4, April 2013.

[7]. Mehdi Hojabri, "Ensuring data storage security in cloud computing with effect of Kerberos", International Journal of Engineering Research & Technology (IJERT) 2012.

[8]. Y. ShashankRao, Dr. N. Chandra Sekhar Reddy, **"**Kerberos as a Service in Cloud Computing Security Issues", International Journal of Science and Research (IJSR) 2014.

[9]. Er.Abhijeet, Mr. Praveen Tripathi, Er.AnujaPriyam and Er.Vivek Kumar, "Implementation of Public Key Cryptography in Kerberos with Prevention of Security Attacks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 248 - 253, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[10]. SujayPawar and Prof. Mrs. U. M. Patil, "A Survey on Secured Data Outsourcing in Cloud Computing", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 70 - 76, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[11]. AbhishekPandey, R.M.Tugnayat and A.K.Tiwari, "Data Security Framework for Cloud Computing Networks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, pp. 178 - 181, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[12]. A.Madhuri and T.V.Nagaraju, "Reliable Security in Cloud Computing Environment" International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 2, 2013, pp. 23 - 30, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.