Cloud Computing With Two Factor Authentication for Government Information System and Security

Hardayal Singh Shekhawat
Associate Professor (IT), Govt. Engineering College, Bikaner, (India)
Research Scholar: Suresh Gyan Vihar University, Jaipur (India)
shekhawat.hardayal@gmail.com

***Abstract*— Cloud computing refers to the technology which delivers on demand access to application software's, development platform and infrastructure, over the internet offers attractive advantages to the government. Due to benefits like low cost, increased flexibility, elastic scalability and pay-per-use, public sector is planning to adopt Cloud Computing. However privacy and authentication is the big challenge before the government to adopt cloud computing. In order to address these privacy and authentication issues this paper presents two factor authentication model in cloud computing for government information system and security. This paper introduces hybrid cloud model with strong two factor authentication system where critical government data, which will be available to the authenticated users, will be saved in private cloud and general data will be saved in the public cloud to make available to general people. Finally the model proposed in this paper enables government to apply necessary privacy and authentication security to government information system.**

***Keywords*— Cloud Computing, Hybrid Cloud, Two-Factor, Authentication, Government Information System, Security.**

I. INTRODUCTION

Cloud computing has become nedd of the public sector due to its various advantages. The United States federal government has the largest annual IT budget of any organization, almost $80 billion in 2010 alone. To save money and improve services, the government is beginning to adopt a *cloud first* approach towards procuring new and replacement systems [1]. The benefits for moving into the cloud are the same for the government as they are for private firms, but challenges are much bigger. The biggest challenge is authentication and access control. Authentication aspect of cloud computing points towards identity federation and authentication to facilitate transection between cloud provider and user. Threat of accessing critical data by un autherised user is not only from the intruders but also from malicious employees of the government. In this research paper efforts have been made to analyze the use of hybrid cloud computing model with two factor authentication security for government information system.

The remainder of this paper is organized as follows. Section 2 describes the review of literature. Section 3 discusses cloud computing models. Section 4 addresses cloud computing authentication issues. Section 5 proposes our two factor authentication cloud model for government information system**.** Section 6 concludes our paper with summary.

II. REVIEW OF LITRETURE

Governments all around the world are implementing cloud computing [2] for core functions of their IT infrastructure [3]. Cloud computing delivering infrastructure, platform and software applications on demand via network offers attractive advantages to the public sector [4]. Cloud computing provides a great opportunity for governments across the globe, to provide reliable e-governance with the features like low Infrastructure cost [5], pay-as-you-go, high availability and dynamic scalability [6,7].

Governments (organizations) are adopting hybrid cloud environments where they will combine the advantages of a public cloud with an internal private cloud [8, 9]. Organization builds a private cloud solution to handle high sensitivity applications but also use public cloud solution to surge, support low sensitivity applications [10]. Japanese central government has decided to use hybrid cloud for their local governments where internal task and some data will be hosted on the private cloud [11] and rest on the public cloud. Most of the concern with the cloud computing are related to security and privacy of the data [12]. A hybrid approach combines access to the public cloud that adds to or replace existing state infrastructure with private cloud services meeting specialized access and security requirements [13].

Security aspect of cloud includes authorization, authentication and access control [14]. User authentication is often the primary basis for access control [15]. Two factor authentication is an important, strong and effective solution for real problems [16].

III. CLOUD COMPUTING

Cloud Computing is computing paradigm, where a large pool of systems is connected in public or private network, to provide dynamically scalable infrastructure for application, data and file storage. With the advantages of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly [17].

A. Public Cloud

Public Clouds are owned and operated by third party and services are made available to clients through internet. Data on Public Cloud are not publicly visible, service provider typically provide an access control mechanism for their users. Public cloud provides elastic, cost effective pay-per-use means to deploy solution.

B. Private Cloud

Private Clouds are exclusively built for a single enterprise. Private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

C. Hybrid Cloud

A hybrid cloud combines both public and private cloud. The pay-per-use model of public clouds attracts various government organizations, which reduced cost and development time, but the public nature of cloud as a big issue for adoption. To handle the challenges of public cloud and use the advantages of private cloud a hybrid approach can be used. In this model users typically outsource non critical information and processing to the public cloud, while keeping critical services and data in their control in private cloud. The success of this hybrid approach depends on how public and private cloud interacts and works together in union.

IV. AUTHENTICATION

The process of verifying a user's identity is typically referred to as user's identification and authentication. Password are the methods used most often for authenticating computer users but this approach has often proven inadequate in preventing unauthorized computer resources when used as the sole means of authentication [18] .

Existing authentication methodologies involve three basic factors.

- Something the user knows (e.g. Password, PIN)
- Something the user has (e.g. ATM Card, smart card)
- Something the user is (e.g. biometrics characteristics, such as fingerprints) [19]

A. Single Factor Authentication

The most basic form of single factor authentication is user ID and Password combination. Where user claims its identity by presenting a user ID and a secret password known only to the user and authentication system. Authentication system checks the claimed password for claimed ID with its secure list of user ID and Passwords. If the user ID and password presented by the user matches with the user ID and password stored with the authentication system then user considered as the authenticated user and given access. This type of authentication system is extremely weak. This authentication system is inadequate for high risk transaction like government information system and banking system.

B. Two Factor Authentication

Tow factor authentication method uses two separate form of identification out of three basic forms, something the user knows or something the user has, or Something the user is. Two factor authentication method is stronger then the single factor authentication method.

A good example of two factor authentication used in our daily lives is an ATM cash machine. In order to withdraw cash from ATM machine you must first insert your credit card (Something you have) and then enter your pin (something you know)[20] . By using something a user knows with something a user has the same level of authentication can be brought to the online world.

V. PROPOSED TWO FACTOR AUTHENTICATION CLOUD MODEL FOR GOVERNMENT INFORMATION SYSTEM

Figure 1 shows the proposed model of hybrid Cloud Computing with two factor authentication for e-governance. This model discusses basic security points that should be considered while using hybrid cloud model with two factor authentication for government information system and security.

A. Two factors of Authentication

This model introduces two factor authentication systems, where we use tow factors to identify authorized user to access government information system. First factor proposes, something the user knows (User ID and Password) method and second factor proposes something the user is (fingerprints) method. The advantage of using this model is user need not to carry any hardware device or card which is necessary in case of, something the user has (e.g. ATM Card, smart card) factor of the authentication. This two factor authentication is stronger then traditional password authentication [21].

B. Encryption

Encryption is the most important part of the cloud for e-governance information and security. Encryption on the data can be used at various places [22], For example, data in transit, data at rest and data in memory or process. Encrypting and managing encryption keys of data in transit to the cloud or at rest in the service provider's data centre are critical to protect data privacy and comply with compliance mandates [23]. In our model user will need to enter his User ID, Password and Finger print in the options available on the user browser. This user information will be encrypted before sending it to the Authenticator of cloud, over the internet.

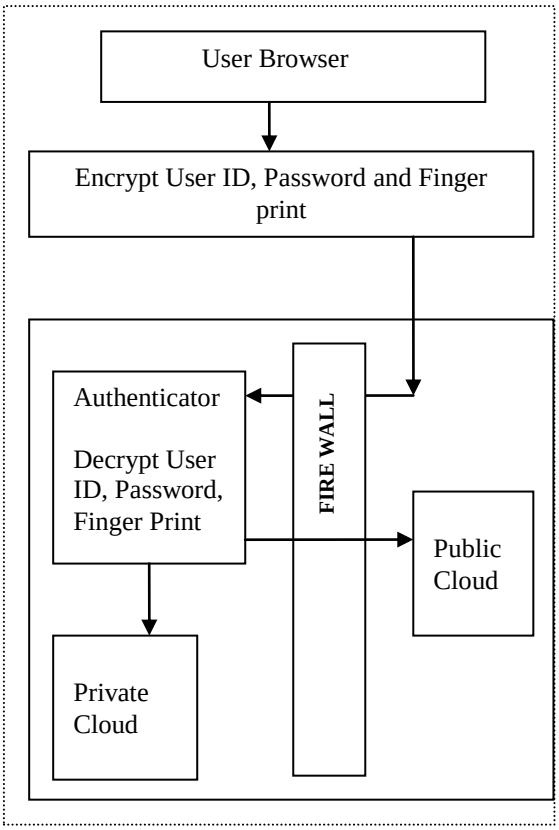

Fig 1. Hybrid cloud model with two factor authentication for e-governance

C. Hybrid Cloud

This model uses hybrid cloud to store government data and information. Where critical government information and data will be stored in private cloud and general information for citizens will be available on public cloud. By using hybrid cloud, advantages of both private and public cloud can be taken. Private cloud has high security and public cloud has other advantages like pay-per-use.

D. Firewall

Authenticator and private cloud of our model is firewall protected. The level of security afforded by the firewall is a function of which ports are opened by the customer and for what duration and purpose. The default state is to de deny all coming traffic, and developer should plan carefully what they will open when building and securing their applications [24].

E. Authenticator

Authenticator is the system which is responsible to authenticate the user on the basis of identity supplied by the user. The encrypted information which is supplied by user will be decrypted before using. Authentication system then checks the claimed password for claimed ID and finger prints with its secure list of user ID, Passwords and finger prints. If they matches with the user ID, password and finger print stored with the authentication system then user considered as the authenticated user and given access to use the cloud for government information stored on them.

Users Authenticated for private cloud, like government officers or administrators will be given access to the private cloud and rest will be sent to public cloud.

F. Private cloud

Data privacy and security related challenges cannot be ignored for a large category of the business scenario where customer information and business critical intelligence is involved [25].

By building private enterprise cloud, government can keep the sensitive data within their control and can use the existing infrastructure effectively.

G. Public cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model [26]. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider.

VI. CONCLUSION

Single factor authentication is inadequate for government information and security. This paper has introduced tow factor authentication system. Two factors suggested in this paper are, something the user knows (User ID and Password) and something the user is (fingerprints). Two factor authentication method is strong and adequate for government information system. With two factor authentication, hybrid cloud computing method is used to store government data and information. The hybrid approach uses private cloud to store critical information and public cloud to store less sensitive information for government information system. Two factor authentication system and hybrid cloud model will provide government with a simple, cost-effective and strong authentication way to provision IT services, irrespective of where the services are hosted or provisioned.

REFERENCES

[1] Cloud computing by government agencies, http://www.ibm.com/developerworks/industry/library/ind-govcloud/
[2] David C. Wyld , The cloudy future of the Government IT : Cloud Computing and The Public Sector Around The World. http://airccse.org/journal/ijwest/papers/0101w1.pdf
[3] Lockheed Martin, Awareness Trust and Security to shape government cloud adoption.

www.lockheedmartin.com/data/assets/isgs/documents/CloudComputing WhitePaper.pdf
[4] Russell Craig, Jeff Frazier, Cloud Computing in Public Sector. http://www.cisco.com/web/about/ac79/docs/wp/ps/Cloud_Computing_112309_FINAL.pdf
[5] Juniper Networks, Identity Fedration in Hybrid Cloud Computing Environment. http://www.juniper.net/us/en/local/pdf/implementation-guides/8010035-en.pdf
[6] Prem Jadhwani, John Mackinnon, Cloud Computing Building a Framework for Successful Transition. http://www.gtsi.com/cms/documents/White-Papers/Cloud-Computing.pdf
[7] Reddy Raja A, Vasudeva Verma, Cloud and E-Governance. www.imaginea.com/docs/Whitepaper-Cloud-egovernance.pdf
[8] Lorraine M. Campos, Stephania E. Giese, Joelle E.K. Laszlo, Transcending The Cloud. http://www.reedsmith.com/_db/_documents/Cloud_Computing_Government_Contracting.pdf
[9] Torry Harris, Cloud Computing – An Overview. http://www.thbs.com/pdfs/THBS-Cloud%20Computing%20final.pdf
[10] Ted Alford, Gwen Morton, The Economics of Cloud Computing. www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf
[11] Cloud Computing Use case Discussion Group, Cloud Computing Use case White Paper Version 2.0. www.opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-2_0.pdf
[12] Duncan Goss, David Tucker, Cloud Computing in Vermont State Government. www.leg.state.vt.us/reports/2010ExternalReports/251891.pdf
[13] Vivek Kundra, State of Public Sector Cloud Computing, www.cio.gov/documents/StateOfCloudComputingReport-FINALv3_508.pdf
[14] Sunil Tadwalkar , Cloud Computing – Still a long way to go. http://www.mahindrasatyam.com/corporate/documents/Cloud_Computing.pdf
[15] Trusted Computing Grup. http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf
[16] GPayments Pty Ltd. http://www.gpayments.com/pdfs/WHITEPAPER_2FA-Fighting_Internet_Fraud.pdf
[17]Torry Harris, www.thbs.com/pdfs/Cloud-Computing-Overview.pdf
[18]NIST Computer Security Handbook, http://www.sos.cs.ru.nl/applications/courses/security2008/nistiadraft.pdf
[19] Authentication in an internet Banking Environment. http://www.ffiec.gov/pdf/authentication_guidance.pdf
[20]Andrew Kemshall, Phil Underwood, Options for Two Factor Authentication. http://www.securenvoy.com/WhitePapers/white_paper_two_factor_authentication.pdf
[21] It Solutions, Inc http://www.itshsv.com/pdf/TwoFactorAuthenticationPDF.pdf
[22]Cloud computing information assurance framework, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework.pdf
[23]IBM Point of View: Security and Cloud Computing, ftp://public.dhe.ibm.com/common/ssi/sa/wh/n/tiw14045usen/TIW14045USEN_HR.PDF
[24] Amazon web services : Overview of security process. http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf
[25] Realizing value proposition of cloud computing. http://www.infosys.com/cloud-computing/white-papers/documents/realizing-value-proposition.pdf
[26] CLOUD COMPUTING – An Overview http://www.thbs.com/pdfs/Cloud-Computing-Overview.pdf