Cloud Computing Security: An Enhanced Authentication Mechanism

Amar Nath Bhargava[1], Neha Bhardwaj[2]
[1, 2] Madhav Institute of Technology and Science, Gwalior, MP

Abstract- *Cloud computing holds the possibility to dispose of the necessities for setting up of high-cost computing infrastructure for IT-based arrangements and services that the industry uses. It guarantees to give an adaptable IT architecture, open through internet from lightweight portable devices. This would permit multi-fold increment in the limit and abilities of the current and new software. In a cloud computing environment, the entire data dwells over an arrangement of networked resources, empowering the data to be gotten to through virtual machines. Following these data-centres might be situated in any part of the world past the span and control of users, there are multifarious security and protection challenges that should be comprehended and tended to. Likewise, one can never prevent the likelihood from securing a server breakdown that has been seen, rather regularly in the late times. There are different issues that should be tended to concerning security and privacy in a cloud computing environment. This broad survey paper expects to expand and break down the various uncertain issues debilitating the cloud computing reception and dissemination influencing the various stake-holders associated with it.*

Keywords- Authentication, Cloud, Security.

I. INTRODUCTION

Cloud computing is one of the revolutionary technologies that is expected to dominate and reshape the information technology industry in the near future. This emerging computing technology provides highly scalable computing resources (e.g. information, applications, and transactions) in a way that is accessible, flexible, on-demand, and at a low cost it provides unique opportunities for organizations to run business with efficacy and efficiency by allowing businesses to run their applications on a shared data center thus eliminating the need for servers, storage, processing power, upgrades, and technical teams. Furthermore; in cloud computing model, business organizations do not need to purchase any software products or services to run business because they can simply subscribe to the applications in the cloud; those applications normally are scalable and reliable and ultimately allow business leaders to focus on their core business functions to enhance performance and increase profitability. Many organizations have become interested in the cloud computing concept due to many compelling benefits presented by this emerging computing paradigm. Cloud computing vendors are offering scalable services and applications via centralized data centers utilizing thousands of server computers which provide easy access to computing resources anytime and anywhere; the capability of cloud computing to quickly scale and provide access to computing services and resources anytime and anywhere, allowing organizations to quickly respond to changing business needs without the expenditures of time, space, money, personnel, and other resources needed for traditional infrastructures for example, New York newspaper organization were able to convert 11 million scanned and archived hard copies into portable document format (PDF) files in 24 hours by renting 100 servers from Amazon's cloud services at a cost to the organization was approximately $250. Alternative methods for the conversion would have required cost and taken weeks or even months to complete [3].while cloud computing offers enormous potential for reducing costs and increasing an organization's ability to quickly scale computing resources to respond to changing needs, there are risks associated with cloud computing. Specifically, cloud computing may mean that an organization relinquishes control, resulting in exposure to breaches in confidentiality, losses in data integrity and availability. However; as with any technology, cloud computing has its own disadvantage such as releasing control of maintaining confidentiality, integrity, and availability of sensitive business data; In general, most cloud computing consumers want to be assured that cloud providers have effective security policies and controls in place to comply with data protection standards and meet regulatory compliance requirements prior to making a decision to migrate their data or applications to the cloud.[1]

A. Privacy Preserving in Cloud

Privacy issues exist for a long time in the computing literature. Data storage in the Cloud Computing system which is located in multi regions to make the system more tolerant may also raise the privacy problems. Such research contributions are given below.

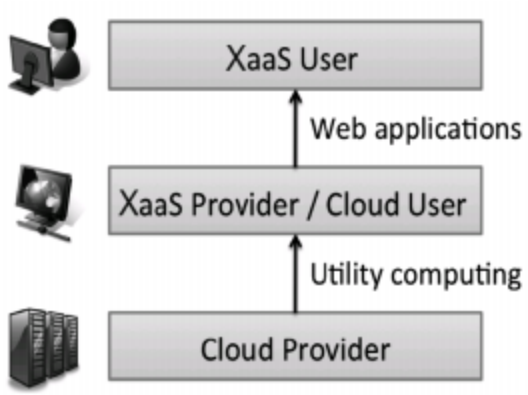

Fig. 1 Users and Providers of Cloud Computing

B. Security and Privacy in Cloud

This paper [1] discusses the flaws that occurred in famous Google docs, salesforce.com, epic.com due to cloud security lack. Cloud computing is secure if users can depend on them to behave as users expect, satisfying 5 goals, say availability, confidentiality, data integrity, control and audit.

The relationship between the users and providers in cloud computing system is discussed in terms of 3 roles say Cloud provider, Xaas provider/Cloud user and Xaas user as shown in Figure 1, where X could be D (Data), S (Software). P (Platform), I (Infrastructure), and so on depicted in Figure 1.[2]

II. PRACTICES FOR CLOUD SECURITY

A. Secure access

Usually users access the cloud using client web browser. Make sure browsers are properly updated and protected from browser exploits. By using this, data can be prevented from threat to some extent.

B. Backups and restoration

There should be proper mechanism provided by the service provider so that customer is able to have backups of the cloud based resources and data. Some services like Amazon S3, Amazon Dynamo DB provide automatic data restoration.

C. Data Integrity

To ensure data integrity, limits the area of use of resources for users. This can prevent the modification of data and hence data integrity is maintained. In case data integrity is enforced restore the data from backup with the help of backup services provided.

D. Encryption of data

Data encryption provides protection to the data. Encryption should be done before the data is moved to the cloud [4]. If an unwanted user wants to access the critical data, encrypting the data makes it much more difficult for unwanted user to do anything with wrong inception.

E. Evaluation

Evaluate applications, business processes and data according to their value and risk associated with them then create cloud with precautions and tools to make the cloud[3]

III. CLOUD SECURITY CATEGORIES AND ISSUES

Table 1: Cloud Security categories

NO	Category	Description
1	Security Standards	Defines the standards needed to take precautionary measures in the cloud computing so as to prevent attacks. It directs the policies of cloud computing for security without compromising reliability and performance.
2	Network	Consist of network attacks such as Denial of Service (DoS), Connection Availability, internet protocol vulnerabilities, DoS, flooding attack, *etc.*
3	Access Control	Access control and Authentication and. It captures the issues that affect the privacy of user information and data storage.
4	Cloud Infrastructure	Attacks that are strict to the cloud infrastructure (IaaS, PaaS and SaaS) such privileged insiders and tampered binaries
5	Data	Data related security issues, including integrity, data migration, confidentiality, and data warehousing.

Table 2: Cloud Security Issues and Classifications

NO	Category	Issues
1	Security Standards	Absence of legal aspects (Service level agreement) Absence of security standards Compliance risks

		Trust Absence of auditing
2	Network	Network security configurations Appropriate installation of network firewalls Internet Dependence Internet protocol vulnerabilities
3	Access	Malicious insiders Service and Account and hijacking Privileged user access Browser Security Authentication mechanism
4	Cloud Infrastructure	Quality of service (QoS) Sharing technical flaws Insecure interface of API Multi-tenancy Reliability of Providers Server Location and Backup Security Misconfiguration
5	Data	Data location Data loss and leakage Data redundancy Data privacy Data protection Data recovery Data availability

IV. LITERATURE REVIEW

According to Arun et al. [5] the privacy issues in the cloud environment are handled and assessed by using privacy protocols and assessment techniques which are also addressed. The trust issues in cloud computing has been addressed with different models. An inter-cloud and intra-cloud standard of cloud interoperability has been identified in order to highlight the challenges exist during the cloud interaction. The cloud resources are deployed over cloud environment with different models also faces a problem. This paper focuses on a recent survey related to the cloud interoperability, security, privacy and trust based on standards and guidelines have been analyzed. The overall focus on this paper is to establish an interoperability among different cloud service providers for effective interaction by maximizing the QoS of cloud computing.

The research by Sharma et al. [6] proposes a new model by extending the Technology Acceptance Model (TAM) with three external constructs namely computer self-efficacy, trust, and job opportunity. One of the main contributions of this research is the introduction of a new construct, Job Opportunity (JO), for the first time in a technology adoption study. Data were collected from 101 IT professional and analyzed using multiple linear regression (MLR) and neural network (NN) modeling. Based on the RMSE values from the results of these models NN models were found to outperform the MLR model.

The large data centers emit carbon-dioxide which leads to global warming. So to address both of these issues, Gill et al. [7] have proposed a framework which tackles with security and is energy efficient. Signature and anomaly based hybrid IDPS detects, logs, prevent and alert the security Admin. The Nesting of the VMs provide easy management and IDPS can deal better as the grouping of VMs has been done on the basis of security protocols. In this paper, a comprehensive survey on existing cloud security frameworks has been done. Based upon the limitations on existing frameworks a new framework has been proposed to provide security in virtual networks that is based on Intrusion Detection and Prevention System (IDPS) and its prototype implementation has also been done.

In their paper, Khan et al. [8] present a survey of security issues in terms of security threats and their remediation. The contribution aims at the analysis and categorization of working mechanisms of the main security issues and the possible solutions that exist in the literature. We perform a parametric comparison of the threats being faced by cloud platforms. Moreover, we compare various intrusion detection and prevention frameworks being used to address security issues. The trusted cloud computing and mechanisms for regulating security compliance among cloud service providers are also analyzed. Since the security mechanisms continue to evolve, we also present the future orientation of cloud security issues and their possible countermeasures.

According to Krishna et al. [9] Cloud computing has a probable scope for cost savings to the enterprises but the security risk are also gigantic. Enterprise considering into cloud computing technology as a tactic to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. The asset of cloud computing in information risk management is the facility to manage risk more effectively from a integrate point. Although Cloud computing can be seen as a new marvel which is set to reform the way we use the Internet, there is much to be thoughtful about. There are many new technologies emerging at an express rate, each with technological developments and with the potential of making human's lives at ease.

Piplode et al. [10] discuss about the cloud computing security issues and challenges. This paper also analyze cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of a Cloud computing require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these

networks. The future of cloud computing is really appealing, giving the vision of cheap communications.

V. PROPOSED WORK

First the methodology that has been proposed for enhancing the authentication process in cloud environment proceeds in the following steps:

1. The home page shows various menus such as Register, Login here, About us and Contact us on the left side of the window.

Fig. 2 Home Page

2. After selecting Registration in the menu bar, the Registration form will open. Registration form has several fields such as Name, Password, and Confirm Password.

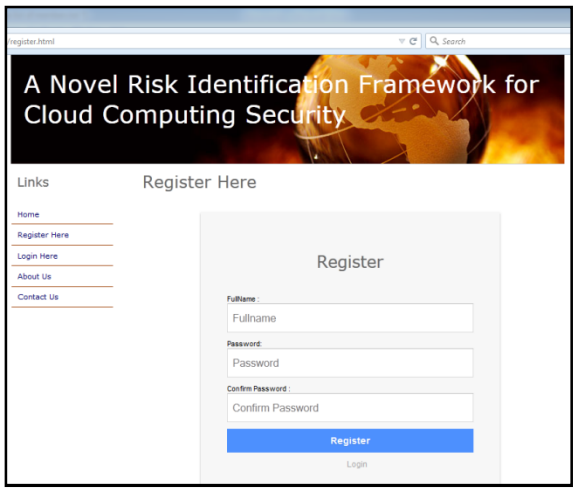

Fig.3 Home Page for User Registration

After filling the above details and clicking submit, a unique user id is generated and the user is required to enter the frontal face image.

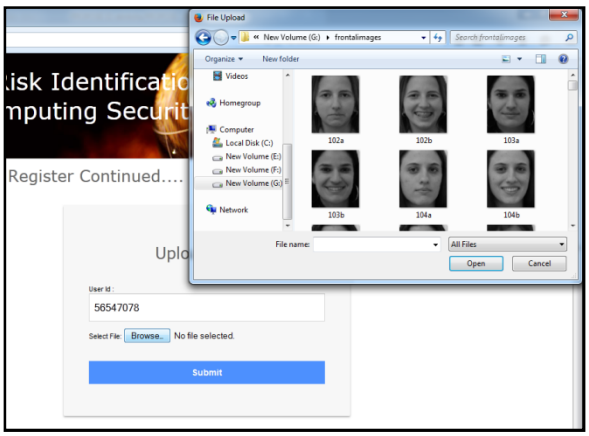

Fig 4. Selection of frontal face image for registration

3. Select Login in menu bar then login form is displayed. In Login form, fill the mentioned fields, i.e. User Id and Password then click submit button. Next, the image verification form opens where the image being provided is matched with the previously uploaded face image. If the image is correct then User Home page opens and now the user can access the cloud services.

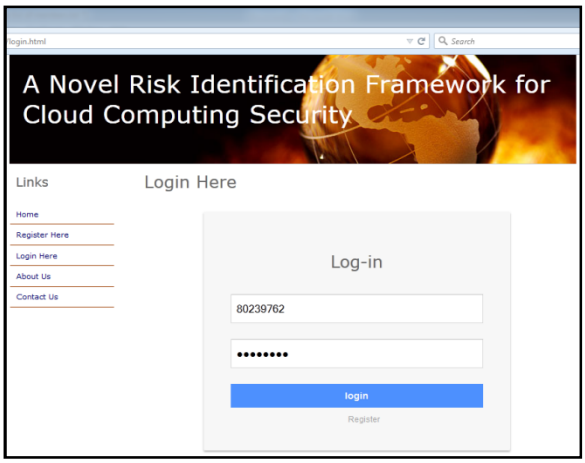

Fig. 5 Login page

4. If you entered correct user id and password, you are proceeded to the face image verification form. Choose the correct image and user home page is opened.

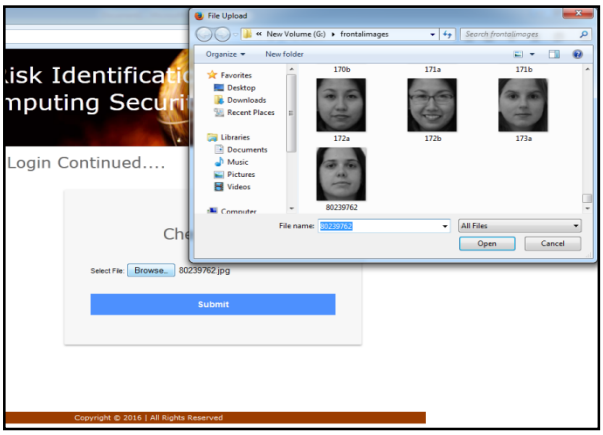

Fig.6 Face image verification

5. Next step is the selection of preferred service. The user can choose the required service among Private, Public or Hybrid Storage.

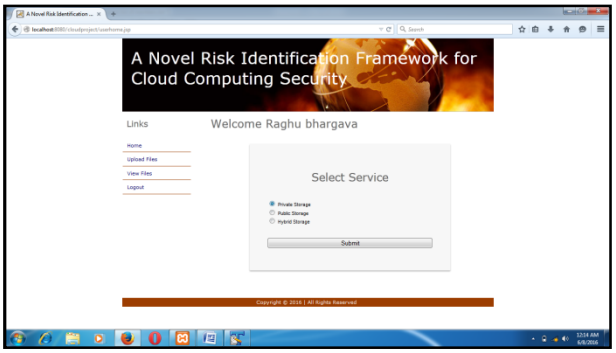

Fig.7 Selection of Service

a) Private Storage

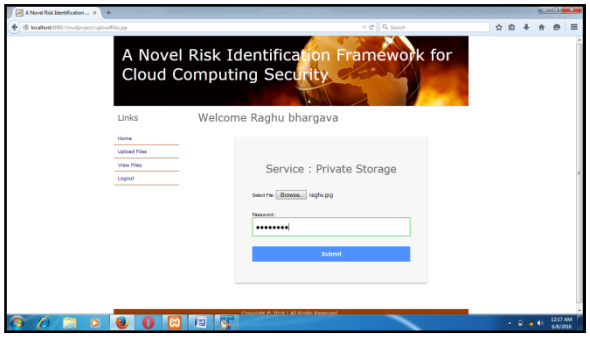

Fig 8. Storing image and providing encryption key

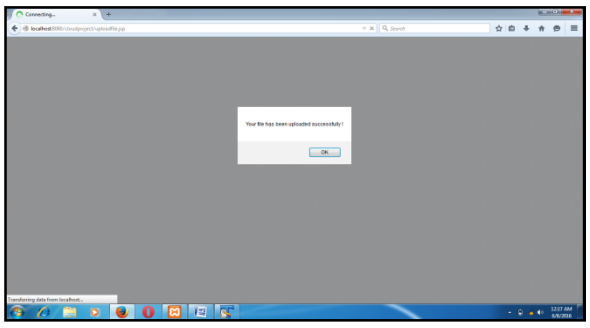

Fig 9. File uploaded and encrypted successfully

Similar procedure is followed while downloading the stored data by providing the same key used for encryption.

b) Hybrid Storage

After following the same procedure for registration and selecting the Hybrid storage service, uploading the data requires the user to enter a security question and its answer which will be used later for retrieval of the stored data.

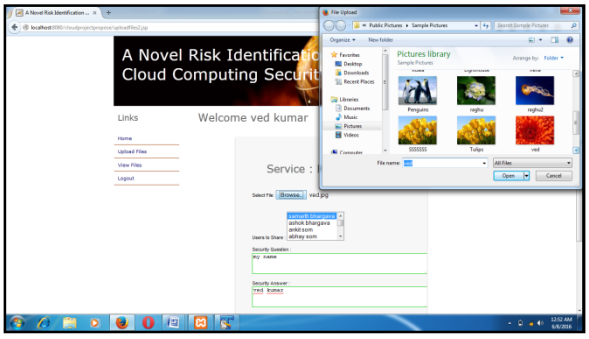

Fig 10. Uploading data in Hybrid Storage

c) Public Storage

The public cloud does not require any specific security measures, since the public cloud does not contain data that might require dedicated security mechanism.

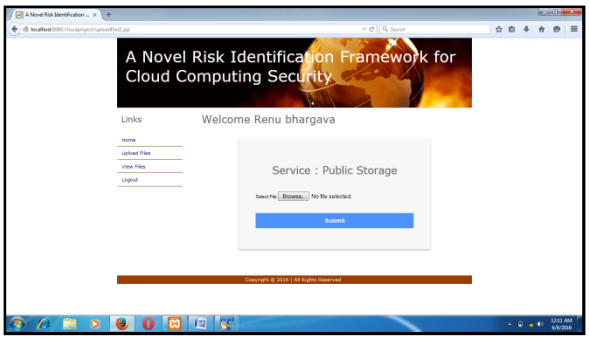

Fig 11. Uploading data in a Public Cloud

VI. CONCLUSION

In this paper base results security web created, in base security web Home Page, Registration Page, Login Page, About Page, and Contact Page. In proposed results same security web created but some page fields are different in Registration Page and Login Page in compare to base web security pages. In base security web- Registration Page have fields like Name, Email, Password, Confirm Password and Submit Button you fill all fields and But in proposed results Registration Page have same all fields but we add new field Choose Palm image it increase authentication in proposed web. In base security web –Login page have fields like Email, Password and Submit button there is no security in base web. But in proposed web, web security increase with the help of palm image verification. In proposed Login Page at first you enter Email and Password click submit button then palm authentication page is shown in window for matching palm image. If palm image is correct then user home page is opened otherwise error message is shown. In this proposed web result increased security with the help of palm image verification.

REFERENCES

[1] Yasir Ahmed Hamza, Marwan Dahar Omar "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing" International Journal of Computational Engineering Research, Vol. 03, Issue 6.

[2] R. Sumithra, Sujni Paul "A Survey Paper on Cloud Computing Security and Outsourcing Data Mining in Cloud Platform" International Journal of Knowledge Management & E-learning, Volume 3, Number 1, January-June 2011, pp. 43-48.

[3] Jasleen Kaur, Anupma Sehrawat, Neha Bishnoi "Survey Paper on Basics of Cloud Computing and Data Security" International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

[4] B. Rex Cyril1, DR. S. Britto Ramesh Kumar2 "Computing Data Security Issues, Challenges, Architecture and Methods- A Survey" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 02 Issue: 04, July-2015.

[5] C. Saravanakumar, and C. Arun "Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing" IEEE-2014.

[6] Sujeet Kumar Sharma, Ali H. Al-Badi, Srikrishna Madhumohan Govindaluri, Mohammed H. Al-Kharusi "Predicting motivators of cloud computing adoption: A developing country perspective" (ELSEVIER-2015).

[7] Komal Singh Gill, Anju Sharma "IDPS based Framework for Security in Green Cloud Computing and Comprehensive Review on Existing Frameworks and Security Issues" IEEE-2015.

[8] Minhaj Ahmad Khan "A survey of security issues for cloud computing" Journal of Network and Computer Applications.

[9] B. Hari Krishnaa, S. Kiranb, G. Muralia, R. Pradeep Kumar Reddy "Security Issues In Service Model Of Cloud Computing Environment" 2016 International Conference on Computational Science, ELSEVIER-2016.

[10] Rajesh Piplode and Umesh Kumar Singh "An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering.

[11] Graham Murray, Independent Consultant - WebMiner.co.uk, Dunfermline, Scotlan "ASP.Net and SAS® - A New Model for Developing Web-based SAS System Applications.