Secured E-Learning System Over Cloud Data Center

[1]Piyushika, [2]Neetesh Gupta
[1,2]Dept. of Computer Science & Engineering, Technocrats Institute of Tech. & Sc., Bhopal, MP, India

Abstract
Cloud computing is facing more and more challenges as it is spreading around the world. Additions of new devices are more threatening for the users of the cloud. Data security is the biggest challenges as it can be compromised or misused by cloud service provider, hackers, or over the network. The major problems are related with authentication, authorization and man in the middle attacks. To cater with high security of data, this work proposes to use a security key mechanism to be provided by authentication server created on the cloud or elsewhere. The users of the cloud will require proper authentication, authorization and security key to use the data from the provider services. This work proposes to apply high security of the data with high performance and provides an online implementation of the same.

Keywords
Cloud Computing; Hybrid Cloud; Security; Authentication Server, Authorization, Server

I. Introduction

"A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers."

Cloud computing is becoming a buzz word in computer industry and everyone is looking to associate in one way or other with this brand new concept. Cloud computing is a very current topic and the term has gained a lot of traction being sported on advertisements all over the Internet from web space hosting providers, through data centers to virtualization software providers [1].

Such complex technology and business models setting entails an extensive research and provides the motivation towards writing this paper. The main goal is to "clear the air on hybrid cloud computing security" and provide an unbiased and independent, albeit critical outlook of the technology.

Special emphasis is put on the critical examination of each strategy as now more than ever in the face of the global economic crisis, companies face higher refinancing and investment costs and as any company thinking about adopting or moving to cloud computing technology would do in practice; short-to-medium term disadvantages of the technology have to be pragmatically and carefully weighted out against any hyped long-term potential efficiency achievements, be it strategic, technical or cost related [1].

In order to understand the vision, goals and strategy behind cloud computing, two key concepts that form its foundations need to be explained first.

- Autonomic Computing
- Utility Computing

A. Hybrid Cloud Computing

A hybrid cloud is a composition of at least one private cloud and at least one public cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms.

B. Challenges in Hybrid Cloud Computing

Here are some challenges to consider when setting up hybrid clouds:

1. on Demand Startup and Shutdown:
2. Cloud-based Node Discovery
3. One-Directional Communication
4. Latency
5. Reliability and Atomicity

C. Creating a Cloud and Applying in Industry

From small start-ups to major corporations, companies of all sizes have embraced cloud computing for the scalability, reliability, and cost benefits it can provide. It has even been said that cloud computing may have a greater effect on our lives than the PC and dot-com revolutions combined [3].

Filled with comparative charts and decision trees, Implementing and Developing Cloud Computing Applications explains exactly what it takes to build robust and highly scalable cloud computing applications in any organization. Covering the major commercial offerings available, it provides authoritative guidance through the implementation process [3]. It puts cloud computing into historical context and considers how cloud computing affects project management, budgeting, and lifecycle management in your organization. It also explains how to:

- Choose the best combination of platforms, tools, and services
- Develop new cloud applications from scratch
- Migrate legacy software
- Prevent lock-in to a single vendor
- Estimate costs and benefits
- Address reliability, availability, and security concerns
- Use inter-clouding, Cloud Brokers, and other techniques for safe deployment in public, private, and hybrid clouds
- Take advantage of the latest developments

II. Existing System

Cloud computing is setting off great changes in the IT industry. There are more and more researches on cloud computing. And this paper focuses on cloud computing too. At the beginning this paper describes the characteristics and definitions of cloud computing, and then introduced its services patterns (including SaaS, PaaS and IaaS) and deployment patterns (including public cloud, private cloud and hybrid cloud), at the end lists the cloud security challenges that cloud computing faces [1].

Ensure continuity of the cloud platform services and high availability of user data and business: Amazon data center downtime event, Google's Gmail failing to use event and so on are associated with cloud computing availability. To a certain extent, the events above discourage the enthusiasm of the enterprise to use public cloud. Cloud computing service need to provide a fault tolerant mechanism to backup user data to reduce the impact in application when the original data is destroyed. In addition, the software itself may have loopholes and a large number of malicious

attacks happen, all these above greatly increase the possibility of service interruption. How to protect the high availability of software services and user application and how to provide convenience security management to the thin-client user have become one of the biggest challenges of cloud security [2].

Ensure the safety and privacy of user data: user data stored in the cloud system, for malicious attacks, the primary purpose is to get user privacy, and then to obtain economic benefits. In this case, laws, regulations and processes are the problems that are the most urgent to be solved, and relevant laws and regulations should be established and improved to protect third-party security, to meet requirements listed by companies, especially to clear responsibility division when problems arise and to provide protection mechanisms as cloud service providers exit. In the domestic, most businesses are reluctant to store sensitive information in third-party, and they still focus on building private cloud. Only Security system and regulations gradually be perfected and security technology continues to progress, the future of public cloud services will get a sustainable evolution [3].

Perfect the cloud standards: Interest-oriented IT development process leads to cloud standards exist everywhere. Many manufacturers have defined their own application standards and data formats, forcing the user deploying IT system and their own business in accordance with the framework set by different service provider. Ultimately, all of this leads to business fragmented and chaotic system which are adverse to users' application. In cloud computing, cloud computing security standards and evaluation system provides an important technical and management support [4].

It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn't move them to cloud.

According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues stages of data life cycle.

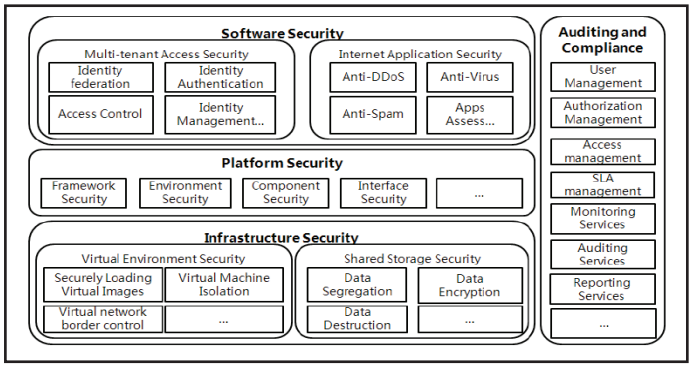

Fig. 1: Cloud Computing Security Architecture

The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern. These concerns include whether personal information can be stored or read by third parties without consent, or whether third parties can track the web sites someone has visited. Another concern is whether web sites which are visited collect, store, and possibly share personal information about users. The key to privacy protection in the cloud environment is the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements [5].

Software as a Service is becoming a popular research field in software development for its feature of low costing entry, easy implementation and zero infrastructures. SaaS is a multi tenant model which is different from traditional software in user data security, software development and deployment. This paper firstly analyses SaaS architecture, secondly introduces key technology of SaaS system from user data security, configurability user application and maturity model. Finally, this paper gives the future research directions [5].

III. Proposed Algorithm

On the cloud, there are many different services available. Among which some requires authentication, some are directly accessible and others are requiring additional authentication.

Since there can be many servers on the cloud and the application, data maybe distributed. Hence for secured data sharing additional methods of security are applied such as

1. Re-Authentication
2. Authorization
3. Encryption and Decryption
4. Hand-shaking mechanism

In this work we have applied encryption and decryption using RSA algorithm of the messages being communicated between the teachers and students.

Some of the data has been with encryption within the database which will be decrypted and provided to only authorized students.

1. Teacher will authorized student for messaging
2. For encryption and decryption we are using RSA algorithm which uses public and private keys for encryption and decryption respectively.

In this work, when a student will login, he will get a key from Authentication Server, which will be used when student will try for messaging with teachers after checking authorization.

The key (authorization token) is being generated for providing to users as follows:

Key format: <CC><NNNN><CC>
Where; C: stands for character
N: stands for number

Various steps in proposed algorithm are as follows:

Step 1: User A Write an e-Learning message on server 'A' and User 'B' reads it on Server 'B' on the cloud.

Step 2: Server 'A' will use the cloud application to send information to all the servers on the Cloud in secured way.

Step 3: Server 'A' first takes a Key from the Authentication Server, which provides the key after full confidence on Server 'A'.

Step 4: Server 'A' connects to Server 'B' and specifies the key obtained from AS to Server 'B'

Step 5: Server 'B' verifies the key from the AS and obtains a key for itself.

Step 6: Server 'B' sends the acknowledgement to Server 'A' and key obtained to Server 'A'

Step 5: Server 'A' verifies the key from AS and starts communication with Server 'B'; Server 'A' sends the user and e-Learning data to Server 'B'.

Step 6: Server 'B' stores the data in its database.
Step 7: All communication happens with encrypted text.

For generating above key we have used random pattern generation mechanism as follows:

```
Algorithm GenerateKey ( )
Begin
        Key: =" "
    For i=1 to 2 do
        X: =Random (65, 90)
        Key: =key+ (char) X
    End do
    For i=1 to 4 do
        X: =Random (48, 57)
        Key: =key+(char) X
    End do
    For i=1to 2 do
        X: =Random (65, 90)
        Key: =key+ (char) X
    End loop
    Return key
End
```

A. Flow Chart For Key Generation

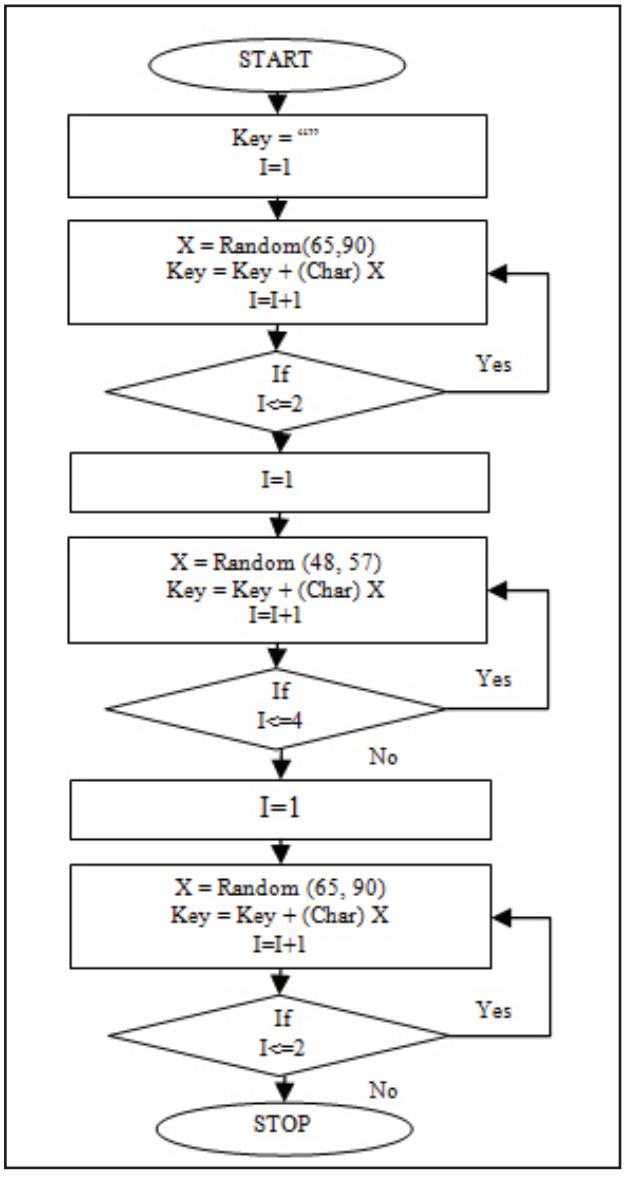

Fig. 2: Flow Chart Showing the Key Generation

The relative security of cloud computing services is a contentious issue that may be delaying its adoption. Physical control of the Private Cloud equipment is more secure than having the equipment off site and under someone else's control. Physical control and the ability to visually inspect the data links and access ports is required in order to ensure data links are not compromised. Issues barring the adoption of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services.

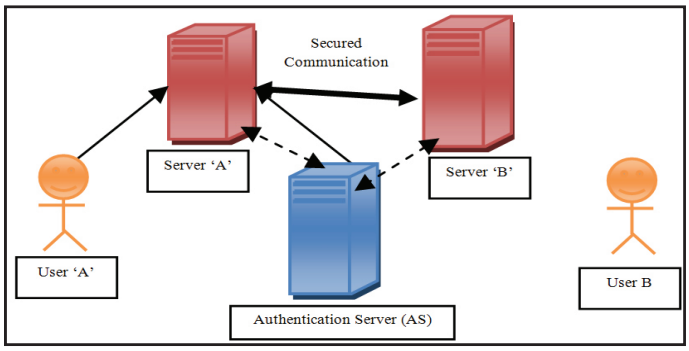

Fig. 3: Working of the Proposed Algorithm

The main advantages of such a Cloud Computing are:

- Load on data centres is distributed
- Server fail occurrences do not affect to the users
- Communication is available to the users irrespective of the state of the inter cloud hardware
- Fast communication
- Secured Communication

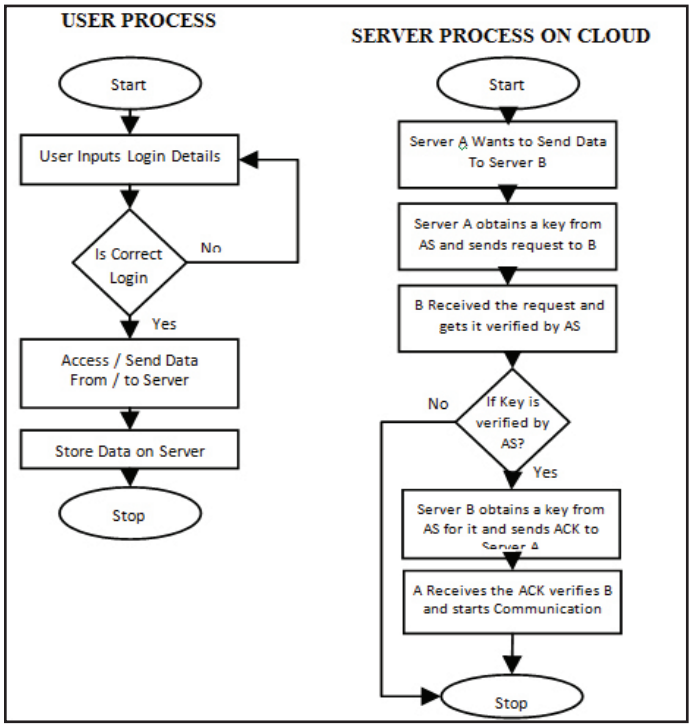

Fig. 4: Flow Chart of Proposed Algorithm

B. Backup Plan

The proposed work is expected to be working upto the mark but in case if the proposed work is not working as expected then I the use of symmetric key cryptography shall be providing security of the data so that it will not be hacked during the transfers and hence the system will not fail completely.

IV. Results & Discussion

A. Performance Evaluation

For performance evaluation of the proposed system, we have recorded the time taken in transferring the messages to the server and storing in database between students and teachers to and fro. These timing have been calculated using stop watch class of the C#. The graph has been drawn by calculating the average time taken in messaging for students and teachers separately. The graph below shows the average time taken in processing for the students and teachers. The graph indicates that the average time taken in processing in not very high for around 20 messages for students and 20 messages for teachers. This is to infer that the application of the proposed algorithm does not burden the system and provided good average timing taken in processing.

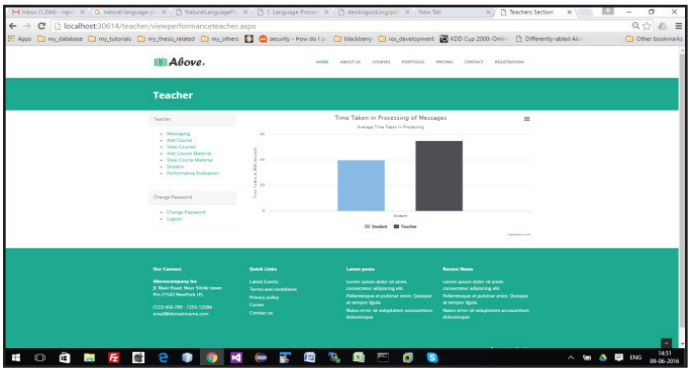

Fig. 5: Performance Evaluation of the Proposed system

Comparison between the Existing System and Proposed System Work done by Irfan Gul, Atiq ur Rehman, M Hasan Islam for security of the E-learning system auditing has been considered for comparison in this work. According to the authors, they have focused on cloud security issues in general and cloud security auditing in particular. They have carried out a critical analysis of strengths and weaknesses of these auditing models and techniques. Since cloud computing is in its stage of infancy, a common, interoperable and cloud-specific auditing mechanism need to be designed to maintain trust and transparency within the cloud environment.

It is found that the e-Learning system operates completely. Furthermore, by comparing the destination data with the data source, the outcomes are correctly. The application interacts with the services and retrieves the learning resources. The results indicate that the interoperability of applications performed correctly.

Following comparison table has been drawn between the existing work and proposed work:

Table 1: Comparison Between Existing and Proposed Systems:

Existing System	Proposed System
Existing System focuses on Auditing of the security methods	Proposed System focuses on Performance of the Security Methods
Strengths and Weakness of the Security system has been analysed	Performance and Efficiency of the Security system has been analysed and evaluated
No concrete results have been shown for the work done and results have been drawn using analysis only	Concrete results have been shown using the graph and found to be encouraging for future enhancements and applications

In work done by Jian Liao and Minhong Wang, to evaluate the effectiveness of the model, three questions should be discussed as follow.

1. Can the learners rather than teachers tutor learners themselves to make more performance or improvement in the scale of whole group?
2. Does the cloud system recommend the appropriate resources, especially the service providers which the learners really need or are satisfied with?
3. Is the free market economy mechanism in cloud effective to improve the utility of resources in the whole group to the greatest extent?

Based on these questions, a pilot test of investigation and interview had been conducted qualitatively and quantitatively. In the pilot test, the initial findings show an obviously positive attitude towards the solution. Interview data indicate that although when the learners face the problems in study, they prefer to ask for the teacher, if the higher grade student can provide the similar reply, they will also be satisfied.

Furthermore, talking with classmates or higher grade students is subject to make the learners feel free, and then, discussing the problem more deeply. However, a problem should be emphasized that is for some opening questions, if learners received different answers from different higher grade students, they still hope to appeal to teacher to provide an authoritative answer.

In respect of their work, our work is not only providing a high security and performance but is also found to be acceptable among the students and teachers both. Since no proper survey have been done therefore our system shall be tested for the same in future in lieu of the above questions.

V. Conclusion and Future Work

This work was aimed to provide the high security over the cloud computing environment for the applications running on the cloud. These proposed algorithms have two fold securities and will involve verification of the students over the cloud. The work will require the students to have the security code and must have been authorized by the teacher then it will make them access the services. The internal processing of the authentication server communication is done to decrypt the data and show it to the students if the students are properly authorized and carries the security key provided to them by the authentication server. The implementation of this work has been done to show that the work is providing high security of the data to the authorised and authenticated users of the system.

VI. Future Work

The proposed algorithm can be tested on heavily loaded real time servers providing e-Learning. The system can also be provided with additional security algorithms and automated to test the performance. The proposed work can be improved by adding more services related with the e-Learning.

References

[1] Shakeel Ahmed, Khalid Buragga, Ashwani Kumar Ramani,"Security Issues Concern For E-Learning By Saudi Universities", Department Of Computer Science, Department Of Information Systems, CCSIT, King Faisal University, Saudi Arabia. School of Computer Science, DAVV, Indore, India.

[2] Latifa Ben Arfa Rabai, Neila Rjaibi,"Quantifying Security Threats For E-Learning Systems", Department of Computer

Science, International Conference On Education And E-Learning Innovations.
[3] E-Learning Ecosystem Based on Service-Oriented Cloud Computing Architecture, 2013 5th Conference On Information And Knowledge Technology (IKT).
[4] Pablo Sánchez Barreiro, Diego García-Saiz, Marta Elena Zorrilla Pantaleón,"Building Families of Software Products For E-Learning Platforms: A Case Study", IEEE Revista Iberoamericana De Tecnologias Del Aprendizaje, Vol. 9, No. 2, May 2014.
[5] From Monolithic Systems to a Federated E-Learning Cloud System 2013 IEEE International Conference on Cloud Engineering.
[6] A Collaborative Learning System Based on Cloud and E-Commerce 2011 Eighth IEEE International Conference on E-Business Engineering.
[7] Exploration of Cloud Computing Adoption For E-Learning In Higher Education. 2012 Second Symposiums on Network Cloud Computing and Applications.
[8] Cloud Computing; A New Business Paradigm for E-Learning, 2011 Third International Conference on Measuring Technology and Mechatronics Automation.
[9] An Enhanced E-Learning Ecosystem Based on an Integration Between Cloud Computing and Web2.0
[10] From Monolithic System to a Federated E-Learning Cloud System, 2013 IEEE International Conference on Cloud Engineering.
[11] "Cloud Computing Data Breaches".
[12] Securing User Authentication Using Single Sign-On In Cloud Computing.
[13] Implement of Cloud Computing for E-Leaming System.
[14] P. S. Barreiro, D. García-Saiz and M. E. Z. Pantaleón, "Building Families of Software Products for e-Learning Platforms: A Case Study," In IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, Vol. 9, No. 2, pp. 64-71, May 2014.
[15] Safwan Mahmud Khan, Kevin W. Hamlen,"Hatman: Intra-cloud Trust Management for Hadoop", 2012 IEEE Fifth International Conference on Cloud Computing, IEEE 2012.
[16] Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom,"Cloud Computing Security: From Single to Multi-Clouds", 2012 45th Hawaii International Conference on System Sciences 2012 IEEE.
[17] Deyan Chen, Hong Zhao,"Data Security and Privacy Protection Issues in Cloud Computing", 2012 International Conference on Computer Science and Electronics Engineering 2012 IEEE.
[18] Zhang Yandong, Zhang Y ongsheng,"Cloud Computing and Cloud Security Challenges", International Symposium on Information Technology in Medicine and Education, 2012.