Secure Access of Intelligent Tutorial System on Cloud Using RSA Algorithm

Prof. Sweta G. Phegade[1], Prof. Tejal H. Oza[2] and Prof. Kalyani Neve[3]

[1,2,3]G.H. Raisoni Institute of Business Management, Jalgaon

ABSTRACT

Intelligent Tutoring System on the cloud considers the student’s learning style and quality of education. This paper presents a general architecture of ITS using the cloud paradigm for effective working of distance learning education system. In ITS cooperative learning is achieved either by interaction between the student and the tutor or inside the group of learners. Intelligent Tutorial System is generally used for any trends of study like mathematics, physics, computer etc. Cloud computing is nothing but privatization of Internet on demand and with complete scalability of required resources which is very useful for Intelligent Tutoring System. ITS hosted on the Cloud will provide effectual services using cloud’s secure layer. This paper further discusses the security challenge faced by intelligent tutorial system’s access through cloud. This security threat can hence be trounced using RSA algorithm. Internally RSA implements a public-key cryptosystem wherein each user has his own encryption and decryption procedures.

Keywords: Cloud, Data Security, Domain, Encryption, Encryption, Intelligent Tutoring System, Interface, RSA.

Introduction

In Intelligent Tutoring Systems (ITSs) are computer-based instructional systems with models of Instructional content that specify what to teach and teaching strategies that specifying how to teach. They make inferences about a student's mastery of topics or tasks in order to dynamically adapt the content or style of instruction. Expert systems (or knowledge bases, or simulations) give ITSs depth so that students can "learn by doing" in realistic and meaningful contexts. In recent years ITSs have moved out of the lab and into classrooms and workplaces where some have been shown to be highly effective. While intelligent tutors are becoming more common and proving to be increasingly effective they are difficult and expensive to build. Authoring systems are commercially available for traditional computer aided instruction (CAI) and multimedia-based training, but these authoring systems lack the sophistication required to build intelligent tutors (Tom Murray, 2003) . In Intelligent Tutoring System student learns better through one-to-one teaching than through class room teaching. Intelligent Tutoring System (ITS) is one of the best ways of one-to-one teaching. The origin of the ITS evolves from the field of Computer Assisted Learning (Gonzalo 2010). They generally provide a high level of guidance and control interaction process. ITS instructs about the topic to a student, who is using it. The student has to learn the topic from an ITS by solving problems. The system gives a problem and compares the solution it has with that of the student and then it evaluates the student based on the differences. The system keeps on updating the student model by interacting with the student. As the system keeps updating the student's knowledge, it considers what the student needs to know, which part of the topic is to be taught next, and how to present the topic. It then selects the problems accordingly (B. H. Sreenivasa Sarma and B. Ravindran, 2007).

Existing system of ITS

There are four modules in Intelligent Tutoring System, namely Expert, Student, Tutoring and Communication modules as shown in Fig.1.

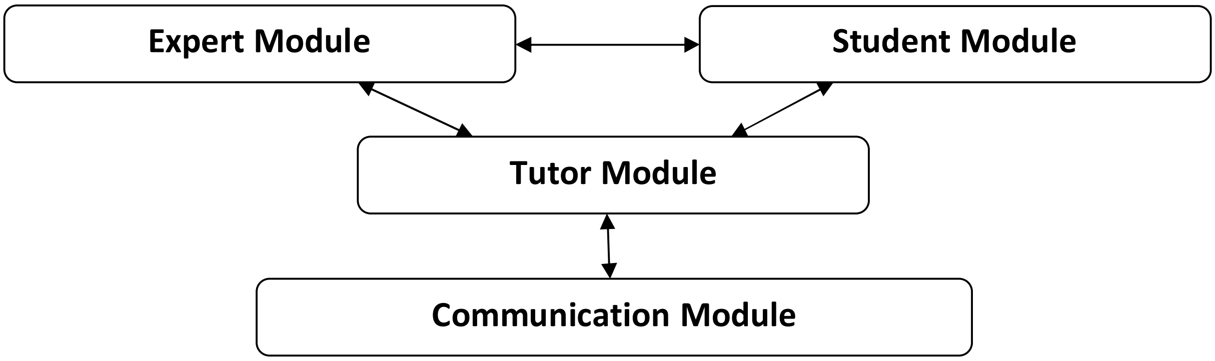

Figure 1: Intelligent Tutoring System

The expert module is a set of questions being taught. The tutoring module contains pedagogical knowledge for instructions and presentation to the students. The student module contains the information about the students. And the communication module will provide the interface between students and the System

This paper further discusses about hosting the ITS system on the cloud The emerging cloud computing model attempts to address growth of web-connected devices, and handle massive amount of data. To a large extent, cloud computing is based on virtualized resources. Cloud computing provides the facility to access shared resources and common infrastructure, offers services on demand over the network to perform operations that meet changing business needs.

The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop deploy and manage their applications 'on the cloud'.

This paper also throws light on the generic architecture of Intelligent Tutoring System using cloud paradigm. The paper is divided into parts. In the first part, we describe the conversion of common standalone ITS architecture—to one capable of operating over the Cloud. The second part, discusses data access security from the cloud which would be an issue.. This issue can be overcome by implementation of RSA algorithm (client side). So the paper further discusses theoretical implementation of the RSA for secure access of Information from any ITS hosted over a cloud.

Architecture of its using cloud

The above paper discusses ITS with its modules and architecture hosted on cloud. The structure of ITS system mainly consists of four modules, viz. Expert, Student, Tutoring and Communication. Providing the credentials any user can access information from ITS hosted over the cloud. These credentials are unique for every user. The architecture of ITS hosted over Cloud is shown in figure 2. Each of the following described modules have a very important role to play for the sound working of ITS.

1. *Expert Module (Knowledge of Domain)*

The expert module contains knowledge about the subject to be taught to the students, and it is the base for analysis of student's answers. In other words, expert module informative concepts, which are small pieces of information in which the knowledge of the expert is divided in order to explain the subject to the people, and the knowledge necessary to solve the exercises.

This knowledge must be efficiently organized, so that it can be easily accessed, modified and extended. Students using these systems usually solve problems and associated sub problems within a goal space, and receive feedback when their behavior diverges from that of the expert model.

The basics of its functioning are:

a. Information is divided in very small, but fully understandable informative concepts.
b. Each of these informative concepts will point to other concepts that must be shown necessarily before or after it, inside a particular block of concepts. Each block will point to other clocks that must be shown necessarily before or after it, in a given module.

c. A determined group of blocks will form a module, and all the modules together will form the whole course. Each module will point to the next one inside the course.

2. *Students Module (Knowledge of the person being taught)*

The student's module keeps individualized information related to each student that is doing the course. This module is responsible for knowing what informative concepts have already been taught to a student, how many exercises he has done and the degree of success and time he has used to complete them.

It is used to evaluate the understanding of the people and to identify his particular way of learning, in order to let the system adapt to this method. It is also useful to know what topics he finds more difficult to understand. This model also informs the routines of the tutoring model. The student model represents the learner's emerging knowledge and skills. Information such as learning preferences, past learning experiences and advancement may also be relevant in adapting the teaching process.

3. *Tutoring Module (Knowledge of teaching strategies)*

The tutoring module contains the pedagogic knowledge and is in charge of selecting the appropriate topics to be shown in the course. Thus, this module will put forward the necessary concepts and exercises in order to let the people face the training successfully. It also has all the strategies, rules and processes that drive the interactions between the student and the system, in order to make decisions about the informative concepts to show and the exercises that the people must do, along with the moment when he must be interrupted in order to correct him or make suggestions.

Systems in the Tutoring Strategies category have the most sophisticated set of primitive tutorial actions, compared with systems in other categories. In addition some systems in this category represent multiple tutoring strategies and "meta-strategies" that select the appropriate tutoring strategy for a given situation (Tom Murray, 2003).

4. *Communication Module (Knowledge of how to apply the tutoring knowledge to the needs of an individual)*

This module integrates three types of information that are needed in carrying out a communication: knowledge about patterns of interpretation (to understand a speaker) and action (to generate utterance) within communication, domain knowledge needed for communicating content and knowledge needed for communicating objective (Indira Padayachee, 1999).

This module is in charge of the communication between the people who follows the course and the ITS. This module must inform the tutoring module of the actions that are performs by the people all along the course. This action may be visualization of an informative concept, the answering of an exercise in any of the forms that it may adopt, or one of the actions performed inside the Cloud. This idea gives us a clue about how the integration between both systems can be carried out.

This module makes possible the presentation of informative concepts and exercises in an easy to understand, perceptive way. This is essential, since an improperly designed communication module may result in a system that nobody ill use, either because it is ugly. A well designed communication module causes the interaction between the people and the system, to be much more pleasant.

To host an ITS over the cloud we eliminate the Communication module from the ITS architecture and hosting service providers like Amazon Web Services, Google Apps or Microsoft Azure to host an ITS over their cloud as shown in figure 2.

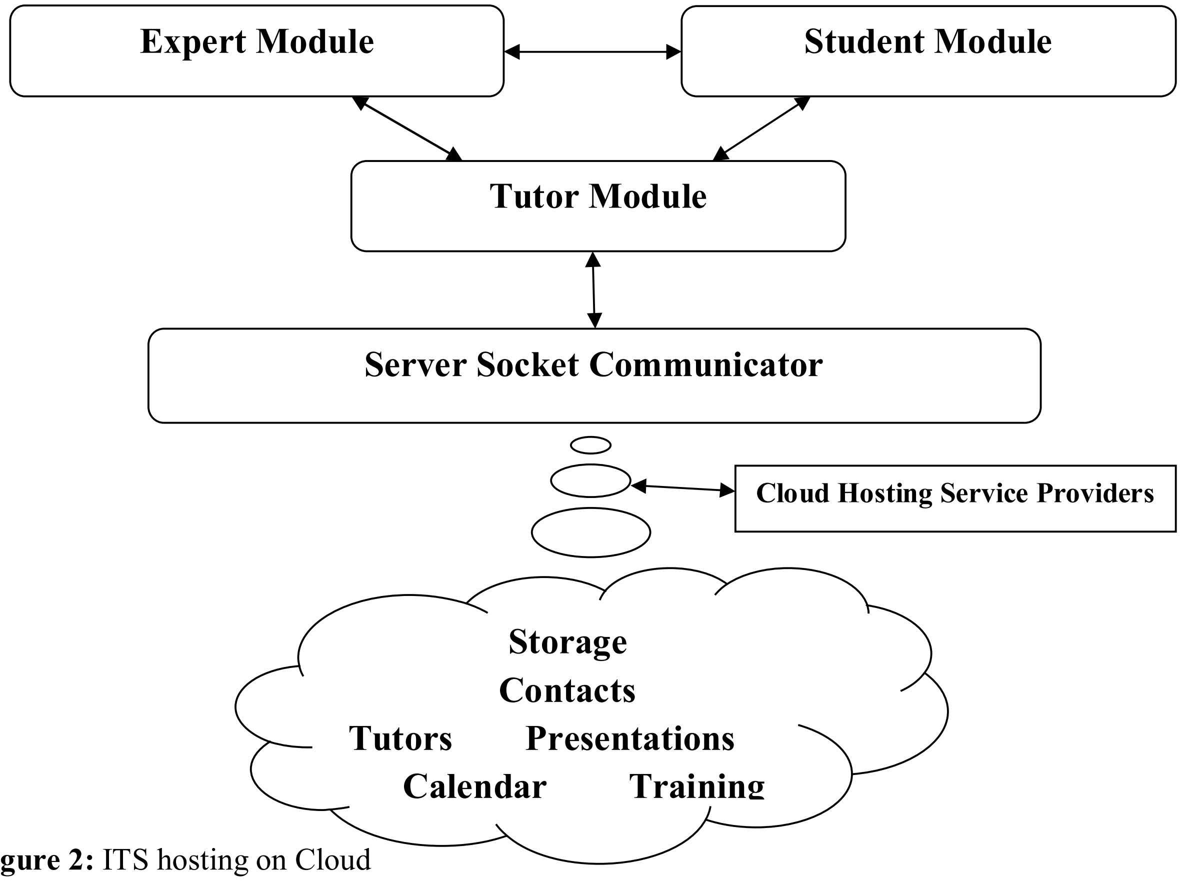

Figure 2: ITS hosting on Cloud

So how these service providers can provide the cloud services, we see this by taking one example of Amazon Web Services. Here steps are provides to host the system over AWS cloud and its diagram in figure 3 (Matt Tavis, Philip Fitzsimons, 2012).

Below is the short description of the various components of the figure above:-

Elastic Load Balancer: - spreads traffic to server Auto scaling group.

Exterior Firewall moved to every Web Server instance via Security Groups.

Auto Scaling Web Tier Group of EC2 instances handling HTTP requests.

Backend Firewall moved to every back-end instance.

App Server Load Balancer Software LB on EC2 instances to spread traffic over app server cluster.

Auto-scaling App Tier Group of EC2 instances running the actual app. Instances belong to Auto Scaling group.

ElastiCache Provides caching services for app, removing load from database tier.

DB Tier MySQL RDS DB creates a highly available architecture with multi-AZ deployments. Read-only replicas can also be used to scale read intensive applications.

Steps to hosting Intelligent Tutoring System on Amazon Web service Cloud.

1. Create an instance of EC2 using Amazon web services.
2. Select type whether a micro or large instance would be required.
3. Attach an Elastic Load Balancer to the EC2 instance
4. Create a bucket for database to be attached to the EC2 instance.
5. Now the infrastructure is ready on the AWS (cloud) to host ITS
6. Host the ITS on the EC2 instance using an Elastic IP

Intelligent Tutoring System

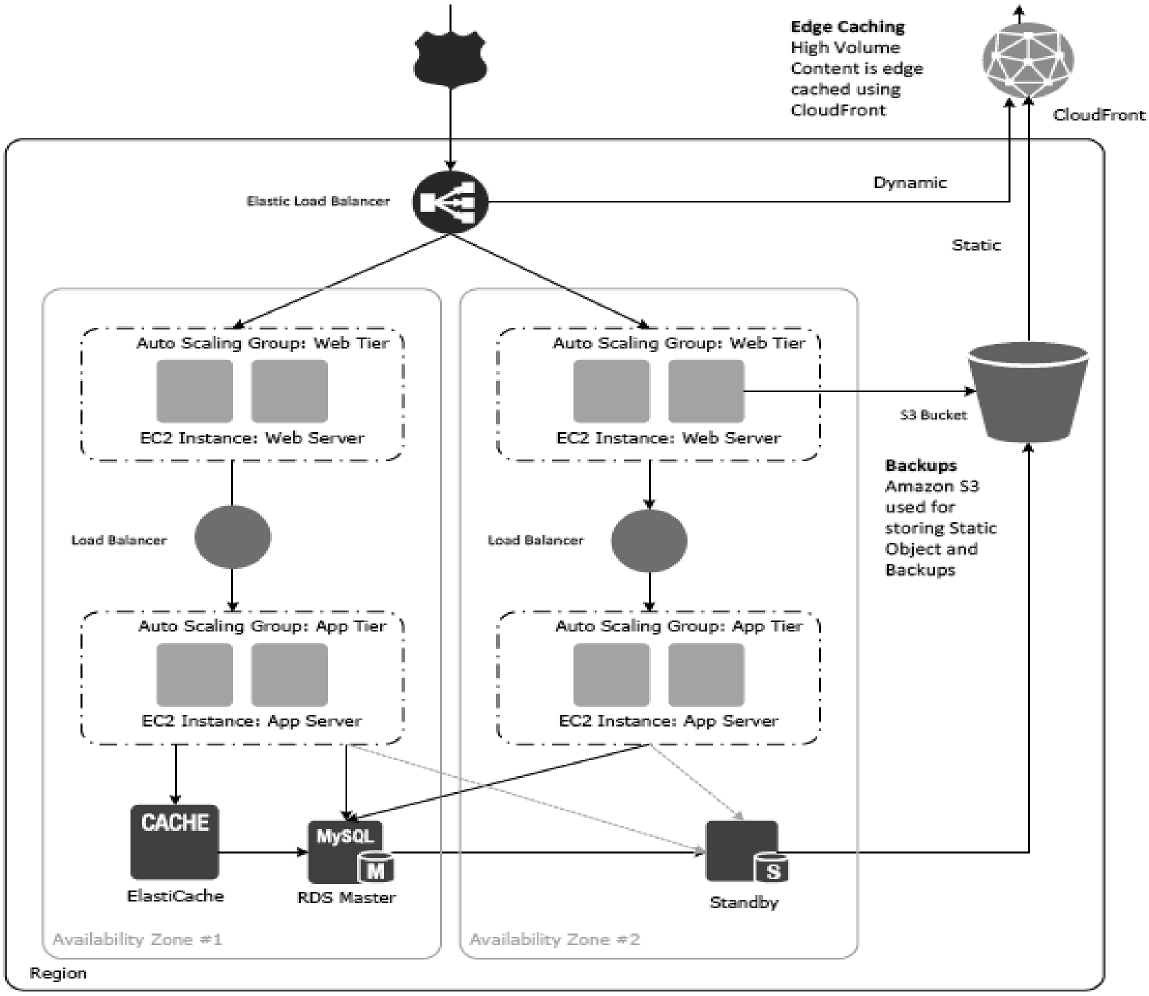

Figure 3: Hosting ITS on AWS

This technology is established on a computer network, it allows multiple computers to function as one. Once we host ITS over cloud we deals with different important key concepts like content delivery, security, Privacy and Confidentiality, Data integrity, Data location and Relocation, Storage, Backup and Recovery. As moving more tutorial data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends computer based security measures mostly capitalizes on user authorization and authentication.

Challenges faced by Cloud

Security

Being able to keep important data secure has always been a priority in ITS, but a technology that takes information outside of the virtual ‘secure walls’ can raise red flags. Also, users will need to include provisions that directly specify how cloud computing providers plan on protecting data.

Privacy and Confidentiality

Once the expert host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access by students. The cloud seeker i.e. people who access ITS from cloud should be assured that data hosted on the cloud will be confidential.

Data integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point.

Data location and Relocation

Cloud Computing offers a high degree of data mobility. Students do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. This, then, requires a contractual agreement, between the Cloud provider and the ITS that data should stay in a particular location or reside on a given known server.

Storage, Backup and Recovery

When you decide to move data to the cloud the cloud provider should ensure adequate data flexibility storage systems, backup services which are certainly important for ITS system that run cloud based applications.

Use of RSA algorithm to overcome the Security Problem

Mainly next part of this paper will discuss the security challenge faced by ITS and overcome it by using RSA algorithm. Thus the main concern with reference to security of data residing in the Cloud is: how to ensure security of data that is *at rest*.

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned student user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data.

RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the ITS user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or ITS user. Once the data is encrypted with the Public-Key (Devid Morgan, 2007), it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps (Parsi Kalpana1 , Sudha Singaraju2, 2012):

1. Key Generation
2. Encryption
3. Decryption

1. Key Generation

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the Intelligent Tutorial System user.

1. Choose any two prime numbers call them p and q
2. Multiply them call product n = p*q
3. Multiply their "predecessors" (p-1, q-1) call product k.
4. pick some integer call it e
   i. between 1 and k (exclusive)
      sharing no prime factor with k
   ii. Find the integer (there's only one) that call it
      a times e divided by k leaves 1

then keys are:

– Public: e together with n (e is for "encryption")

– Private: d together with n (d is for "decryption")

For applying this key generation step on cloud data for accessing tutors we take some sample data to generate the key.

A. Choosing two prime numbers p=5 q=11.
B. Multiply them n = p*q we get 55
C. Multiply their "predecessors" (p-1,q-1) k=40
D. pick some integer e=3

a. between 1 and k (exclusive)

b. sharing no prime factor with k

E. Find the integer (there's only one) that d = e^{-1} mod k

a. thus d= 3^{-1} mod 40 = 27

then your keys are:

– public: e together with n {3, 55}

– private: d together with n {27, 55}

2. Encryption

Encryption is the process of converting plain text to cipher text which is shown in following figure 4.

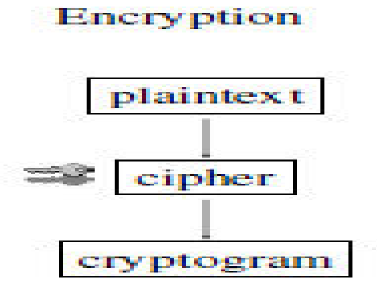

Figure 4: Encryption

For encryption following steps can be carried out:

Encrypting with public key {e,n} i.e. c = m^e mod n

1. Choose a plaintext message call it m

-in the form of a number less than n

2. Raise it to power e

3. Divide that by n call remainder c

then your cipher text result is c

For encryption, The Public-Key (3, 55) is given by the Cloud service provider to the ITS user who wish to store the data.

a. choose a clear text message means user map the data to an integer m=7

– in the form of a number less than n

b. Raise it to power e 7^3=343

c. Divide that by n c = 343 mod 55 (55x6+13)

then your cipher text result is c c=13

3. Decryption

Decryption is the procedure of converting cipher text into again plain text and pass it to students whose access the ITS notes which is shown in figure 5.

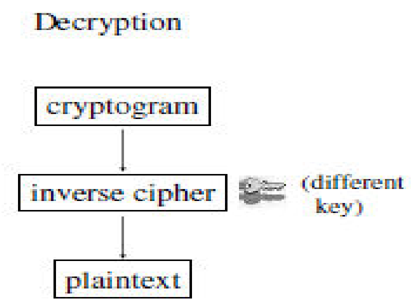

Figure 5: Decryption

For encryption following steps can be carried out:

Decryption with private key {d, n} i.e. m = c^d mod n

1. Take cipher text c
2. Raise it to power d
3. Divide that by n call remainder r

Then recovered result is r is identically the original plain text message m

When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data to the ITS user (If the user is valid).

1. Take cipher text c = 13
2. Raise it to power d

    13^{27}=1192533292512492016559195008117

3. Divide that by n

    13^{27} mod 55 = 7 then your recovered result is r, r=7

Conclusion

This paper has discussed the AI sub domain of intelligent tutoring systems and the Cloud combination. The cloud paradigm though is evolving speedily, yet when an organization has to host its data or service on a cloud, there are many concerns as to whether the data would be secure or not, whether the access will be authorized or not. So this paper provides a way to use cloud for hosting an ITS service and also helps to overcome security as a challenge over the cloud by using the RSA algorithm. Hence the data hosted on the cloud will be encrypted, so if any intruder tries to breach the system hosted on the cloud also, he will not be able to recover the data.

References

Gonzalo Mendez, Angelica de Antonio, Pilar Herrero Facultad de Informatica, 2010, PRVIR: an Integration between an Intelligent Tutoring System and a Virtual Environment, Universidad Politecnica de Madrid, 28660, Espana.

B. H. Sreenivasa Sarma and B. Ravindran, 2007, Intelligent Tutoring System auding Reinforcement learning to teach Autistic students, India Institue of Technology Madras, Chennai – 36, India.

Tom Murray, 2003, An Overview of Intelligent Tutoring System. Authoring Tools updated analysis of the State of the Art.

Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham(2010), *International Journal of Information Security and Privacy*, 4(2), 39-51, 39 .

http://enwikipedia.org/wiki/Cloud computing Accessed on May 2009.

Indira Padayachee, 1999, "Intelligent Tutoring Systems: Architecture and Characteristics" University of Natal, Durban, Information Systems & Technology, School of Accounting & Finance padayacheei@nu.ac.za.

Parsi Kalpana , Sudha Singaraju, Sept 2012, Data Security in Cloud Computing using RSA Algorithm, Sreenidhi Institute of Science and Technology.

Avi Kak (2013), Lecture 12: Public-Key Cryptography and the RSA Algorithm.

Milan (2009), Lecture Notes on Computer and Network Security: The RSA Algorithm.

Devid Morgan (2007), The RSA Algorithm, a foundation of public key substitution ciphers.

Hyacinth S. Nwana (1990),Intelligent Tutoring System: an overview, University of Liverpool, Liverpool L69 3BX, UK.

Matt Tavis, Philip Fitzsimons (2012), Web Application Hosting in the AWS Cloud Best Practices.