Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Cloud-Based Result Security System Using Digital Certificate

Eke B. O. (PhD)*, Nweke O. E.
Department of Computer Science, University of Port Harcourt,
Nigeria

Abstract— Developments in Cloud Computing and its robust nature has made academic institutions to build their institution applications which include results around the Cloud. The challenges of security of data in when it is managed as a service (DBaaS) in the Cloud and the believe that the data is really secured remain a problem for Cloud application service users. In order to ensure trust and security of students results and who access it an efficient security method is required. This paper investigates some of the privacy and security issues encountered in cloud computing, and a cloud result security system is developed using a two form authentication. This is achieved by the use of digital certificate in combination with normal Cloud security system for authentication of users and encryption for storage of data. We apply the MVC architecture in developing the user interface in order to control unauthorized access to different parts of the application, using role based authorization. Though this study is carried out using students results of higher academic institutions, but other organizations can also adopt the security techniques applied here to secure their Cloud application systems.

Keywords— Cloud, Security, digital certificate, students result, DBaaS, Unauthorized access

I. INTRODUCTION

The use of the cloud for deploying computing services has come to stay, we find a particular application of these in the education sector were students results are computed and published (managed) through the cloud. This is quite an effective way of carrying out such task in the sense that it reduces the burden attached to manual processing and the cost of setting up individual infrastructure for a result automated systems. But the issue of security in the cloud still remains a key factor to the progress of the adoption of cloud based systems and other cloud based services [1].

The most common implementations of the student result systems in Nigerian Universities have been in the form of standalone systems, Campus Area Network (CAN) and web applications which are accessible over the internet. The aforementioned methods of implementation can be quite demanding on the side of the institution, as they will have to acquire a vast amount of computing resources, and also train personnel to manage these systems, in addition is the cost of software licenses, update/patches etc. A cloud computing approach is employed so as to overcome the financial and intricate challenges encountered in developing and maintaining these systems, a case whereby the applications are made available as a service in the cloud. Universities interacting with the result service are not burdened with software license, updates, security patches, backup and a host of other administrative and technical task associated with on-premises result system.

While there are interesting gains to the adoption of Cloud Computing there are concerns in the privacy of users and the aspect of data security. The data been conveyed through the internet is stored in remote areas. Additionally, cloud service providers render their services to numerous clients at a time which could also help augment the series of security breaches. In managing confidential information such as student personal information- result and transcripts, security has to be critically considered as it can be a major source of worry for University management and other users of the cloud application[1].

Authentication based on one factor is becoming obsolete due to the vulnerability of the password-based mechanisms, in addition to the rising number of threats to the Internet. The impact is negative on cloud computing solutions as it poses a threat to the safety of online transactions by organizations and other individual consumers. In order to ensure a well secured network, proper combination of several security measures for both data and the network itself is required. Data breach, loss of data, vulnerable interface, service traffic hijacking and distributed technology weaknesses, constitutes a number of security concerns in the cloud.

In this paper, the Public Key Infrastructure (PKI) is explored as an added building block for securing students results in the application services using the cloud as a service platform, this infrastructure comprises digital certificate.

II. CLOUD COMPUTING

NIST [2] defines Cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A. Cloud Computing Service Models

Cloud Computing Service Models include the following services :

1) Software-as-a-Service (SaaS): Software-as-a-Service (SaaS) is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations [3].

2) Platform as a Service (PaaS): PaaS provides an environment for easy development and deployment of applications. For example, a PaaS system might provide an environment that lets a user self-provision a web server, database and filesystem, then build an application on them [4].

3) Infrastructure as a Service (IaaS): In IaaS the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications [1].

4) Database-as-a-Service (DBaaS): Cloud-based services are available for almost every component of the modern application stack including the database layer. DBaaS (Database-as-a-Service), cloud database services exist for almost all of the modern relational databases (MySQL, Postgres, etc…), as well as for NoSQL databases such as MongoDB, CouchDB, and Neo4J [5].

B. Deployment of Cloud Services

Cloud services are often deployed in various ways which includes:

1) Private cloud: Private cloud is described as the cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).

2) Community cloud: Community cloud is described as a cloud whereby infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).

3) Public cloud: Here, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

4) Hybrid cloud: In a hybrid cloud, the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.

C. Benefits of Cloud Computing

IBM [6], Sclater [7], and Crucial Cloud hosting [8] identifies the benefits of cloud computing as: scalability, cost saving, improve accessibility, less personnel training, back up/ storage, resource and time savings, flexibility, disaster recovery, lower environmental impact, end user satisfaction etc. IBM [6] specifically states that Cloud adoption has particularly affected the higher education sector, where the benefits of introducing these innovative systems are even more conspicuous. An added benefit to cloud computing is that it helps institutions to focus on their primary business which is education and research Sclater [7].

D. Risks of Cloud Computing

Decision makers in institutions most times express concerns in relocating their data to the cloud or even delegating services outside the institution. Some IT personnel are at the risk of losing their jobs to the cloud providers. Sclater [7] noted risks in the following areas:

1) Data security: The security of data poses a huge risk in the minds of potential clients. Institutions may contemplate their data been more secured in a familiar location rather than an unknown area. Hence they fear moving their data to a service provider to host for them in an area unknown to them.

2) Availability: Despite the fact that service availability is an advantage to opting for cloud, there is also the probability of some high profile providers suffering from denial of service attacks. This is why it is preferred to employ several cloud service provider so as to prevent single point of failure as this helps to reduce such risk.

3) Unsolicited advertising: Cloud providers usually send update emails, advertising and newsletters to customers without their consent.

4) Multitenancy threat in the cloud: As it is with the public cloud, multiple users' data are saved and retrieved from a shared server; hence if there is occurrence of a security breach, it may affects every user whose data is on the server.

III. SECURITY

A system which precisely delivers the facilities needed by a user and averts the unlawful and or unauthorized use of system resources is called a secured system. While any action that compromises the security of a system is called a security attack [9].

A. General Categories of Security Attacks

System security attacks can be categorized into the following:

1) Interruption: This refers to the attack on the availability of data. Data and resources are expected to be readily available round the clock once they are needed and requested for by authorized parties. Availability can be affected by intentional or un-intentional acts.

2) Interception: Unauthorized users need not retrieve data because an attack can be activated when someone who is not authorized to view confidential data gets to retrieve it, this can be referred to as a raid on confidentiality.

3) Modification: This is an attack on the integrity of data. In order to maintain data integrity we need to prevent intentional and unintentional modification of such data. It is more essential to protect data from modification rather than protecting them from detection.

4) Fabrication: This refers to an attack on authenticity. Authenticity means that message is coming from a clear source. It assures that a communication participant is who he says he is.

There are other categories of security attacks aside the ones discussed already, some of which are;

5) Password Attack: We can explain password attack as, repeated attempts to find user information (user name or password). There are a couple of techniques been used for password attack these include; Trojan horse, IP spoofing and packet sniffers which can show the detail of the user like username and password. Different types of password attacks exist, which include:Dictionary Attack, Brute force attack and Hybrid Attack. Different password cracking programs are available like Lophtcrack, NTSweep, NTCrack, Crack, John the Ripper etc.

6) Man-in-the-Middle Attack (MITM): This type of attack occurs when a hacker successfully encroaches communication between two different parties. If this happens the possible turn outs may be an attack on the confidentiality and availability of data.

B. Security Countermeasures Tools

The following tools are used to defend against security attacks;

1) Password Protection: This is a method of authentication typically done with the use of a username and password combination. There are several factors affecting the security of a password protected system. As mentioned earlier many methods of attacking password protected systems have been devised and so many attackers have gained illegal access into so called secured systems through these methods. This proves that the password protection method when applied alone is not sufficient to secure a system, as strong, long and encrypted passwords might not necessarily mean that they are completely safe; it's just a matter of time. Nowadays passwords are broken in a couple of weeks compared to earlier when it could take months.

IV. DIGITAL CERTIFICATE

Entrust [10] defines Digital certificates as electronic files that are used to identify people and resources over networks such as the Internet. Digital certificates also enable secure, confidential communication between two parties using encryption. When you travel to another country, your passport provides a way to establish your identity and gain entry. Digital certificates provide similar identification in the electronic world. Just like one will go to a passport office to obtain an international passport for identification in another region, a Certification Authority is expected to sign and issue Certificates to user, it serves as a third party package for identifying users. As soon as a CA signs a certificate, the user can identify themselves to others.

Digital Certificates comprises of the public key and name of the certificate holder, a serial number, expiration dates, and the digital signature of the certification authority that issued it. Trusted agency such as GlobalSign, VeriSign, Inc., Thawte Consulting, Symantec, Comodo Group, etc. can always verify the content of these certificates.By default every web browser contain list of trusted CA root certificates [11]. If two users possess a valid certificate and trust a common CA that has probably issued the user certificate they can both verify their identities [12].

Secure Sockets Layer protocol developed by Netscape is a standard Internet protocol used for secure communications, the secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL). A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS [13].

Related Works

Hashem et al [14] in their work proposed a security architecture for cloud computing which ensures secure communication system and hiding of information from others. As comprised in their model, AES based file encryption system and asynchronous key system was used for exchanging information or data. They also addresses this issue by defining and enforcing access policies based on data attributes, and allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Kumar [15] in his work proposes an efficient methodology of "data sharing in the cloud. In his technique, the secret key holder can release a constant-size aggregate key for flexible choices of cipher-text set in cloud storage, but the other encrypted files outside the set remain confidential. Secure cryptographic architecture and working methodology are proposed in his paper for optimal services over the cloud".

Muhammad [16] emphasizes that "one of the key points in security is that it could be a perceived risk that can be considered and addressed with right processes in place such as categorizing sensitive data and applying appropriate data masking before transferring the data to cloud computing".

Marinescu [17] agrees that security can be an added issue a computer cloud could be a target-rich environment for malicious individuals and criminal organizations and hence security is a major concern for existing users and for potential new users of cloud computing services.

For data security in a private cloud Kumar [15] proposed a frame work double authentication techniques and specialized procedures that can efficiently protect the data from the owner to the cloud and then to the user.

V. ANALYSIS OF THE SYSTEM

First, the existing system is a cloud service that enables universities access to student result computation system just like using an email service. The student result computation system is available as Software as a Service, it enables subscribing universities utilize the services of the system via the internet using their local browser. Software installation is not required since the result service is hosted in the cloud. It is readily available and can be accessed anywhere. Universities interacting with the result service are not burdened with software license, updates, security patches, backup and a host of other administrative and technical task associated with on premises result systems. The computed result data is encrypted during transmission and before storage in the database using "Advanced Encryption Standard (AES) 256 encryption algorithm. AES is a specification for the encryption of electronic data established by the US National Institute of Standards and Technology in 2001". According to Boxcryptor [15] it was noted that "AES is one of the most commonly used encryption algorithms available today and is used in encryption in governments, banks and high security systems". However the authentication of users relies on the username and password combination. The username and password can be easily broken

A. Analysis of a System with Digital Certificate

In a typical digital certificate system as shown in figure 1 when a message sender sends the message, the first thing that is done is to obtain an encrypted version of the message before sending it out through the communication channel. In order to do this, the original message will have to pass through a hash function; this will produce a hash of the message. The hash is combined with the sender's private key and sent alongside the sender's digital certificate. Upon receiving the message, the recipient validates the certificate accompanying it to be sure its valid, if it is then the receiver goes ahead to compare the encrypted message with the hash that was sent to him, If they are the same then this means the message has not been altered, if they are not then the message has either been altered on transit or the message is not coming from the one who sent it. Normally a slight change in the hash algorithm can change the entire message, so it has a high degree of accuracy.

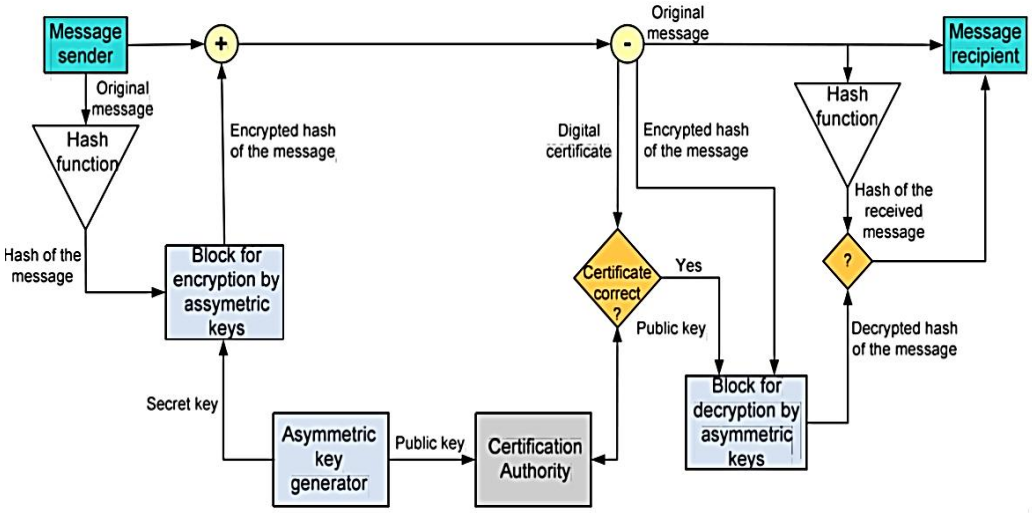

Fig.2: Block Scheme of a System with Digital Certificate (source: Adopted from Kovinić, 2011)

B. Architecture of the Proposed System

Our proposed system makes use of a two form authentication before using digital certificate. A Client and SSL handshake is used for first authentication, then a username and password combination for second authentication. In a typical digital certificate system when a message sender sends the message, the first thing that is done is to obtain an encrypted version of the message before sending it out through the communication channel. In order to do this, the original message will have to pass through a hash function, that will produce a hash of the message. The hash is combined with the sender's private key and sent alongside the sender's digital certificate. Upon receiving the message, the recipient validates the certificate accompanying it to be sure its valid, if it is then the receiver goes ahead to compare the encrypted message with the hash that was sent to him, if they are the same then this means the message has not been altered, if they are not then the message has either been altered on transit or the message is not coming from the one who sent it. Normally a slight change in the hash algorithm can change the entire message, so it has a high degree of accuracy.

In order for a user to be able to initiate a transaction with the Result System, he will be required to registers details with the Certification Authority (CA) and request for a certificate, the CA through a Registration Authority identifies the user and confirms user's qualification to obtain such certificate, after which the certificate can be issued to the User by the CA (The RA does not issue a certificate, but only verifies user identity and makes recommendation to the CA). The level of verification of a user will depend upon the type of certificate the user requests for. The User can now access the result system facilities after installing the digital certificate.

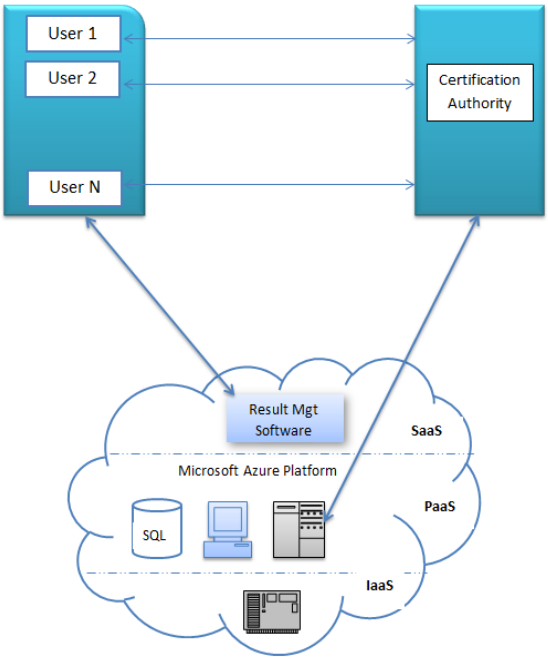

Fig.2: The Proposed System Architecture

VI. DESIGN

Object Oriented Design deals with developingobject-oriented model of a software system to implement the needs that has been recognized. The objects in an object-oriented design are closely associated to the solution to the problem. There may be close relationships between some problem objects and some solutions object, but the designer inevitably has to add new objects and to transform problem objects to bring to effect the possible solution." [18]

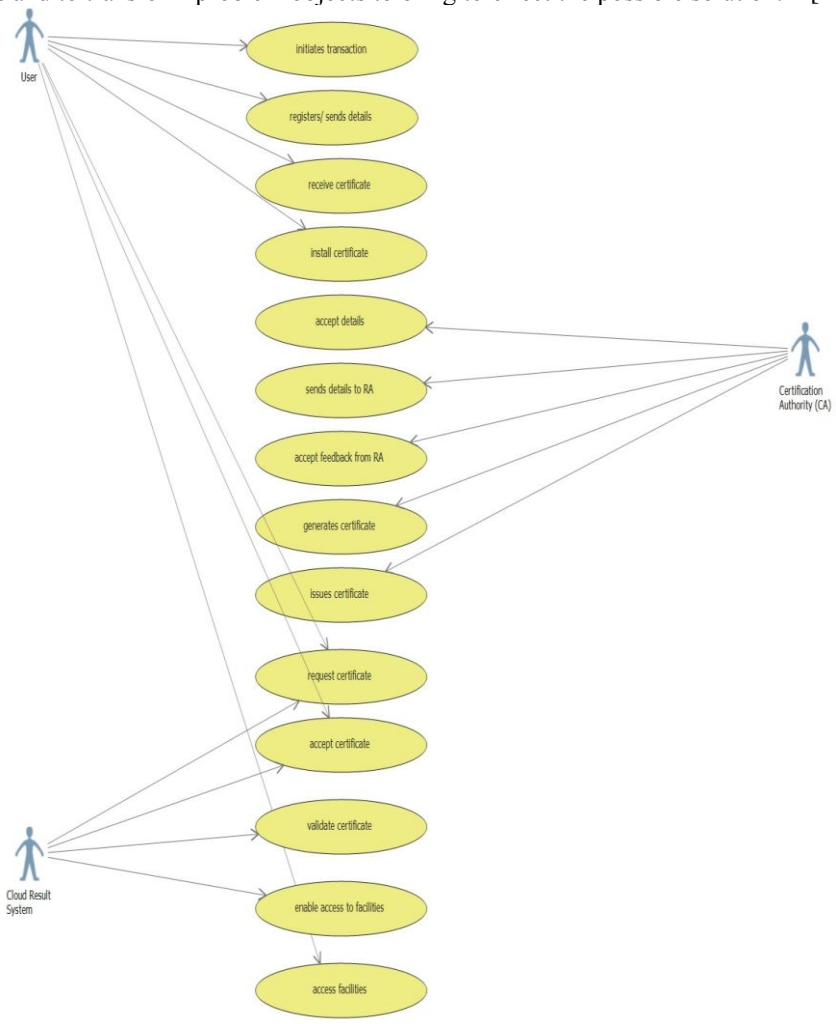

Fig.3: Use Case Diagram of the proposed system

This section contains the architecture and the model of the proposed system with the help of different UML diagrams. We decided to make use of three of them which are the use case, the sequence and the class diagrams.

A. Use Case Diagram of the System

A use case diagram visually explains a possible set of ways users can interact with a particular system. These users are often referred to as the actors. It is used to symbolize the interaction between a person, a system or part of a system and a possible use case. We use lines to connect them in order to show their relationships. The use case diagram of figure 3.2 identifies three actors, the user, certification authority and the result system. The user can initiate a transaction with the result system, register his details in order to obtain a user credential, receive and install certificate after it has been issued by the CA, also the user can request for server certificate upon connection to the result server, accept or decline the certifciate in a case where it is not valid.

B. User Interface Design of the System

The User Interface is a very important part of every application as this is the part the user sees and interacts with.The Model-View-Controller (MVC) design will be applied to the user interface components, specifically the website that allows user to configure the system.The MVC design technique divides the application into three major parts; the model, the view, and the controller. The view subsystem refers to the website interface that displays information to the user. The model subsystem will include the entity objects in the system, and the controller subsystem will process user input and manage the model. Using MVC decouples the access to data from the presented data.

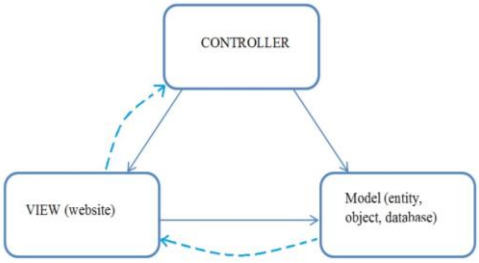

Fig. 4: Model View Controller Architecture

VII. TOOL FOR IMPLEMENTATION OF THE SYSTEM

The application implemented in this work is a cloud-based result security system which makes use of digital certificate for client and server authentication, access to the site is secured using SSL which is an essential technique for securing website today. Username and password combination is used as a second form of authentication. The passwords and data are encrypted during transmission and before storage in the cloud data center using SHA-2 encryption algorithm. The User Interface is developed using Model View Controller to control user access to various aspects of the application and conceal irrelevant details from users. The application offers a secured and cost effective method to the management of students' results.

The software application has three main sections, namely: the students, university and guest. Students can log in and do their student registrations, course registration, view their courses and view their results through the students section. Lecturers can log in to view course allocation and upload student scores. Guests can log in to make enquiries. The login window requests a registered user credential which is used to authenticate user before a user role can be assigned.

The application was developed using Microsoft Visual Studio Ultimate 2013 IDE with Azure SDK installed. Built on ASP.NET MVC using Telerik Kendo UI, Microsoft SQL Server, JavaScript, HTML, and CSS on a local computer as a web application, the project was initially debugged and tested on the local machine before it was migrated to Microsoft Azure platform. This was done by creating an account with Microsoft Azure. The storage, servers and database required for the running of the application were configured on the cloud before migration. The service runs and stores its data in Microsoft datacenters.

VII. CONCLUSION

In this paper a security technique for result system protection was successfully developed using digital certificates. The certificates and application were tested both offline and in the cloud and were working fine. The research demonstrates the use and adoptability of digital certificate in the cloud which makes it more convincing for potential subscribers to use the cloud platform for their result management and other business services. Universities subscribing to this software are assured of the security of their connections and data in the server.

ACKNOWLEDGMENT

The Department of Computer Science Board Chairman Dr. P. O. Asagba is acknowledged for his effort at making sure that the research proceeded as anticipated in the department within the period of the first presentation. The support of the Head of Department Dr B. O. Eke is also acknowledged for directing and offering training that assisted the implementation stage of this work. Engr. Okereke Emeka is also acknowledged for constantly reminding the supervisor of the need to read and correct the work.

REFERENCES

[1] Chase, N. (2014). Understanding the Cloud and Building Your Own Infrastructure-As-A-Service. Cloud Platform Research Report, DZone. 15, 16.

[2] NIST (2011). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145.1-3.

[3] Obunadike, G., Tyokyaa, R. and Umeh, A., (2014). A Phase Approach for Adopting Private Clouds as a Collaborative Platform for Nigerian Universities.Information and Knowledge Management.www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol.4, No.9.

[4] Labourey, S. (2014).CloudBees: 4 Key Things You Should Know About Platform-as-a-Service. Dzone Research - The 2014 Cloud Platform Research Report.

[5] William S. (2016) How to Choose a DBaaS, DZone Guide to Data Persistence, DZone USA

[6] IBM (2012). Applying the cloud in education: An innovative approach to IT.White Paper by International Business Machine, 3- 7

[7] Sclater, N. (2010). Cloud Computing in Education, Policy Brief.UNESCO Institute for Information Technologies in Education, Russian Federation, Moscow, 2010. 3-5

[8] Crucial Cloud Hosting, (2014). Cloud Computing in Education: Introducing Classroom Innovation. Whitepaper by http://www.crucial.com.au.2-7.

[9] Ahmad, N. and Habib, K. (2010).Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution.Blekinge Institute of Technology. 41-50

[10] Entrust (2007). Understanding Digital Certificates & Secure Sockets Layer: A Fundamental Requirement for Internet Transactions. 'Author'.4.

[11] Evgeny, M. (2014). Investigation of Digital Certificates: Creation of self-signed certificate on Windows 8. 3-5

[12] Eklund, J. (2010). A Workflow Based Architecture for Public Key Infrastructure: Improvements to an existing open source Certified Authority application. ISSN-1653-5715. 2-5

[13] Bhiogade, M. (2002). Secure Socket Layer. National institute of technology, rourkela. Informing Science InSITE.

[14] Hashem, M., Hoque, S., Kar T., and Nafi, K. (2012).A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture. International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 181-186.

[15] Kumar, N. (2015). Cryptography during Data Sharing and Accessing Over Cloud, International Transaction of Electrical and Computer Engineers System, Vol. 3, No. 1, 12-18 Available online at http://pubs.sciepub.com/iteces/3/1/2 © Science and Education Publishing.12-17.

[16] Muhammad, A. (2013). Perspectives and Reflections on Cloud Computing and Internet Technologies. www.acm.org. NordiCloud. 2-3 Oslo, Norway.

[17] Marinescu, D.C. (2013). Cloud Computing: Theory and Practice. 273, 278

[18] Somerville, I. (2007). Software engineering, eight edition; Addison Wesley; England.207-285

