A Novel Framework to Improve Secure Digital Library at Cloud Environment

Heba Sayed
Hesham N. Elmahdy
Fathy Amer
Faculty of Computers and Information,
Cairo University

Sherif Shaheen
Faculty of Arts

hobasyd@gmail.com
ehesham@fci-cu.edu.eg
dr_fathi_amer@yahoo.com
s_shaheen@cu.edu.eg

Abstract - **Cloud computing is an advanced computing technology used by different organization or individuals for transferring, overseeing and storing over the internet. Security is an important issue that needs to be studied deeply and accurately when designing the digital library. Security shortcomings in libraries, combined with assaults or different sorts of disappointments, can prompt private data being improperly gotten to, or loss of honesty and integrity of the information put away. This paper will be introduced the concept and characteristics of cloud computing, the relationship between cloud computing and digital library will be analysis, the cloud computing security management problems under the environment of digital libraries will be studied , the availability level will be taken into research consideration while studying security management problems in digital library cloud computing. The main goal will be trying to present a possible solution for the preventing security threats and hackers on a digital library management system based on cloud computing.**

Keywords-Cloud computing, Security, Digital library, Confidentiality, Availability, Integrity, Security threats.

I. Introduction

Cloud computing is a sophisticated technology designed to transfer processing and storage space that belongs to the computer to giant servers and then accessed through the Internet, Cloud computing has risen and emerged as a wonderful choice and better than traditional computing. It enables users to gain access to huge computing resources in an economical and efficient fashion. There are several cloud computing services and storage that offered by general storage provider companies, such as google apps services and amazon web services. A digital library can be defined as a technology for storing the knowledge and preserving data from loss to get it when needed, this data or knowledge can be found on different such as books, thesis, research documents, articles, audio and video. A digital library can give access to huge numbers of the information that is organized in the network over the world, which is an essential segment of any research experience.

By utilizing cloud technologies, library administrations can be made online without stressing over right versions of stages or the underlying technology. The proposed system aims to give multilevel security to the information over cloud, trying to provide an algorithm work against various attacks. So, we try to give a possible solution for the preventing security threats and hackers on digital library at cloud computing. The proposed Model used to design the digital library is the DELOS Reference Model. This model has 6 main components: the user, the content, the functionality, the architecture, the quality, and the policy [1]. The utility of this model is to offer a way to define digital libraries for DL designers.

A. Problem Statements

The digital library in the cloud computing environment faces the problem of data storage security, user information privacy and personal rights management, cloud data resource rights, The increasing volume of intellectual production and the diversity of its subject, and sources caused many problems which face researchers and information institutions, the most highlight of these problems are those related to give storage space for information, and variety of style treatments. In addition, problems related to information flow and the methods to be transmitted over the network without any loss of data, so security is an essential issue in digital library design. There are three factors that should be considered in the proposed work when constructing the security model for the digital library, they are confidentiality, integrity and availability.
Vulnerability in the safety system causes a weakness on the security system; these vulnerabilities are exploited to penetrate the security system by a threatened person who can perform unauthorized actions within the building cloud security system, by entering it in an unauthorized account or manner.
This research aims to develop techniques for building secure and scalable digital library systems based on cloud technology to serve large number of users by enhancing the cloud based services, library services and resources.

B. Motivation

The growing need for digital libraries to manage large amounts of data, these data need to be secured, so the security weaknesses must be studied carefully. As indicated by an investigation by the Oracle Corporation [2].information volumes are developing at 40% every year and by 2020 it will have developed to multiple times of its size in 2009. On the other hand, cloud computing promises the possibility for unlimited scalability. Also, the benefit of the cloud is that because of its ability to provision services on-demand, this is very important reasons. Security is an essential issue in digital library design because of various attacks.

Security vulnerabilities in digital libraries [3], suffering from types of attacks that can lead the failure on the library system; it can lead inappropriately access to confidential information. These [3] thus can amazingly affect the trust of the publishers or other content providers.

II. LITERATURE SURVEY

Cloud computing security challenges have been widely researched, Lingling Han [4] gave a new advanced library stage used to tackle the issue of library resources putting away and sharing to give quick, protected, helpful and proficient administrations to clients. Goyal [5] characterized the advantages and examinations of cloud computing administrations on the parameters of valuing, most extreme point of confining, information security, and information reinforcement. Qingjie MENG [6] defined cloud computing method of library computerized assets , cloud key appropriation plan to adjust to library applications was displayed, the improved customary PKI, the PKI-based distributed computing correspondence and security assurance components for the library are presented. Library distributed computing key dissemination, confirmation and encryption strategies, increasingly secure homomorphic encryption component for library data recovery. Surendra [7] talk about the Cloud Computing in libraries, how make viable library benefits of distributed computing, Issues, Challenges and Benefits of distributed computing. Varun [8] delineated a concise portrayal of what precisely cloud computing security-related issues are, and talks about information security and security assurance issues related to cloud computing over all phases of information life cycle. Demonstrating, the current answers for information security and protection assurance issues in the cloud. What's more, depicts future research work. Guo Xin [9] dissected the idea of cloud computing and related innovation, presented the necessities of the development of computerized library, talked about how to plan the engineering of Digital Library Based on distributed computing. Dev Ras [10] described the architecture of cloud computing to building and managing libraries, tried to make progress current user service model in the university library by using Cloud Computing. Tamanna [11] proposed a procedure for information classification in cloud condition, concentrated on describing the information considering the security essentials of the data that separates the information into basic, confidential and highly confidential utilizing improved machine learning calculation. Nabeil Eltayieb et al [12] presented an attribute based secure information sharing (ASDS) conspire for cloud condition, which gives information access control, confidentiality, information validation, and adaptable client denial. Also, the proposed plan can oppose intrigue attack and replay assault. The examination of security properties and the correlation execution with other information sharing plans have exhibited that ASDS is truly reasonable for cloud condition.

III. **T**ECHNOLOGY DESCRIPTION

The goal of this section is to go through the definition and benefits of cloud computing, then illustrated the security problems of digital library under the environment of cloud computing , finally studying different security threats that affect cloud computing.

A. Cloud Computing Definition

There are many definitions of cloud computing, one of these definitions refer to NIST that define the cloud computing as " Distributed computing is a model for empowering helpful, on-request arrange access to a common pool of configurable figuring assets (e.g., systems, servers, stockpiling, applications, and administrations) that can be quickly provisioned and discharged with insignificant administration exertion or specialist organization cooperation, this definition is the most broadly used [8].

B. Benefits of Cloud Technology

The benefits of Cloud Computing are that it offers colossal measures of power regarding figuring and capacity while offering improved scalability and flexibility. In addition, with effectiveness and financial matters of scale, Cloud technology administrations are getting to be a less expensive arrangement [13].

On-demand self- service, Autonomous System, Scalability and flexibility, and , shared resources are some of the essential characteristics of cloud computing that separates it from each other technologies[13][14].

C. Cloud Computing Security Management Problems for Digital Library

The motivation behind the digital Library Management framework is to take into account putting away subtleties of an expansive number of books, magazines, Journals and theory. Therefore, there are some great issues that need to be referenced when allowing moving sensitive data and application to the public cloud environment. Most of organizations prefer to use cloud computing, but it still suffers from some weaknesses.

D. Threats of Cloud Computing

There are some security threats that have an effect on a cloud computing, this research will be mention some of these threats and then covered some of them:

- Data Loss: Data loss can have large effects monetarily, operationally and even lawfully as data loss may result in the inability to meet consistence strategies or information security prerequisites.

- Data Ownership & Control: Moving to the cloud implies that the service provider or organization could have some level of access to your information.

- Data Breaches: Data breach threats exists whether data is stored internally or on the cloud, some cloud administrations might be increasingly vulnerable against potential attacks and the hijacking of information because of new strategies for assault.
- Malicious Attacks & Abuse: hackers or even approved clients may conceivably assault and abuse cloud storage for illicit exercises. Examples of malicious threats include:-
  a. standard specifications
  b. Insider breaches and hacks
  c. Theft of proprietary data or intellectual property
  d. Industrial espionage or IT sabotage
  e. Fraud
  f. Improper disposal of documents or leaving doors unlocked.

- Insider Threat: Insider threat comes from people within the organization; This can lead to the misuse of important data Insiders are frequently familiar with the association's information and intellectual property as well as the techniques that are set up to ensure them.

- Unauthorized Access: Unauthorized access could be happened when someone tries to reach to a website or an area of a system by using someone else's account or other methods. For example, if somebody kept easy to guess password Some framework managers set up alarms to tell them when there is an unauthorized get to endeavor, with the goal that they may explore the reason. These cautions can help prevent hackers from accessing a safe or private framework. Many secure frameworks may likewise bolt a record that has had too many fizzled login endeavors.

- Distributed Denial of Service Attacks (DDOS): is attacked by dumping sites with a torrent of unnecessary data is sent via infected devices and with the wide spread of the Internet Denial of service has become more exciting for hackers.

IV. MODEL AND DESIGN FOR DIGITAL LIBRARY

The new security design of the digital library system must contain at least one addition to previously designing systems. Proposed design model that will be introduced on digital library is a DELOS Reference Model that has 6 main components in a digital library: content, user, functionality, architecture, quality, and policy. We introduce the security issue of the two layers of this model: the user and the content security issue. The utility of this model is to provide a way to define digital libraries for DL designers. In this section, the following question will be studied: What are the security issues that need to be measured to secure the digital library?

A. Proposed Model

The proposed system aims to give multilevel security to the information which is flowing over the cloud, also provides a degree resistance against various attacks. So, this research will present a possible solution for preventing security threats and possible vulnerabilities on a digital library system at cloud computing platform

- The covered threats are:
  1 Unauthorized access

2. Session hijacking attack
3. Denial of service attack (DDOS)
4. Cross-site Scripting (XSS)
5. Blocking Brute Force Attacks
6. SQL Injection
7. Device Cookies.

All Covered Threats are dealing with public cloud on platform as a service model.

- The security Level will be covered:
  1. Three layer to log in
  2. Hide admin login page
  3. Password Authentication Delay
  4. Using CAPTCHAS
  5. Verification code
  6. Alternate XSS Syntax
  7. XSS using code encoding
  8. XSS using Script via Encoded URI Schemes

Figure 1 describe the details of the proposed model, in this figure apply the security threats on digital library in the three cases : Admin account, user account, database account under the Public cloud environment on platform as a service model

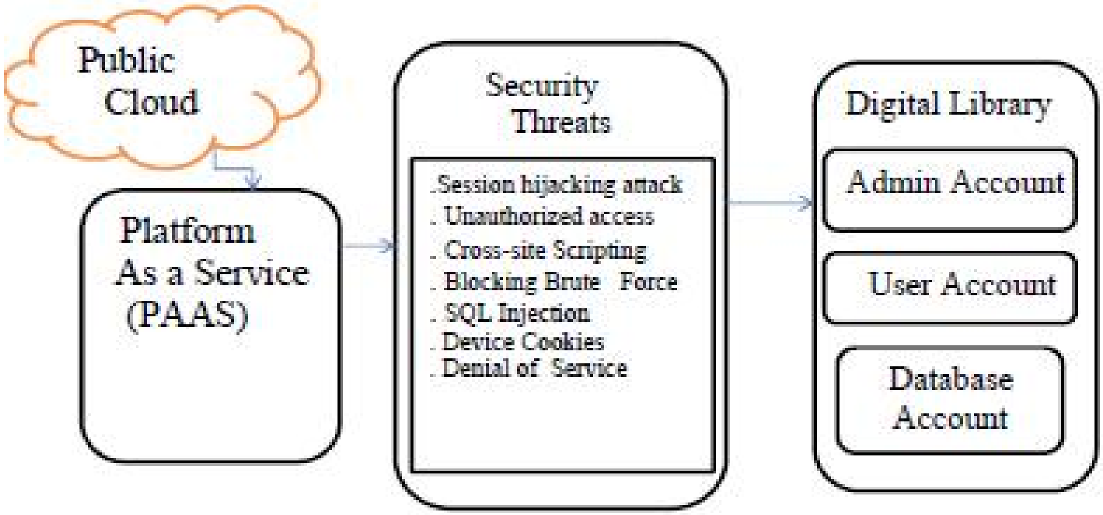


Figure1 : Proposed Model

Knowing that , the cloud library management system was implemented according to the standard specifications in PHP, html, Apahe server and Mysql by using Xampp server.

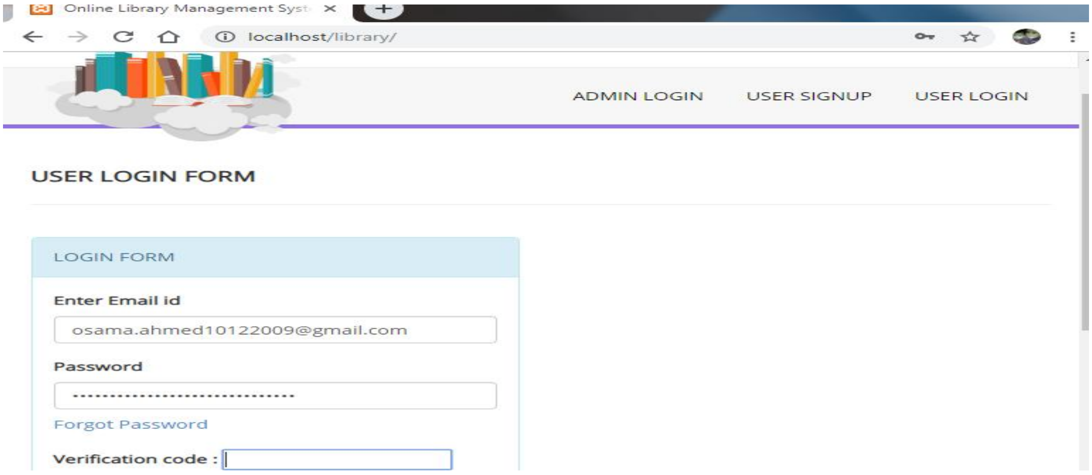
V. EXPERIMENTS AND RESULTS

According to DELOS Reference model, there are two security requirements for accessing the contents of the digital library:

Firstly : - the authentication: the end user must register to the system first to have an ability to log on to the library framework.

Secondly: - the confidentiality: Preventing unauthorized access to the data by encrypting the content using encryption algorithm.

The proposed frameworks for online digital library system under the environment of cloud computing are shown in figure 2 , 3 and 4. The figure 2 shows the home page for cloud library system, on this page we can go to the rest of the pages after registration and after achieving security metrics "confidentiality, integrity, availability", After using Bluehost account to reserve space on the cloud.



USER LOGIN FORM

LOGIN FORM

Enter Email id

osama.ahmed10122009@gmail.com

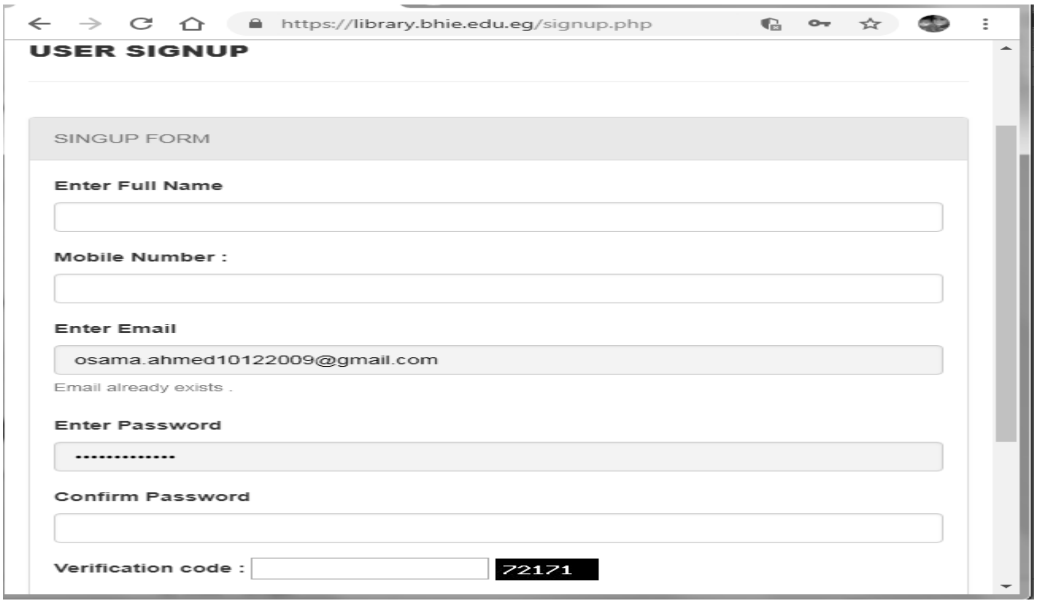
Password

••••••••••••••••••••••••••••••

Forgot Password

Verification code :

Figure 2: Framework for Cloud Library Management System



USER SIGNUP

SINGUP FORM

Enter Full Name

Mobile Number :

Enter Email

osama.ahmed10122009@gmail.com

Email already exists .

Enter Password

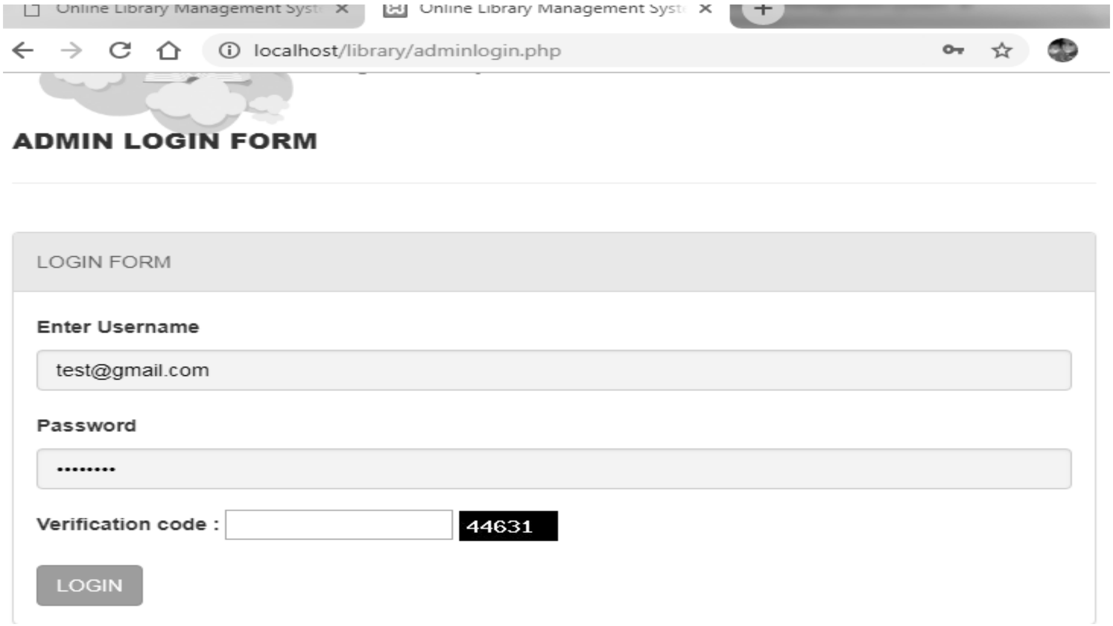
•••••••••••••

Confirm Password

Verification code : 72171

Figure3: Registration Page for Cloud Library System after Applying Security Threats

In the figure3, if the end user tries to go to admin page, he will get this message "Invalid Details", This is one of achieving the security requirements to prevent attackers Penetrates the library system**.** The admin has the authority to add, update and delete categories, books and authors.


Online Library Management Syst
Online Library Management Syst
localhost/library/adminlogin.php
LOGIN

ADMIN LOGIN FORM

LOGIN FORM

Enter Username

test@gmail.com

Password

••••••••

Verification code : 44631

Figure 4: Admin Login Page (end user or hackers cannot go to admin page)

This approach is differed from other approaches because it is a new idea to measure and evaluate a security of online digital library system using quantitatively metrics to decide the advantages of proposed algorithm. Each of this security metrics has threats that are affected on it. To achieve the integrity metric, we can prevent unauthorized access to make change, deletion or addition of the data saving on cloud library by using three layered to login.
The results of the experiment are shown in figure5 and figure6.

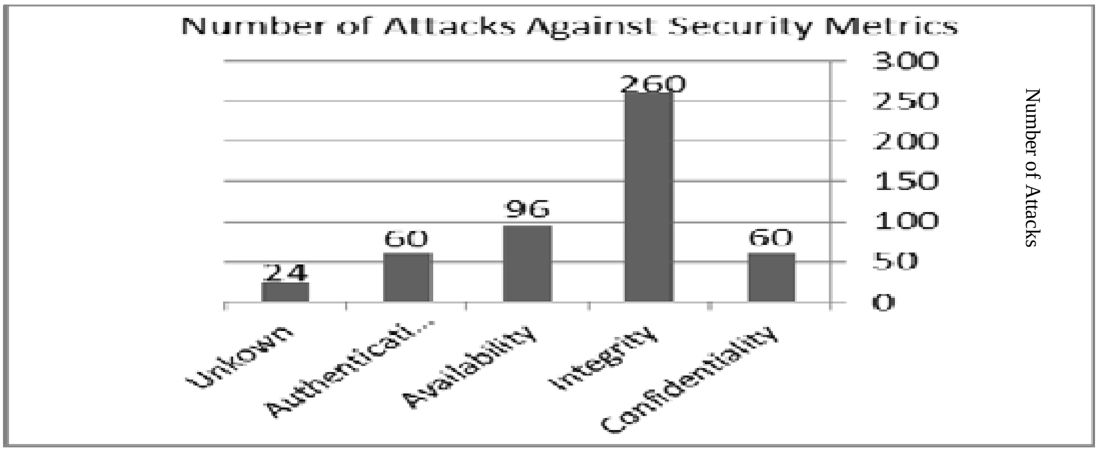


Figure 5: Security Evaluation

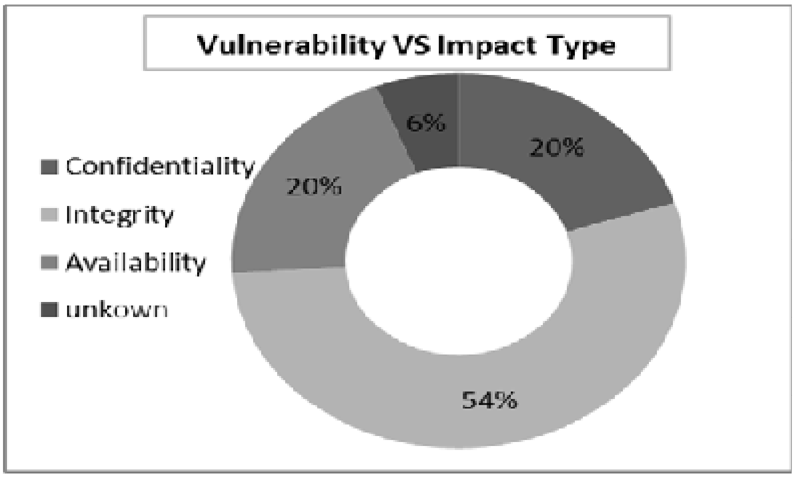


Figure6: Vulnerability VS Impact Type

In these two last figures, threats to integrity are the highest one, so the integrity is on the risk. According to the above results, to apply more security for cloud data storage and solving the problem of integrity, making these steps:-

- Always encrypting sensitive data.
- Taking the necessary preventative measures to ensure your systems, networks and applications are secure.
- Taking a backup of the data, continuously.
- Using multiple layers to log into the system of cloud library to prevent unauthorized access
- Using protection technology on the integrity such as watermarks, digital signatures, finger prints
- To achieve authentication and integrity, using remote desktop to grantee that the admin did not work from home.

VI. **C**OMPARISON ANALYSIS

In this section, various approaches for constructing secure digital library illustrated on table1. The comparison analysis between the existing approaches and our scheme in terms of security metrics are illustrated on table2.

TABLE I

Comparison between different digital library models

Digital library model	Objective	Techniques used	Benefits	Cloud model
lpoulo_2013, Cloud Computing for Digital Libraries[15]	Achieved secured data on public cloud	AWS using java to develop typical digital library services	Save time, money, High scalability	IaaS, Public cloud
Martine Bellaïche,Security in cloud computing [16]	Deploying a secure application on AWS	AWS Using simulation such Cloudsim	enhance the energy saving capabilities	IaaS,
Elsherbiny2011	scalable and flexible	5SL Model to generate DL	Generation of DL using 5SL	Did not consider , but PaaS can be used
Online DL Mangement system, (new proposed)	Multi- level To achieve confidentiality, integrity, availability	Online Digital library framework using DELOS Model using Bluehost account	Easy to test application, cost effective	PaaS, Public cloud

TABLE II
Comparison between proposed scheme and other existing scheme in terms of security metrics

scheme	Security Achievement	Confidentiality	Integrity	Availability	Approach used
Elsherbiny2011, "Secure Digital Library"	Medium, using 5S scheme	Achieved using different security mechanism on each 5SL	Considered on streams, structures, societies.	Considered on Scenarios model using different security mechanism such as firewall	5SL Model, there are security attacks for each model.
Kulwinder Kaur et al. 2016 [17]	Medium, using classification of data to secure sensitive data	Classifying the data into confidential & non confidential	Using hashing approach to achieve integrity	Mentioned but not considered	Data classification using machine learning algorithm
Anupama 2017 [18]	High	Replicated the data among different cloud	Using Hash based message authentication	Data stores on multiple cloud	Data replication
Eltayieb et al.2019 [12]	Achieve: access control, data confidentiality, authentication, integrity, and flexible revocation	manager encrypts data before sending to the cloud	Mentioned but not studied	Mentioned but not studied	New scheme attribute-based secure data sharing (ASDS)
Our scheme	Highly, more security Achieved: confidentiality, integrity, High availability level	Using hybrid security algorithm to prevent unauthorized person to access data	Using hashing function, different protection technology to prevent modification	Achieved on "architecture" using replication to solve the problem of DOS attack	DELOS Reference Model, Multiple layers of security plus encrypted sensitive data to prevent security threats

VII. Conclusions

The motivation behind the library management framework is to take into consideration putting away subtleties of an expansive number of books, magazines, Journals, postulation and take into account include, seek, get, return offices independently to head/Librarian, staff and students.

This research has been studied cloud computing security management problems and apply it on online digital library framework to make it secure. Cloud computing is the innovation of present and future, To carry out new encryption and decryption technique for overcoming the hackers and intruders knowledge to give protect to the cloud storage data on digital library, we proposed the DELOS Reference Model for digital library, this model has 6 main definitions, each of these definition needs some security requirements. There are three factors that should be considered in the proposed work when constructing the security model for the digital library, they are confidentiality, integrity and availability.

The proposed system aims to give multilevel security to the information over cloud, and trying to provide an algorithm works against various attacks. So, we presented a possible solution for the preventing security threats and hackers on digital library at cloud computing.

In the future, it is possible to expand digital library work on the cloud by more studying of scalability of stored data, and it may be able to store a larger amounts of data. On the other hand, it is possible to Served large number of users by enhancing the cloud based services, library services and resources by using any simulation techniques such as Cloudsim simulator.

References

[1] Candela, L., et al. *The DELOS Digital Library Reference Model*. 2007 http://www.delos.info/index.php?option=com_content&task=view&id=3 45

[2] Dijcks, J.-P. Oracle: Big Data for the Enterprise. Oracle White Paper, 2012.

[3] Edward Fox and Noha ElSherbiny (2011). Security and Digital Libraries, Digital Libraries - Methods and Applications, Dr. Kuo Hung Huang (Ed.), ISBN: 978-953-307-203-6, InTech, Available from: http://www.intechopen.com/books/digital-libraries-methods-and-applications/security-and-digital-libraries

[4] Lingling Han and Lijie Wang, "Research on Digital Library Platform Based on Cloud Computing ", pp. 176–180, 2011.

[5] Goyal, S. (2012). A comparative study of cloud computing service providers. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(2), 1-5.

[6] Qingjie MENG, Changqing GONG , "Research of cloud computing security in digital library" ,6th International Conference on Information Management, pp:41- 44 , 2013.

[7] Surendra Kumar Pal,"Cloud Computing and Library Services:Challenge & Issues" , September 2014.

[8] Varun Krishna Veeramachaneni, "Security Issues and countermeasures on Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 4, Issue 5, pp:82-93, September 2015.

[9] Guo Xin, "Analysis of Key Technologies of Digital Library Based on Cloud Computing" , International Conference on Education , pp 695 - 698, 2016.

[10] Dev Ras Pandey, Gauri Shanker Kushwaha, "Cloud Computing for Digital Libraries in Universities", International Journal of Computer Science and Information Technologies, Vol. 6 (4) ,pp: 3885-3889, 2015.

[11] Tamanna, Rajeev Kumar, " Secure Cloud Model using Classification and Cryptography" , International Journal of Computer Applications, Volume 159 – No 6, February 2017.

[12] Eltayieb N, Wang P, Hassan A, Elhabob R, Li F. ASDS: Attribute-based secure data sharing scheme for reliable cloud environment. *Security and Privacy* 2019;2:e57. https://doi.org/10.1002/spy2.57

[13] Shawish, A. and Salama, M. (2014) Cloud Computing: Paradigms. Inter-Cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, Springer-Verlag, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35016-0_2

[14] L. Wang, and G. Laszewski, “Scientific Cloud Computing: Early Definition and Experience,” in Proc. 2008 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, 2008, pp. 825 – 830

[15] L.Poulo, "Cloud Computing for Digital Libraries", Department of Computer Science University of Cape Town, 2013.

[16] Martine Bellaïche, "Security in cloud computing", Polytechnic University of Catalonia, 2016.

[17] Kulwinder Kaur, Vikas Zandu , "A Secure Data Classification Model for achieving Data Confidentiality and Integrity in Cloud Environment", International Journal on Computer Science and Engineering, Vol. 8 No.9, Sep 2016.

[18] Anupama Prasanth, " Cloud Computing: Secure and Scalable Data Access Security Models", International Journal of Computer Applications, Volume 170 – No.4, July 2017