Ensuring Data Governace and Enhancing Data Security in a Private Cloud Environment

Conference Paper · November 2018

DOI: 10.1109/IEMCON.2018.8615066

6 authors, including:

Happy Nkanta Monday
Oxford Brookes College of Chengdu University of Technology
50 PUBLICATIONS **574** CITATIONS

SEE PROFILE

Chiagoziem Chima Ukwuoma
University of Electronic Science and Technology of China
61 PUBLICATIONS **556** CITATIONS

SEE PROFILE

Grace U. Nneji
Oxford Brookes College of Chengdu University of Technology
48 PUBLICATIONS **447** CITATIONS

SEE PROFILE

Ensuring Data Governace and Enhancing Data Security in a Private Cloud Environment

Happy N. Monday
School of Computer Science and Technology
University of Electronic Science and Technology of China
Chengdu, China
mh.nkanta@gmail.com

Jian P. Li
School of Computer Science and Technology
University of Electronic Science and Technology of China
Chengdu, China
jpli2222@uestc.edu.cn

Grace U. Nneji
School of Information and Software Engineering
University of Electronic Science and Technology of China
Chengdu, China
ugochinneji@gmail.com

Chiagoziem C. Ukwuoma
School of Information and Software Engineering
University of Electronic Science and Technology of China
Chengdu, China
chiagoziemchima@gmail.com

David Agomuo
Department of Computer Science
School of Physical Sciences
Federal University of Technology, Owerri
Imo State, Nigeria
agomuodavid@gmail.com

Richard I. Nneji
Department of Chemical Engineering
School of Engineering
University of Lagos, Akoka
Lagos State, Nigeria
richardnneji89@gmail.com

***Abstract*—this paper proposes a new system of ensuring data governance and enhancing data security in private cloud environment. Security and Privacy concerns have been the major drawbacks in cloud computing environments. Security, reliability and privacy enhance users' flexibility in file accessibility. As easy-to-use cloud services penetrate personal computing, users expect to enjoy the same conveniences they have at home in the office. This paper proposes a workable security technique in a cloud computing environment that delivers Infrastructure as a Service (SaaS), and deployed in a Private Cloud to protect data and information stored and shared from potential intrusion, threats, theft, virus, and agents. This paper proposes a system that focuses on data encryption and CAPTCHA methods as regards to security solutions. This paper adopted the Structured Systems Analysis and Design Method (SSADM) for the development, and implementation of the new system. Java play framework is adopted for the implementation of the web based system. The database structure is handled be employing MySQL. The system was implemented and tested using the various test cases which were successful. The test result shows that the proposed method is efficient in data confidentiality, integrity and availability.**

Keywords—Data security, cloud computing, data integrity and accessibility, private cloud, data governance

I. INTRODUCTION

The widespread use of Internet-connected systems and distributed applications has triggered a revolution towards the adoption of pervasive and ubiquitous cloud computing [1]. Cloud storage and Cloud collaboration bring together new advances in cloud computing and collaboration that are becoming more and more necessary in firms operating in an increasingly globalized world [2]. Storing data offsite in the cloud makes it accessible from anywhere without the hassle of maintaining your own local storage and file serving systems [3]-[4]. The ability to backup files, store them in the cloud, and automatically synchronize all that data across multiple devices has radically changed the way we use computers, mobile phones, and other internet-connected devices [5]-[6]. However, cloud computing poses risks related to data security in its different aspects (accessibility, integrity, confidentiality and authenticity) [7]-[8]. As with any storage system, there are certain security properties that are desirable in a cloud storage system: confidentiality, integrity, write-serialize and read freshness [9]. These properties ensure that user's data is always secure and cannot be accessed by unauthorized users and the data is always at the latest versions when being retrieved by the user [10]. Since the adoption of the cloud computing paradigm by IBM Corporation around the end of 2007, other companies such as Google (Google App Engine), Amazon (Amazon Web Services (AWS), EC2 (Elastic Compute Cloud), etc. have progressively embraced it and introduced their own new products based on cloud computing technology [11]-[12].The paper presents a workable security technique in a Cloud Computing environment that delivers SaaS, deployed in a Private Cloud to protect data and information, stored and shared from potential intrusion, threats, theft, virus, and agents[13]. This Paper focused on data encryption and CAPTCHA methods as regards to security solutions. The security covers the following areas: confidentiality, integrity and availability.

In this paper reviews the main cloud computing architecture patterns, a summary of its main features, deployment models and identify the main issues related to security, privacy, trust and availability.

A. Case Study of Cloud Computing Model

Cloud computing is a general term for anything that involves delivering hosted services over the internet [3]. Figure 1 shows the general model of cloud computing.

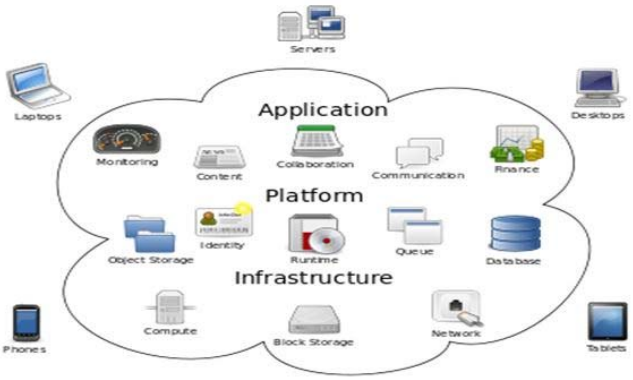

Fig. 1. Cloud computing model

978-1-5386-7266-2/18/$31.00 ©2018 IEEE

B. Cloud Computing Architecture

Cloud computing architecture is based on layers [4]. Each layer deals with a particular aspect of making application resources available as shown in figure 2 below.

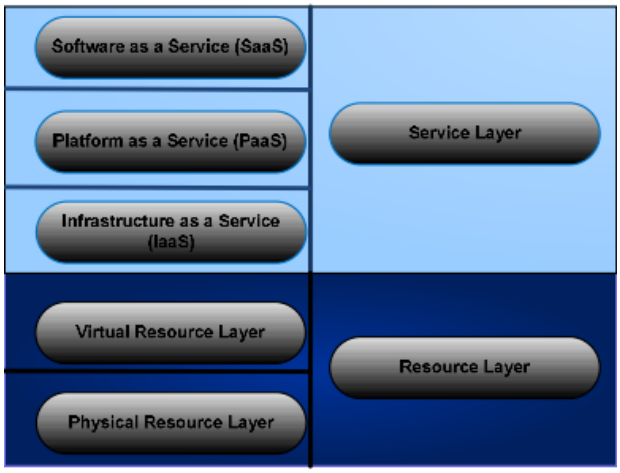

Fig. 2. Cloud computing architecture

II. Analysis of the Existing System

Over the last few years, there has been a drastic change in Information Technology. This includes the various ways in which files can be shared and stored. In the past years, several information sharing tools have been developed for policy-based information sharing. Storing important data with cloud providers comes with serious security risks. This may happen due to bugs, crashes, operator errors, or misconfigurations. Google Drive is used as a case study in this paper. It is an example of cloud application hence; before anyone can use it, the person needs to register. Once registered, a free 5GB will be issued and the application is installed automatically on the PC.

A. Disadvantages of the Existing System

In public cloud computing scenario, such as that of Google Drive, there are multiple security issues that need to be addressed in comparison to a private cloud computing scenario.

- When data is distributed it is stored at more locations increasing the risk of unauthorized physical access to the data.
- By sharing storage and networks with many other users, it is possible for other customers to access your data. Sometimes because of erroneous actions, faulty equipment, a bug or criminal intent. This risk applies to all types of storage and not only cloud storage.
- You can't install Google drive on a public or shared pc because anyone can have access to your private files.

Because of these multifarious security issues in a public cloud (Google Drive), the adoption of a private cloud solution is more secure and aims to address the most important security concepts; confidentiality, availability and integrity, in cloud computing.

III. Analysis of the Proposed System

The proposed cloud-based file sharing system adopts the SaaS service model which is deployed in a private cloud. It is designed practically for uploading, deleting, sharing and retrieving file/data/information safe and restriction to other users. It provides a user authentication name and password and also encrypts the file name of each data thereby restricting hackers from penetrating data. The proposed system is expected to provide a better security to the existing system as follows;

- For confidentiality, the use of encryption technology to encrypt files en route and at rest. Encryption in transit protects data as it is being transmitted to and from the cloud service. Encryption at rest protects data that is stored at the service provider. Hence, personal information may be better protected in the cloud.
- For Security, Authentication Processes requires creating a user name and password that grants you access into the site-can keep hackers out of users' accounts, but only if users actually vary their passwords.
- Simplicity and ease of use, thereby supporting only few operations, in order to simplify computation.
- Authorization practices by listing out authorized clients, who can access data stored on cloud system.
- Easy accessibility of information through File searching and filtering.
- Provision of Virus scanning extension.

A. Use case Scenario of the Proposed System

A use case is a methodology used in system analysis to identify, classify and organize system requirements. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal as shown in figure 4.

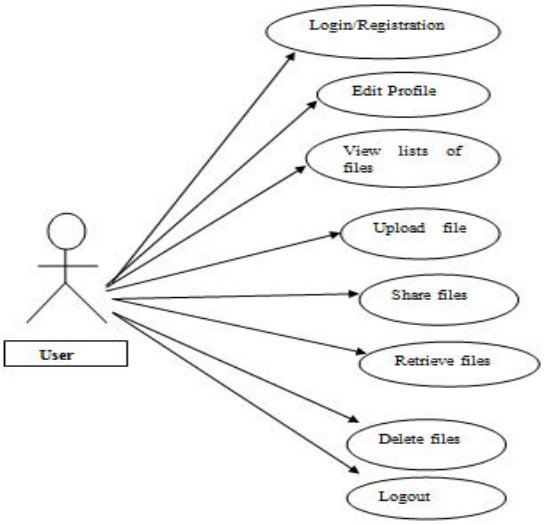

Fig. 3. Use case diagram for the proposed system

B. Entity Relationship Diagram of the Proposed System

This diagram shows how the various entities in the hierarchical model can be related. An entity-relationship model is a systematic way of describing and defining a business process. The process is modeled as components (entities) that are linked with each other by relationships that express the dependencies and requirements between them.

The relationships that can exist between these entities are as follow:

- One –to –one relationship
- Many –to –one relationship
- One –to –many relationship
- Many –to –many relationship

The binary relationships that can exist between the entities using Chen's notation are illustrated as follows;

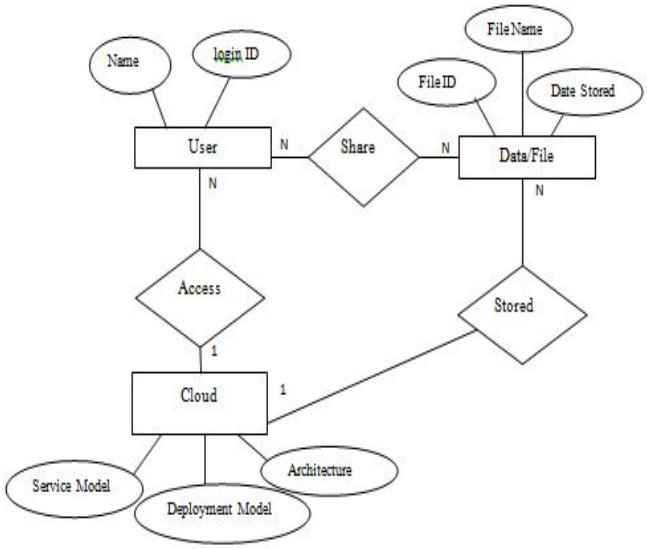

Fig. 4. Relationship between entities in the proposed system

C. Data Sharing Security of the Proposed System

Providing protection (Read, Write, and Append) to a file or group of files such that unauthorized users will not access the files defines file security. Since the problem of file security arises from the desire to share file amongst cloud users in a cloud-based file Sharing environment, the owner of the file chooses or specifies users with whom files are to be shared. In addition, the type of file Access Right to be allowed is specified.

IV. Advantages of the Proposed System

- Its cloud-based file sharing reduces costs, simplifies storage management and reduces risk as data can be centrally managed and protected.
- Users will no longer have the fear of losing their data to hackers, virus and unauthorized users because file names are encrypted.
- Risk of unauthorized access to data can be mitigated through the use of encryption, which can be applied to data as part of the storage service.
- It generates an action key so that users cannot see each other's files.
- No two file names are repeated which is critical to the integrity of the data and the success of any cloud based file sharing initiative.
- Improved user productivity and collaboration as data is readily accessible regardless of where the end users are located.
- Scalability means that the proposed system offers unlimited processing and storage capacity.
- Reliability, in that, it enables access to applications and documents anywhere via the Internet.
- Limited access to the data by Cloud Providers, just to manage it without being able to see what exactly the data is.

V. Disadvantages of the Proposed System

- Due to increased security measures, the data held in the private cloud will be difficult to access from a remote location
- Waging against attacks is entirely the responsibility of the organization

VI. Methodology

This paper uses the Structured System Analysis and Design Methodology (SSADM). It is a waterfall which specifies exactly the flaws and tasks of development of the system and gives a detailed documentation of the system as shown in figure 6 below.

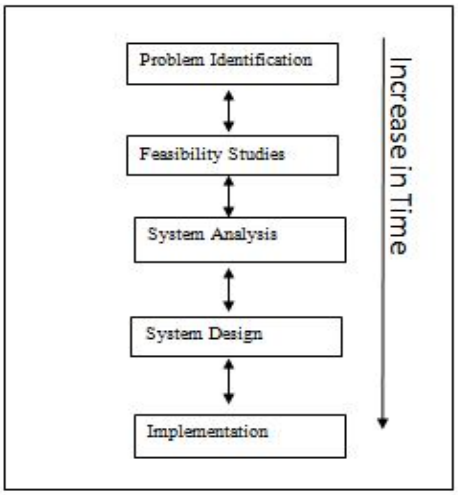

Fig. 5. Hierarchy of the development of the new system

VII. System Design and Implimentation

A. System Design

The design comes up after a detailed investigation and analysis of the existing system and what the new system should do. Figure 7 shows the conceptual design of the new system.

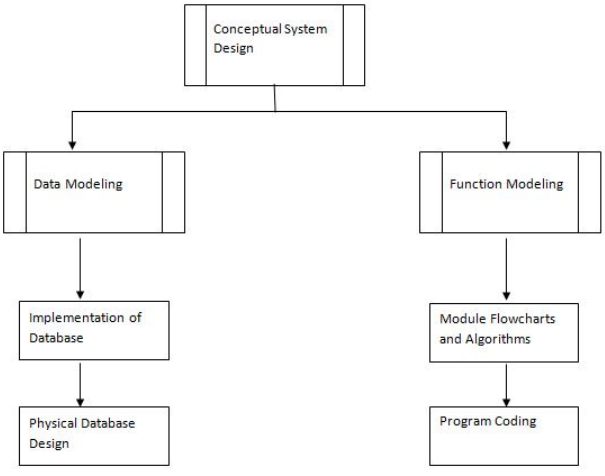

Fig. 6. Conceptual design of the system

The purpose of the system design is to effectively divide the overall problems into small and more manageable problems that can be easily handled by separate program modules.

B. System Architecture

The system architecture of the new system is influenced by the way it tends to overcome the limitations of the existing system. The new system adopts thin-client system architecture Server Side Application (SSA) where the cloud subscribers only have user interfaces to communicate with the server and display the results. All processing is done on the server. The user on the client side does not need any knowledge about the linkage of the server side, but the system administrator or application developers should be familiar with these techniques. The system has a user friendly interface and need to provide consistently reliable and secure access to users. Figure 7 represents the architectural structure of the system.

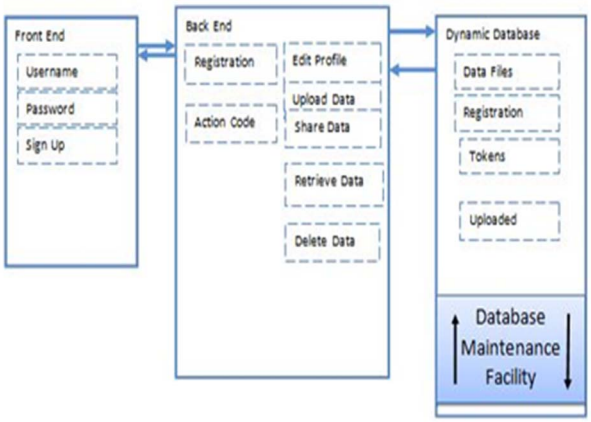

Fig. 7. Architecture of the new system

1) Front End: The front end consists of the user login where customers log in and carry out the computing activities (data storage and sharing). It contains the activity module for the customers for registration subsystem. The procedure involves login or sign up, perform user functions and log out.

2) Back End: The back end for the cloud subscribers contains modules such as edit profile, upload data, retrieve data, share data, delete data etc. This back end system demands for authentication and authorization to grant access to the cloud user.

3) Dynamic Database: This consists of all data sources available for use. The database stores data with their original data formats and projections in their sources.

C. Database Specification Design

The database was designed with MySQL. The database contains information of the entities of the Cloud-based File Sharing System (FSS). It organizes and manages the information to obtain the report required to support the System's relational database where a common field relates to different tables of data to each other. The following tables show the file structures (Field Names, Types, Sizes and their Descriptions) of Registration.dbf, Authentication.dbf and UploadedFiles.dbf respectively:

1) Registration.dbf File Structure: This file contains the features of various fields by which prospective subscribers (users) can make their profile data known to the system and thus subscribing to cloud computing services. Table I below shows the structure of the Registration.dbf file.

2) UploadedFiles.dbf File Structure: This file contains all files belonging to a particular user which have been uploaded and stored. This file holds data needed for servicing some user requests such as share, retrieve,etc. Table II shows the structure of UploadedFile.dbf file;

3) Authentication.dbf File Structure: The file contains all fields needed in order to manage and keep track of all users of the system. Table III shows the database file structure.

TABLE I. REGISTERATION FILE

Field No.	Field Name	Field Type	Field Size	Field Description
1	ID	int	1024	Primary Key of the Table
2	FullName	varchar	100	User's Full Name
3	Email	varchar	30	User's Email Address
4	DateofBirth	Date	8	User's Date of Birth
5	Sex	varchar	8	Sex
6	StateofOrigin	varchar	30	User's State of Origin
7	ContactAddress	varchar	30	Contact Address
8	PhoneNumber	varchar	30	Phone Number
9	UserName	varchar	30	User's Username
10	Password	varchar	30	User's Password
11	Question1	varchar	100	Security Questions 1
12	Question2	varchar	100	Security Questions 2
13	Question3	varchar	100	Security Questions 3

TABLE II. UPLOADED FILE

Field No.	Field Name	Field Type	Field Size	Field Description
1	ID	int	1024	Primary Key of the Table
2	FileID	int	30	File Identifier
3	NameofFile	varchar	100	Name of File
4	DateStored	Date	30	Date the File was Stored

TABLE III. AUTHENTICATION

Field No.	Field Name	Field Type	Field Size	Field Description
1	Username	varchar	100	Username
2	role (cloud user, cloud provider)	varchar	100	Role
3	Email	varchar	100	Email Address
4	Password	varchar	100	Password

D. User Interface Design

Data and storage are considered to be the center of any information system. The computer cannot accept data in human readable form, such as speech or a handwritten document. The HTML viewer is probably the most efficient and user-friendly choice, as no plug-in is needed at the client side. A customized HTML viewer is developed through Dynamic HTML and JavaScript, and contains a set of HTML and JavaScript files.

E. Input Design

This shows a conceptual view of the input template through which the system collects information from the user. The input forms are designs generally based on the necessary data that needs to be entered into the system. This comprises the input needed for an account to be created, a medium through which data are stored. Figure 8 shows a sample of the system's input.

Fig. 8. Sample of input design

F. Output Design

The output from the system designed is generated from the system inputs. More of the output generated is on data storage and sharing information. The output can be a list of stored files, list of cloud users, registration details etc. These outputs can be downloaded or shared with other privileged cloud users. Figure 9 shows a sample of the system's output.

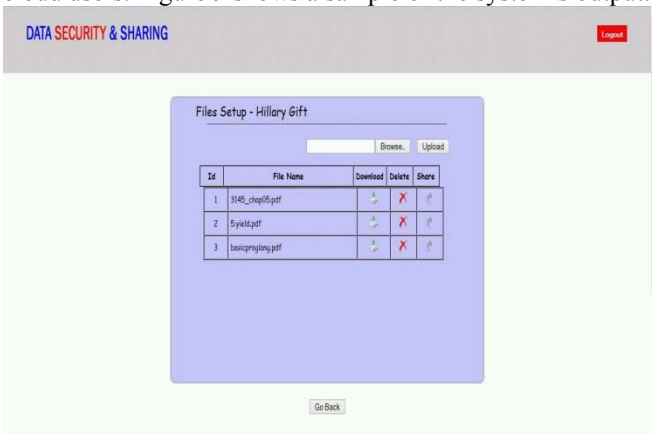

Fig. 9. Sample of output design

G. Security Login Design

The problem of guaranteeing secure access to computing resources in the cloud is gathering special attention. As personal stored data is culturally sensitive, security of information is important. Restricting user access to the web information provides the security needed. Consequently, a security mechanism was designed to limit user access to the cloud environment. To limit user access, the most direct way is to set the user name and password for the website. A table of pairs of user-id and password is therefore created in the MYSQL database. During login, a servlet is invoked to connect to the database and search for the matching pair. If the table contains the correct combination of the given user-id and password, the login is successful, and the servlet delivers the viewer page to the user. Otherwise, an error message will be shown on the user screen and the user will be redirected back to the log in page. The login process is depicted in Figure 10.

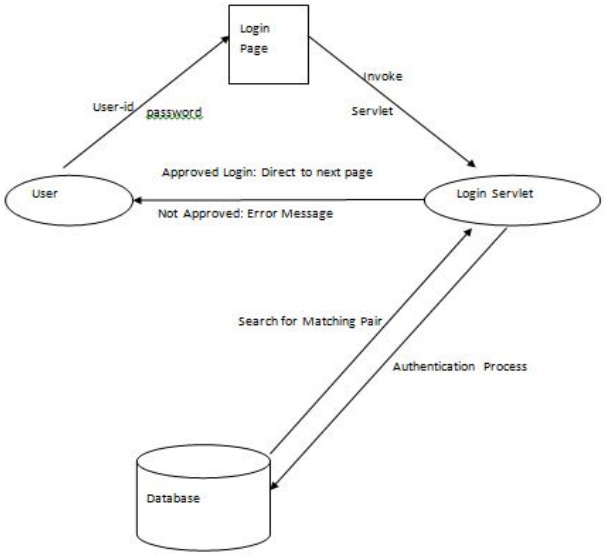

Fig. 10. Security login process

H. Program Flowchart

The flowchart is visually presenting the flow of data through the operations performed within the system and the sequence in which they are performed. Figure 11 show the file sharing flow diagram and while figure 12 shows the sample of the Dreamweaver.

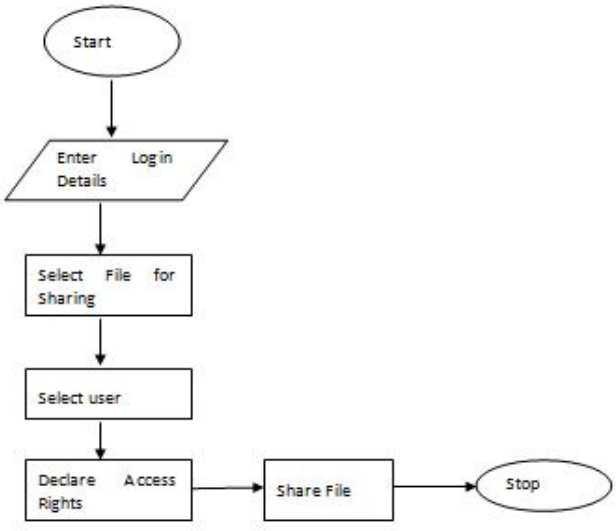

Fig. 11. File sharing flow diagram

I. System Design Tools

1) Front-end Building Tools: In building the front end which is the interfaces users, Adobe Dreamweaver, HTML, JavaScript and CSS were adopted.

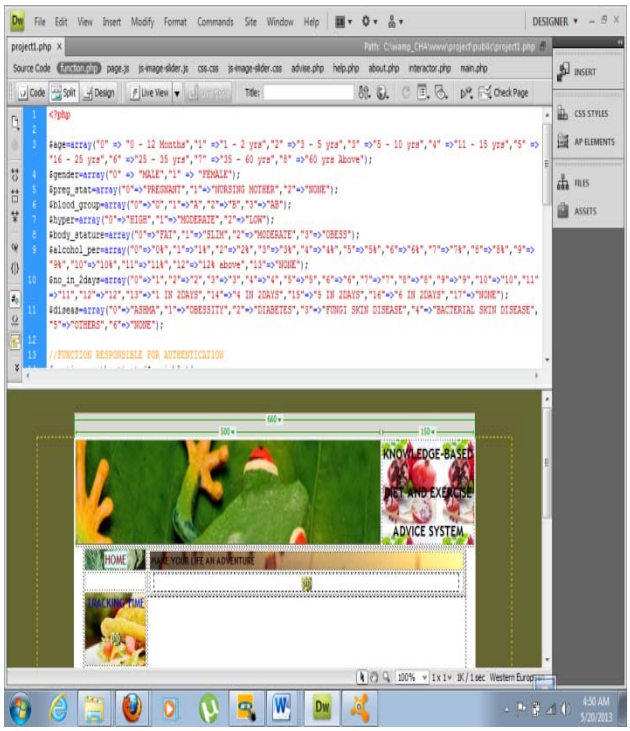

Fig. 12. Sanple of dreamweaver

2) Back-end Building Tools: The back-end of the new system otherwise called the Server-side comprises of the working database, and the model base. The tools used in building the side of the system are PHP, XAMPP and MYSQL.

J. System Requirement

The proposed system is a typical web-based application. Therefore, the basic system requirement consists of hardware and software component.

1) Hardware Requirements: The new system is designed to browse the website with the following hardware minimum requirements:

- Pentium II series processor.
- RAM (Random Access Memory) 1.00 GB and above.
- CD-ROM drive, 48x (speed).
- 10GB (Giga Byte).
- 56kbps full duplex fax modem.
- Floppy diskette or any external drive for backup
- 15'' color flat screen monitor

2) Software Requirements: The new system is designed to be implemented with the following minimum software requirements:

- Operating System: any recent version of Microsoft Windows operating system (windows NT/2000/ME/XP/Vista/7/8), any version of Linux, and any version of Macintosh will enable you to run this system comfortably.
- System Browser Software: Internet Explorer (any version)/ Mozilla Firefox browser/Opera browser/Safari browser or any other system browser.
- Apache WAMP Server (which comprises PHP server, MySQL Server and local server).
- Adobe Dreamweaver 4.0 or any PHP IDE.
- Java script, HTML, CSS.

K. System Implementation

After the development of the system, different testing procedures were carried to validate the proposed method.

1) Authentication and Authorization: The software is incorporated making most of the pages secured or protected which demands only approved users gaining access to such pages. The software utilized the PHP membership to validate and store user credentials which helps to manage user authentication and authorization. The software also utilizes the PHP role management to manage authorization allowing the ability to specify the resources users are allowed to access. It enables the treatment of group of users as a unit by assigning users to specific roles and creating access rules for them. When a user requests for a protected resource, the website will redirect the user to logon page where he has to enter the required credentials (name and password). The membership "validate user" method in the code-behind file checks the name entered and compares it will all the names in the membership store, when it finds a match, it compare the password entered with the password of the match found in the store. If they are both the same, it attaches an authentication ticket to the response that represents the use credentials (the password not included) and if not, returns the user to the logon page with assign up message. If the user is authenticated, the "Isuser_In_Role" method further checks if that name entered has authority to access the resource requested. It does this by checking the access rule if the user's role can access the resource requested for. If it comes out with booken "true", then the user is given access and the page or resource requested for opens and if it comes out with booken "false", the user is returned to the logon page with an access denied message. This procedure helps to ensure that a user does not log in as an administrator and vice-versa thereby viewing resources that are not meant to. It is also important to note that the authentication ticket issued to an authenticated user remains active until the user logs out or the session expires.

L. Testing the New System

After the design and coding of the system, testing the system follows immediately. Also, functionally to see what extent it will be usable. The two methods of testing that were adopted are:

- Integrity testing
- Usability testing

This project has been concerned with the possibility of ensuring data governance and enhancing data security in a private cloud computing environment. This system provides a centralized database for all users. It provides quick and secured access to information or data from the cloud. This new system has alleviated most of the shortcomings of storing information or data using flash drive, CD, diskette which can get missing, corrupted or stolen. Therefore the findings of this project indicate that exploring cloud-based storage and file-sharing services will enable mobility and anytime, anywhere computing.

CONCLUSION AND FUTURE WORK

This paper addresses the challenges of security in cloud data. The achievements recorded in this paper after the development of the new system are;

- Register users for authorization to use this service.
- Give them an action code which hackers cannot have access to.
- Ensure security of data stored to the database.

Future work can be done to extend the method proposed by this paper by introducing intelligent security protocol in cloud computing for a robust data security. It has also achieved most of its major objectives.

REFERENCES

[1] F. S. Al-Anzi, S. K. Yadav and J. Soni, "Cloud computing: Security model comprising governance, risk management and compliance," *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, New Delhi, 2014, pp. 1-6. doi: 10.1109/ICDMIC.2014.6954232

[2] Komal Dhingra, Sumit Kr Yadav, "Spam analysis of big reviews dataset using Fuzzy Ranking Evaluation Algorithm and Hadoop", *International Journal of Machine Learning and Cybernetics*, 2017.

[3] Sumit Kumar Yadav, Kavita Sharma, Arushi Arora, "Security Integration in DDoS Attack Mitigation Using Access Control Lists", *International Journal of Information System Modeling and Design*, vol. 9, pp. 56, 2018.

[4] I. Odun-Ayo, B. Odede, R. Ahuja, *Computational Science and Its Applications – ICCSA 2018*, vol. 10963, pp. 683, 2018.

[5] J. Lee, Y. S. Kim, J. H. Kim and I. K. Kim, "Toward the SIEM architecture for cloud-based security services," *2017 IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, NV, 2017, pp. 398-399. doi: 10.1109/CNS.2017.8228696

[6] T. Yen, A. Oprea, K. Onarlioglu, T. Leetham, W. Robertson, A. Juels, E. Kirda, "Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks", *Proceedings of the 29th Annual Computer Security Applications Conference*, pp. 199-208, 2013.

[7] R. Kaur and J. Kaur, "Cloud computing security issues and its solution: A review," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015, pp. 1198-1200.

[8] Tharam Dillon, Chen WU, Elizabeth Chang, "Cloud Computing: issues and challenges", *24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 150-445X/10, 2010.

[9] Laila Fetjah, Karim Benzidane, Hassan El Alloussi, Othman El Warrak, Said Jai-Andaloussi, "Toward a Big Data Architecture for Security Events Analytic", *IEEE 3rd International Conference on Cyber Security and Cloud Computing*, pp. 1-7, 2016.

[10] V. P. Lalitha, M. Y. Sagar, S. Sharanappa, S. Hanji and R. Swarup, "Data security in cloud," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, 2017, pp. 3604-3608. doi: 10.1109/ICECDS.2017.8390134

[11] R. Swathi and T. Subha, "Enhancing data storage security in Cloud using Certificateless public auditing," *2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*, Chennai, 2017, pp. 348-352. doi: 10.1109/ICCCT2.2017.7972299

[12] D. Dattatray Kankhare and A. A. Manjrekar, "A cloud based system to sense security vulnerabilities of web application in open-source private cloud IAAS," *2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT)*, Mysuru, 2016, pp. 252-255. doi: 10.1109/ICEECCOT.2016.7955225

[13] Youssef Gahi, Mouhcine Guennoun, Hussein T. Mouftah, "Big Data Analytics: Security and Privacy Challenges", *IEEE Symposium on Computers and Communication (ISCC)*, pp. 15-17, June 2016.