Journal of Computer Sciences

Original Research Paper

Design and Implementation of Security in Healthcare Cloud Computing

Molamoganyi Gorata, Adamu Murtala Zungeru, Mmoloki Mangwala and Joseph Chuma

Department of Electrical, Computer and Telecommunication Engineering,
College of Engineering and Technology,
Botswana International University of Science and Technology, Private Bag 16, Palapye, Botswana

Article history
Received: 27-12-2016
Revised: 15-03-2017
Accepted: 10-04-2017

Corresponding Author:
Adamu Murtala Zungeru
Department of Electrical, Computer and Telecommunication Engineering, College of Engineering and Technology, Botswana International University of Science and Technology, Private Bag 16, Palapye, Botswana
Email: zungerum@biust.ac.bw

Abstract: As technology keeps on evolving, different organisations make use of the recent trends in technology and the health sector is no exception. As the cost of healthcare services is increasing, healthcare professionals are becoming scarce. Healthcare organisations have also adopted the latest technology of cloud computing. The introduction of cloud computing has proved to be a feasible idea on the information technology community. Rather than keeping the patient's information in a file in a health facility he/she was treated in, the information is stored in a cloud so that it can be shared amongst all health organisations and health professionals. Information is stored in a central place where it can be easily accessed, thus saving time and avoiding repetition of always writing the information each time a patient is attended to in a different facility. However, there are issues with sharing such information on the cloud since it is sensitive information. Ensuring this sensitive information security, availability and scalability are a major factor in the cloud computing environment. In this study, we proposed a mathematical model for measuring the availability of data and machines (nodes). We also present the current state-of-the-art research in this field by focusing on several shortcomings of current healthcare solutions and standards and we further proposed a system that will encrypt data before it is being sent to the cloud. The system is intended to be linked to the cloud in such a way that, before the client submits the data to the cloud and, the data will go through that system for encryption. The paper presents the steps to achieve the proposed system and also a sample encrypted and decrypted file.

Keywords: Cloud Computing, Healthcare Services, Information Security, Availability

Introduction

In the olden days, information about patients was stored in files in different health facilities where there have been treated. The problem with this method is when the file gets lost, or there is fire, the patient's medical history cannot be retrieved from anywhere and each time the patient is attended at a different facility, a file has to be created which is time-consuming and wastage of resources. With the introduction of cloud computing, there are new possibilities in health sector such as easy and flexible access to medical data, opportunities for new business models (Lohr *et al*., 2010).

Cloud computing is the type of computing used for sharing resources over the internet using virtual machines rather than physical machines resources like servers, storage applications and services can be rapidly provided and released with minimal management effort or service provider interaction (Gavrilov and Trajkovik, 2012).

The application of cloud computing in the health sector is called health cloud. However, as much as the health cloud brings many benefits there are also some challenges. As we know that the health care deals with very sensitive information, there is aneed for an increased security and privacy levels so that this information does not fall into the wrong hands. The availability of the information to the users is also very important. Security needs to be implemented on both the cloud and the client side. On the work of previous researchers, more emphasis was on the security on the cloud rather than on the client side.

As much as information might be accessed by unauthorised users in the cloud, this can also happen at the client's side. The proposed security model focused more on encryption of data before it is sent to the cloud.

The remainder of the paper is organised as follows; second 2 gives discussion on literature review. Section 3 presents an overview of cloud architecture. In section 4, security and privacy issues in health cloud are presented. Section 5 deals with nodes and information availability in cloud computing. In section 6, we present the proposed security solution. The work is concluded in section 7 with future work to be undertaken.

Literature Review

This section covers the previous work which was done on this area. Different authors have come up with the solutions to the security issues on the health cloud.

The authors' in (IHCS, 2013) have worked to mitigate the performance penalties by introducing the Intel Advanced Encryption Standard. New Instructions (Intel AES-NI), built into select Intel Xeon processors, Intel core vPro processors and select Intel core processors, enhances encryption performance enhancement. Intel AES-NI delivers faster, more performance enhancement, more affordable data protection by encouraging pervasive encryption to be standard in cloud networks where it was not previously feasible.

As proposed in (Thilakanathan *et al*., 2014), is a secure data sharing model and protocol that will enable data sharing amongst a group of users specified by the data owner. Secure data model enhances the e-health monitoring system illustrated by adding a security layer that enables efficient and secure data sharing. The original web service now represents the Cloud Data Service (CDS) and added to it, is another web service called Data Sharing Service (DSS) that handles the data sharing aspects of the system. The model works thus; each user in the group, including the Data Owner (DO), has a Key Database (DKDB). However, their keys are partitioned into the (n +1) part where n parts are stored in each proxy and the user keeps the extra part. In this way, none of the users know the full key y required to decrypt the keys in the data key database. When the user requires data access they call the DSS then decrypt the key in the DKDB using all the key pieces in the proxy database corresponding to the calling user. The key is then used to decrypt the data in the cloud. When the data owner requests a user to be revoked, their key pieces in the proxies are simply removed and the original data need not be re-encrypted nor does their need to be any re-distribution of keys to remaining users.

On the other hand, to address the security issues in a cloud hosted healthcare, (Kaur and Chana, 2014) proposed security mechanisms at multiple levels and to provide a role-based access control to ensure the protection of critical medical information about patients. To achieve this, they proposed to combine the use of symmetric cryptosystem for authentication together with the Rule-Based Access Control (RBAC) mechanisms for authorization. Users of Community-Based In-Home Services (CBIHS) are given a unique username and password. Rather than storing the user password in plain text, it is encrypted with a private key (pk) issued by a Trusted Third Party (TTP). Once the users are authenticated according to the username and password they provided, the authorization is implemented based on the user roles.

The authors in (Al-Khanjari *et al*., 2014) proposed the use of privacy domains for e-health. They proposed privacy domains for the patient's medical data as a measure to support the enforcement of privacy and data protection policies. The system must be able to divide execution environments for applications into separate domains that are isolated from each other. Data is kept within a privacy domain and the domain infrastructure ensures that only authorised entities can join this domain. Moreover, data leakage from the domain is prevented by the security architecture and the domain infrastructure.

Furthermore (Lohr *et al*., 2010) extended the concept of trusted virtual domains by focusing on the client platform security. On the client platform, a security kernel is running on top of the hardware, providing isolated virtual machines for application and conventional operating systems. Moreover, there is a Trusted Virtual Domain (TVD) proxy for each TVD, which manages the TVD on the client and configures the security kernel according to the TVD policy. Also, there is a secure Graphical User Interface (GUI) provides input and output, to ensure that users can always identify with which compartment they are interacting from. Furthermore, the client platform contains a trusted hardware component called the Trusted Platform Module (TPM) which can be used for the verification of the integrity of the software on the clients' side. This module is usually implemented as a separate chip integrated on the main board of a computer. TPM provides a set of security and cryptographic functions such as public key encryption, digital signatures, secure key storage, non-volatile memory etc.

In (Barua *et al*., 2011) ESPAC scheme (enabling security and patient-centric access control for e-health cloud computing) was proposed, which allows user who needs access to data to have different access privileges based on their roles and assigns different attribute sets to them. In the initial step using different body sensors, patient health information is sensed and ready to be transmitted to the trusted e-health care service provider. Public key cryptography is used to securely transfer collected Protected Health Information (PHI) to the e-health care service provider. Patient securely transfers a secret key to the trusted e-health care service provider, if he authorised the service provider to build-up the access tree. After receiving the PHI securely, health care service provider classifies the PHI based on the attributes set chosen by the patient. It then makes different privacy levels of data requesters based on their roles and assigns different set of attributes to these different levels. After classification encrypted data securely transfers to the cloud storage.

Authors in (Ikuomola and Arowolo, 2014) proposes architecture of a secure e-health in thecloud using homomorphic encryption and access control (SECHA), it comprises of five basic components (patient, PHR, access control module, user or subject and cloud). Homomorphic encryption allows patients to store encrypted PHR files in a public cloud and take advantage of the cloud provider's analytic services. The scheme prevents unauthorised users from violating privacy and prevents leakage of private information.

Also, (Fakhrul *et al*., 2012) came up with health cloud architecture where Wireless Sensor Networks (WSNs) are integrated with cloud computing for storing patient's health data in the cloud. The proposed architecture is scalable and has the ability to store a large amount of data generated by sensors. The security mechanism is implemented inside the cloud to guarantee data confidentiality, security and fine-grained access control. The security enforcement and key management are totally transparent to the users and do not require their interventions.

In (Alshehri *et al*., 2012), Ciphertext Policy Attribute-Based Encryption (CP-ABE scheme) was proposed. In this scheme the health care providers share one public key for encryption, thus avoiding Publickey Infrastructure (PKI); however each healthcare provider has a distinct secret key for decryption. The secret key of a healthcare provider can decrypt a particular ciphertext only if the attribute set of the healthcare provider's key satisfies the access policy associated with the cipher-text.

Some other issues faced in cloud computing environment are discussed and analysed in (Khan, 2016; Singh *et al*., 2016; Sharma *et al*., 2016).

Hierarchical Architecture of Cloud Computing

Cloud computing consists of three service models; IAAS, PAAS and SAAS.

Infrastructure As A Service (IAAS): This is the lowest layer that provides basic infrastructure support services (Alshehri *et al*., 2012). In this layer the consumers are offered processing, storage, networks and other fundamental computing resources where they are able to deploy and run arbitrary software. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of selected networking components (Mell and Grance, 2011).

Platform As A Service (PAAS) this is the middle layer, which offers the user the flexibility to develop applications using tools provided by the PAAS provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possibly configuration settings for the application-hosting environment (Mell and Grance, 2011).

Software As A Service (SAAS) cloud; in the Fig. 1, the consumer has the freedom of using the providers' applications running on a cloud infrastructure. The applications are accessible from various clients' devices through either a thin client interface, such as a web browser or a program interface (Mell and Grance, 2011).

Cloud computing also consists of deployment models. Each company chooses a deployment model for a cloud computing solution based on their specific business, operational and technical requirements. There are four primary cloud deployment models: Private, country, continent and hybrid model (Al-Khanjari *et al*., 2014). In this study, we shall look at cloud computing in the healthcare domain and classify them on how they are related. This includes private, country, continent and hybrid as shown in Fig. 2 and 3.

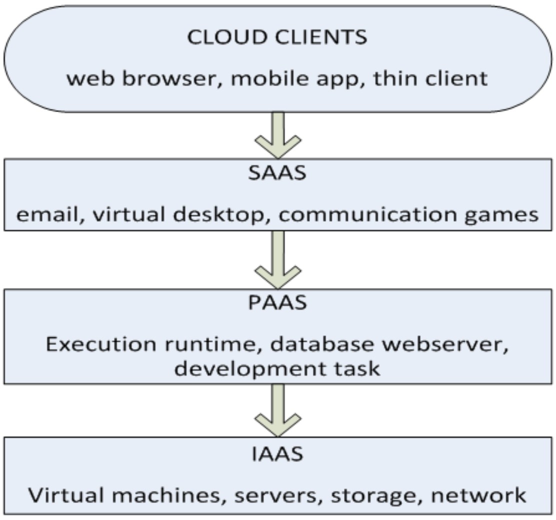

CLOUD CLIENTS
web browser, mobile app, thin client
SAAS
email, virtual desktop, communication games
PAAS
Execution runtime, database webserver, development task
IAAS
Virtual machines, servers, storage, network

Fig. 1. Hierarchical view of service models in cloud computing

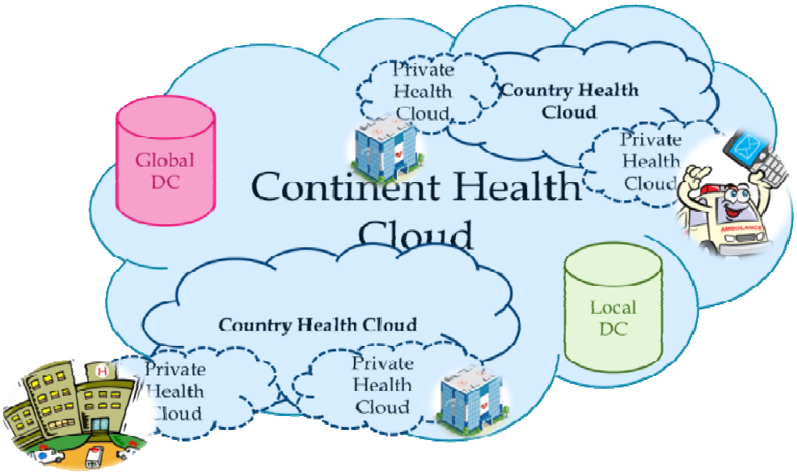


Fig. 2. Global health village model for continental health cloud

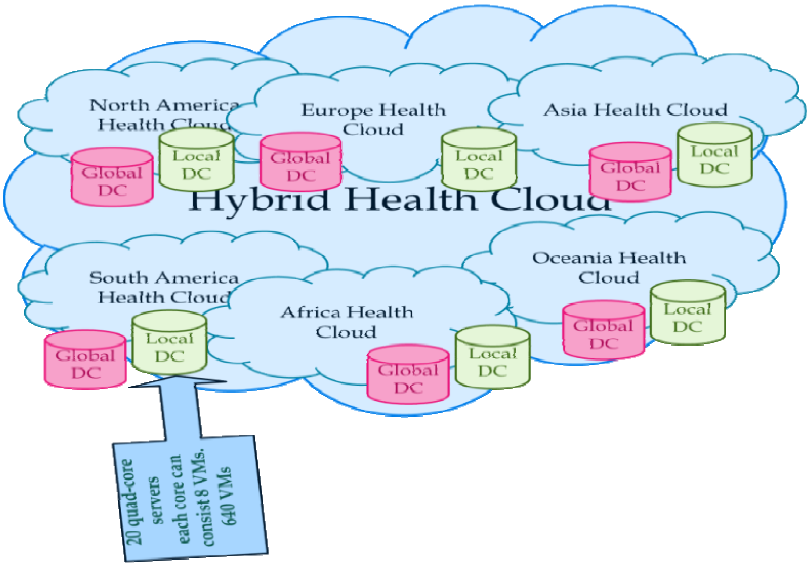


Fig. 3. Global health village model for hybrid health cloud

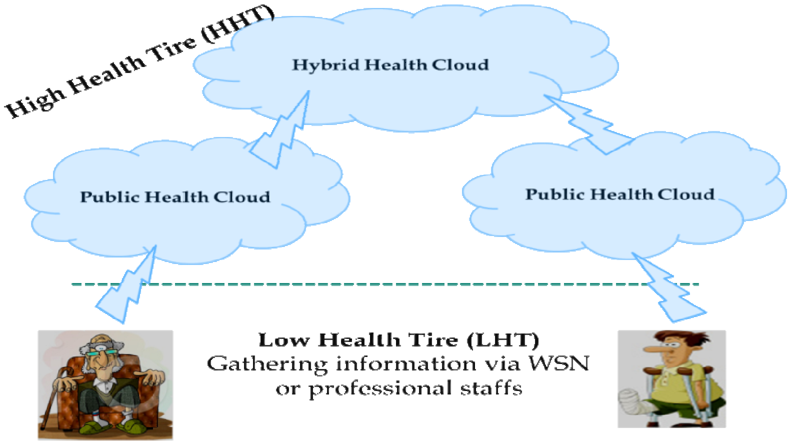


Fig. 4. Information gathering in health cloud system

Private health cloud: In this, the cloud infrastructure is operated solely for a health Care Delivery Organisation (CDO).

Public health cloud: The cloud infrastructure is made available to the general public.

Community health cloud: The cloud infrastructure is shared by several CDO'S and support specific community (Zhang and Liu, 2010). It contains both features of public and private cloud models (Al-Khanjari *et al*., 2014).

Hybrid: The model employs aspects of all the other cloud models and it is the most commonly found cloud deployment model used within large organisations (Al-Khanjari *et al*., 2014). The information generally eminent at the patient's side, or mostly needed at the patient's ends. Figure 4 shows the flow of information and how the data are collected.

Security and Privacy Issues in Health-Cloud

As much as cloud computing has some beneficial factors, it also comes with some security risks. The healthcare deals with some very sensitive information about the patient which needed to be handled with greater care so as not to fall on wrong hands. The main issues in health-cloud security are; confidentiality, privacy, multi-tenancy and integrity.

Confidentiality: Refers to only authorised parties of the system having the ability to access protected data. The threat of data compromise increases in the cloud, due to increased number of parties, devices and applications involved. The more the number of parties increases, the high risks of unauthorised parties accessing data. According to (Thilakanathan *et al*., 2014), the threats to confidentiality can be divided into three; insider attacks, outsider attacks and data leakage. Inside attacks can be in the form of malicious cloud provider user accessing data in the cloud, malicious cloud customer and the malicious third party user gaining access to data. Outsider attacks may be in the form of remote software attacks on the cloud infrastructure and remote hardware attack against the cloud. Data leakage may be due to failure of security access rights across multiple domains and failure of electronic and physical transport systems for cloud data and backups (Fakhrul *et al*., 2012).

Privacy: It is the desire of a person to control the disclosure of personal information. The cloud presents a number of legal challenges towards privacy issues involved in data stored in multiple locations in the cloud, thus increasing the risk of confidentiality and privacy breaches (Thilakanathan *et al*., 2014).

Multi-tenancy: Refers to resource sharing in the cloud, e.g., multiple users use the same resources at thenetwork level, host level and application level. Multi-tenancy presents a number of privacy and confidentiality threats. Reusable objects must be carefully controlled in case they do not create serious vulnerability.

Integrity: A key aspect of information security is integrity. Integrity means that assets can be modified by only authorised partners, in authorised ways.It is protecting data from unauthorised deletion, modification or fabrication (Thilakanathan *et al*., 2014). The integrity of data within complex cloud hosting environments such as SAAS configured to share resources amongst customers could provide a threat against integrity if system resources are effectively segregated. Data segregation can be due to incorrectly defined security perimeters, incorrect configuration of virtual machines and hypervisors. Implementation of poor control procedures can create many threat opportunities (Sen, 2013).

Availability in Cloud Computing

In this section the existing research in availability is divided into two categories; the first one covers information availability and the second one covers the node availability.Availability in cloud computing is the extent to which computational resources of an organization are fully accessible and usable. Denial of service attacks, equipment outages and natural disasters are all threats to availability in the cloud.

Information Availability in Cloud Computing

For having available information/data, redundant instances are expected to be stored in other machines. The redundancy is due to replication of data. Cloud scenarios face a huge amount of data which is known as big data, as such, the replication method affect the storage and communication cost directly. Therefore, a method in which size of the replica is reduced has high priority. In replication model, there is great concern about resource consumption as well as availability. In fact, a tradeoff between cloud resource consumption and availability seems necessary.

Data could replicate among different data centers by two general methods. It can replicate by the use of full data redundancy algorithms or a partial one. In full data redundancy algorithms, all data are expected to be replicated to one or more datacenters based on the selected algorithm. That means it consumes more resources in terms of communication and storage, but it provides high availability. The partial data redundancy algorithms split data into multiple parts and store each part in different data centers. Therefore, the communication and storage cost would be decreased in regards to the size of chunked data. In the case of failure, the portions of data are gathered from all or number of data centers. Further information about the redundancy methods can found in (Hernandez-Ramirez *et al*., 2012).

Deshmukh *et al.* (2012) proposed a model in which servers are divided into two levels which are master and slave servers. Users who want to upload a file and modify it perform these operations on master servers and they do not have any connection with slaves which store chunks of data. Therefore, in case of failure or misbehavior appearance of master servers, chunks of data will be recovered from slaves. Dispersing and recovery of data is performed based on the token keys which are generated through a token generation algorithm. This method supports both security and availability with the assumption that the administrators are responsible for authenticating users as well as chunking data. In fact, with chunking data and storing them in the separate slave servers, the errors are localized.

In (Mar, 2011) Mar discussedthe Secured Virtual Diffused File System (SVDFS) which provide data security, integrity and availability suited for deployment in a public cloud environment. The main idea of this model is the separation between storage and information owners or in other words, it allows data storage outsourcing, but the control of these data is not outsourced. All these is achieved by using a file system interface and registry server that the interface could locate in the cloud or outside the cloud while the registry server is in the data owner site and keeps the metadata that are used in the case of gathering or distributing the data. More data redundancy methods are found in (Bowers *et al.*, 2009; Menascé, 2004; Jouini *et al.*, 2012).

Node Availability in Cloud Computing

Node availability is computed by a fraction of the time that the node is under operation. A node in this study refers to the data centers which include both physical servers and virtual machines.

Parameters used in measuring the node availability are Mean Time to Failure (MTTF) or mean up time, Mean Time to Recover (MTTR) or mean downtime and Mean Time between the Failure (MTBF). MTTF refers to the expected time of operation before first failure occurrences. MTTR is the time taken by each failed machine to be recovered while the MTBF indicates the time between two consecutive failures. There are some factors that are affected by these mentioned parameters.

In Jouini *et al.* (2012) Mean Failure of Cost (MFC) base on the mentioned terms of time was calculated. They worked on availability and security and then calculated the effect of failure with the financial cost that this faultier impose to the organizations or cloud providers.

Daniel investigated the availability of Internet Data Centers (IDC) in (Menascé, 2004) and made it bearable by comparison with performance. IDC has M equivalent machines that respond to user requests and applications which are running in IDC are expected available 99.999 percent of the time. In this research the availability is computed by the use of the Equation 1 as:

$$A_{j=\sum_{M}^{k=j} P^j} \tag{1}$$

where, j indicates, at least, j machines in operation and the probability P_j is computed using Markov chain. P_j is probability that at least j machines are in operation. To explain the performance and availability of machines in the system, a model as given in (Menascé, 2004) is shown in Fig. 5.

For better understanding of availability determination of the system, the following are of interest for the data owner:

- Rate of failure of the machines, the number of the system machines, the number of personnel available to take up the repair of the failed machine, the average time it takes the personnel to revive a failed machine and the probability that exactly j machines are in operation and active at any given time
- Rate of failure of the machines, the number of the system machines, the number of personnel available to take up the repair of the failed machine, the average time it takes the personnel to revive a failed machine and the number of personnel that will guarantee at least j machines are operational for a given probability
- The effect of the average time taken by the repair personnel to fix a machine on the total MTTR
- Effect of the size of personnel involved in the repair of the failed machine, considering Mean Time To Repair (MTTR)

It is then worthy of noting:

- The probability that exactly j machines are operational for a given number of machines in operation for different number of available personnel to repair the failed machines
- The probability that at least j machines are in operation for a given number of machines in operation for different number of available personnel to repair the failed machines

Given the probability P_G that G number of machines has failed is represented by:

$$P_G = \begin{cases} P_0\left(\dfrac{\lambda}{\mu}\right)^G \begin{pmatrix} M \\ G \end{pmatrix} & G = 1, \ldots L \\ P_0\left(\dfrac{\lambda}{\mu}\right)^G \begin{pmatrix} M \\ G \end{pmatrix} \dfrac{L^{L-G} G!}{L!} & G = (L+1), \ldots M \end{cases} \tag{2}$$

When the probability of machines that failed is one (1), given us 100% of available machines in operation, yields:

$$\sum_{G}^{M} P_G = 1, P_G = 1 \tag{3}$$

and:

$$P_0 = \left[\sum_{G=0}^{L} \left(\frac{\lambda}{\mu}\right)^G \binom{M}{G} + \sum_{G=L+1}^{M} \left(\frac{\lambda}{\mu}\right)^G \binom{M}{G} \frac{L^{L-G}G!}{L!} \right]^{-1} \tag{4}$$

The probability P_j that at least j machines are in operation can be written as:

$$P_j = \sum_{i=j}^{M} P_{M-i} \tag{5}$$

where, $P_{M\text{-}i}$ in (5) is the relationship gotten from Equation 2-4.

For our model, we consider number of machines in operation (j) of 60 in the data center for different number of personnel available for the repairs (L) of failed machines as: 10, 5, 3 and 2. This is also with the assumption that MTTF is 250 min (λ = 1/250 = 0.004 failures per minute). The average time taken for a personnel to diagnose and repair a machine (MTTR) is assumed to be equal to 20 min (μ = 1/20 = 0.05 repairs per minute).

Figure 6 shows the probability that at least j machines are operational with respect to j machines in the data center for different number of personnel available to service the failed machines. In the Fig. 6, it should be observed that, for 2 personnel ready to service failed machines, $L = 2$, the probability that at least 20 machines are operational is 0.94 and that of at least 30 machines are operational is 0.18. From Fig. 6, it can be observe that, for the operation of 40 machines, the probability is zero. If we also look at having 3 personnel available to put the failed machines or nodes in action (L = 3), we can have up to 30 machines fully operational. This means that, if we require 40 machines to be operational, with 2 or 3 personnel, it will not be possible. To have 40 machines fully operational, we will need 5 or 10 personnel to be on ground for service. However, to have about 98% of the machines having been fully ready for work or operational, 10 personnel 10 is required as can be seen in Fig. 6.

In the next section, a mathematical model is proposed for measuring the availability in the cloud computing that consider both data and node availability.

Mathematical Model for Availability

This section measures the availability based on all factors that interfere with the system availability. This measurement causes to make better dissension for the optimum of the system in terms of availability. But the clear point is that availability depends on the security or performance and also on the application. Some applications focus on the performance more than security and their policy for redundancy and load balancing will define to an extent how this goal will be achieved. While in other applications, security is more important and as such, they use different techniques for keeping data confidential. These decisions and techniques impact directly to the availability and application providers should map proposed mathematical method to their applications.

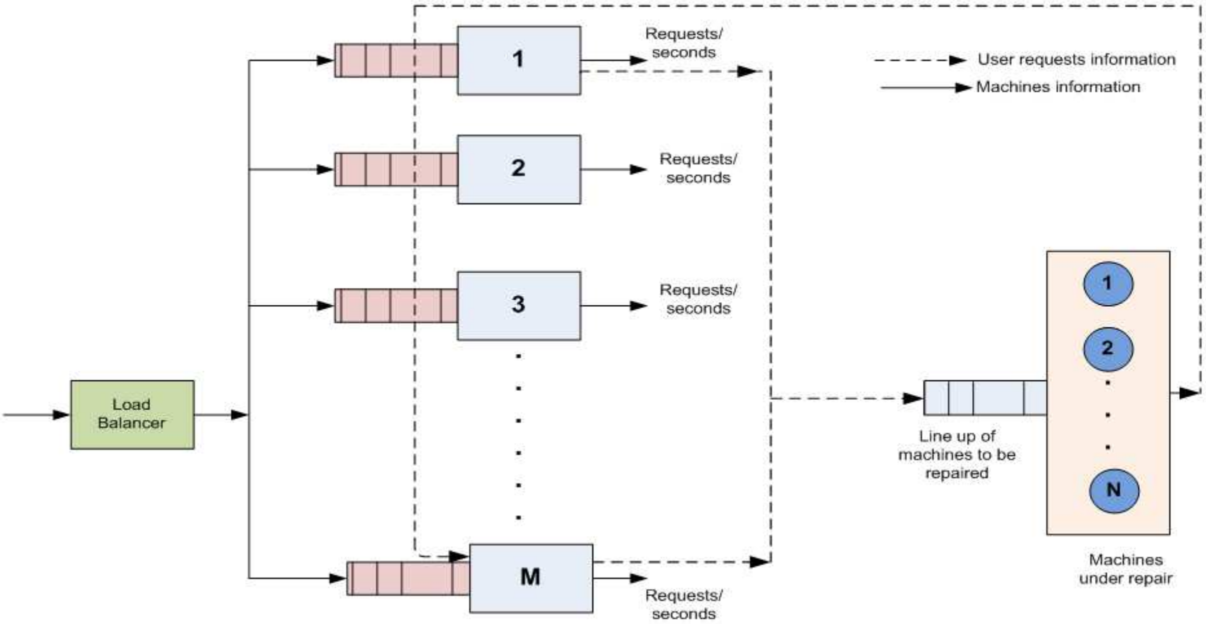


Fig. 5. Availability and performance model for data center

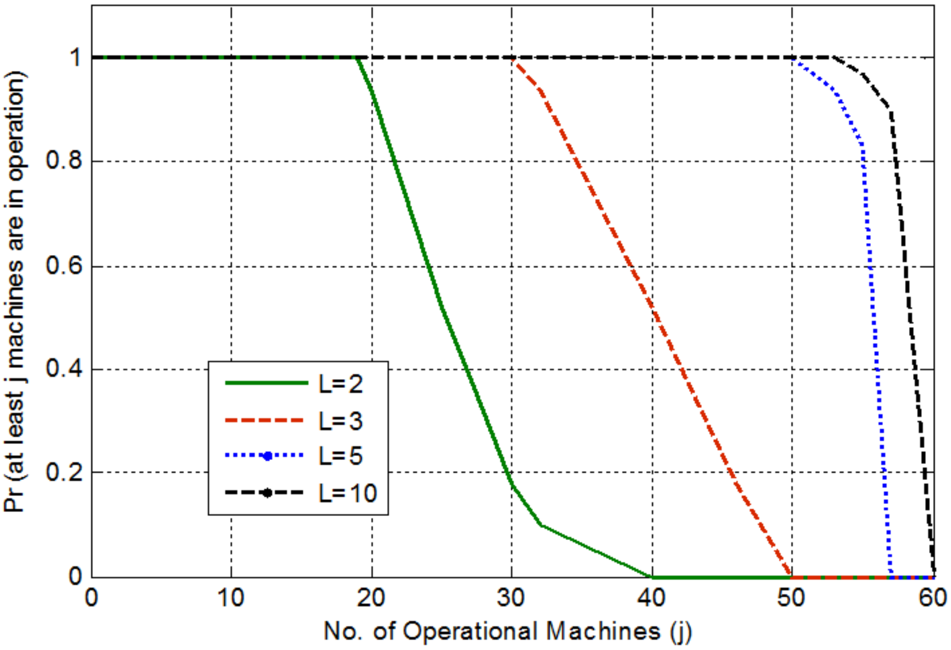


Fig. 6. Probability of at least j machines is in operation

The sets of physical and virtual machines are defined as:

$$P = \{P_1, P_2, P_3, \ldots, P_M\} \quad (6)$$

$$VM = \{VM_1, VM_2, VM_3, \ldots VM_N\} \quad (7)$$

where, P is a set of the physical machines and VM is a set of virtual machines for each physical machine.

Assuming that every VM can play a backup role for the failed one, then the node availability is achieved by the following equation:

$$Availability = \sum\nolimits_{j=K}^{M} \sum\nolimits_{i=L}^{N} p(P_j)\, p(VM_i) \quad (8)$$

The first summation calculates the probability of availability of M physical machines which are under operation and the second one does the same for N virtual machines which are under operation on each physical machine.

The probability of availability of physical or virtual machine is calculated by:

$$p(P_j) = 1 - p(FP_j) \quad (9)$$

where, $p(FP_j)$ depends on the following:

- Rate of failure of j (α)
- Time that j needs to be recovered (MTTR)

The second factor, Mean Time to Recover (MTTR) is also influenced by the following parameters: R, shows the number of machines which are waiting in the repair queue, S, represents the number of staffs who are repairing the machines and Tr indicates the average of time that each machine needs to be recovered and back to the system. Then MTTR is computed as follows:

$$MTTR = \begin{cases} Tr; & IF\ S > R \\ (R - S)Tr; & IF\ S < R \end{cases} \quad (10)$$

To make the calculation more accurate, the assumption made in (8) need to be modified based on the reality. Therefore, the exact number of VMs that host the redundant data is expected to be determined. To this end, graph ($G_{b\_node)}$ is necessary to be defined. The $G_{b\text{-}node}$ represents which node could be a backup node, for a particular one, the directed and weighted graph is expressed as:

$$G_{b\_node} = (P_x VM_y, E, W) \quad (11)$$

where, P_xVM_y represents Y^{th} VM that belongs to the X^{th} physical machine as the node of the graph. While E shows the edge of the graph that gives to the system an input parameter and it is a function of redundancy algorithm which is used for the data availability. Finally, W determines the weight of each edge. Figure 7 illustrates the G_{b_node} graph which has 3 nodes.

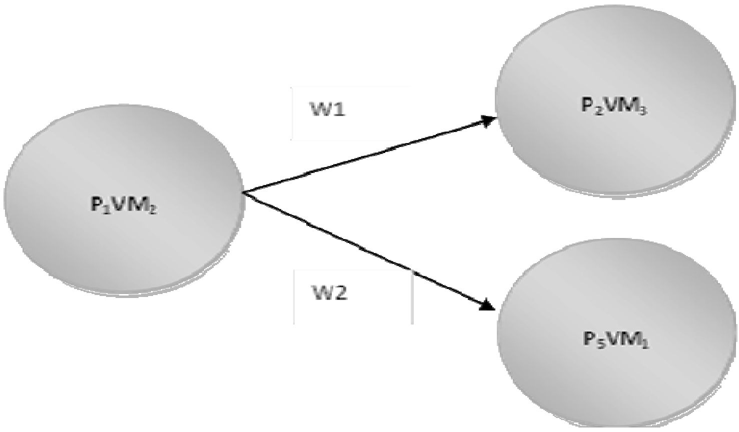


Fig. 7. The G_{b_node} graph

Figure 7 shows third virtual machine by second physical machine and first virtual machine by fifth physical machine have redundant data of the second virtual machine of the first physical one. If one of them is available at the failure time that one will be replaced but if both of them are available, a decision would be made based on the W_1 and W_2.

W is a dynamic parameter which is calculated based on three factors; which are the capacity of CPU, available memory of the second node and the available bandwidth. Therefore, in the case of failure, the requests transfer to the node which has higher *W*.

Data redundancy algorithm has a direct impact on the availability of system because it defines the number of edges of the graph and it adds another weight to the graph that shows the number of virtual machines needed for recovery the data of the system. Then by defining it, the graph would change to the 2-weighted and directed graphs in which decision making will be done based on the combination of both weights.

Proposed Solution

Since we have seen that most of the focus is on the security of the data on the cloud rather than on the client side, the client is responsible for the encryption of their own data, hence, it is a disadvantage on the client since most of them don't know anything about data encryption, so in a system like that most of the clients will just send data without any security hence exposing their personal information to unauthorised people. Our proposed solution is a system that will encrypt data before it is being sent to the cloud. The system will be linked to the cloud in such a way that before the client submits the data to the cloud; the data will go through that system for encryption. After the data has been encrypted that's when it will go to the cloud. This type of system will reduce the pressure of encrypting data on the clients and also every client can be able to send their information on the cloud without worrying about the security. Figure 8 shows a model of the proposed system.

The following steps are taken for successful operation of the proposed system:

Step 1: User request a file from the healthcare.
Step 2: Data owner loads data into the encryption system.
Step 3: The encryption system encrypts the data and saves it into the database.
Step 4: The data owner sends encrypted data to the cloud servers. The cloud provider does not have any access to the data stored. Instead the data users are the ones who are granted access.
Step 5: When the data user wants to access data from the cloud, they send a message to the data owner.
Step 6: The data owner will then check the user's profile to confirm if they are authorised to access that particular data.
Step 7: If the user is authorised to access the data, the data owner will grant the user a random key with a time limit. Once the user access the data, the data owner will store the key in the key database and updates the cloud servers.

The flowchart in Fig. 9 shows a sequence of activities that take place before data can be sent to or retrieved from the cloud. The data owner input data into the encryption system for encryption. After the file is encrypted it will be loaded into the cloud servers. The data user will then request access to data in the cloud from the data owner, then the data owner will determine if the user is authorised to access the data, if the user is authorised then the data owner will generate a random key and send it to the user. The user will then decrypt the data, else if the user is not authorised to access data they will be denied access.

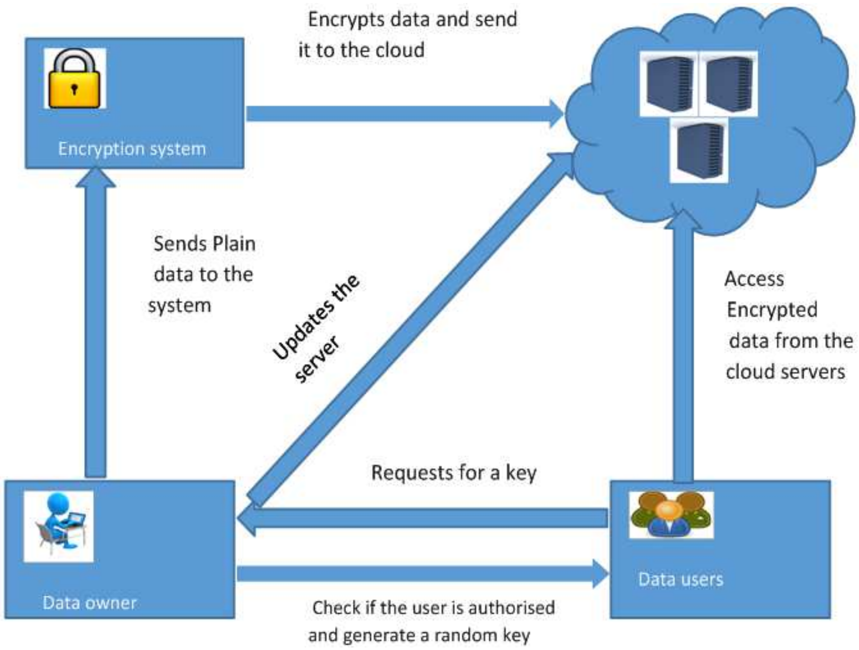


Fig. 8. A model of proposed security system

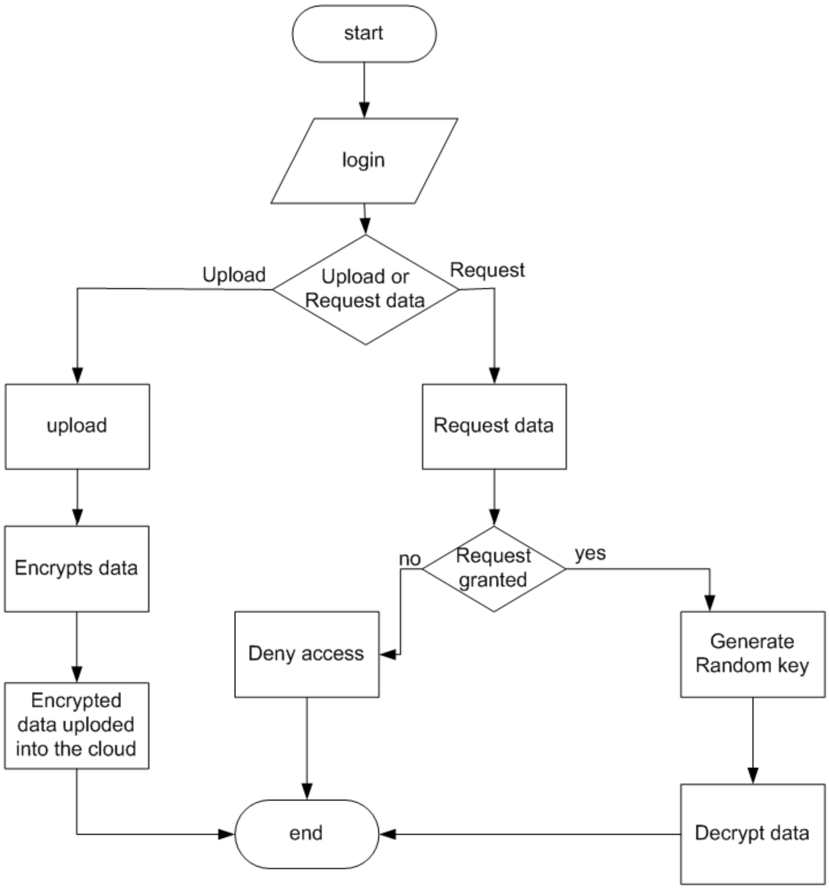


Fig. 9. Flowchart of the proposed model

Low Level Design of the System

Flowchart for Uploading and Encrypting

The flowchart in Fig. 10 shows the process of encrypting information to be secured in the cloud. The algorithmic descriptions as well as the pseudo-code are also shown for better understanding of the encryption part of the proposed system as:

- Data owner logs into the encryption system
- Data owner loads data into the system
- The system encrypts data
- Stores data into the database

```
Pseudocode-1 (uploading and encrypting data)
START
Login
ENCRYPT file
Store in database
EXIT
```

Results of the Encryption System

The image shown in Fig. 11 shows the original file to be encrypted, while the image in Fig. 12 is the result of the encrypted system. The file was loaded into CloudSim simulation software for encryption (Calheiros *et al*., 2011).

CloudSim simulation layer provides support for modelling and simulation of virtualized Cloud-based data center environments including dedicated management interfaces for Virtual Machines (VMs), memory, storage and bandwidth. In general, it provides a generalized extensible simulation framework that enables modelling, simulation and experimentation of emerging cloud computing infrastructure and application services.

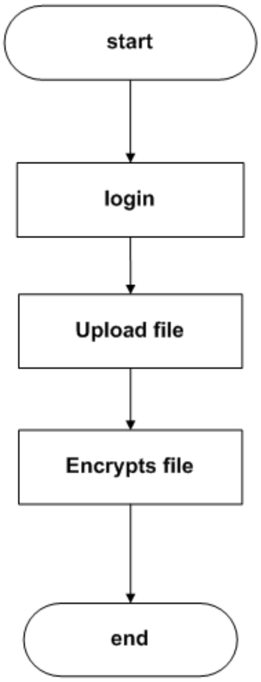
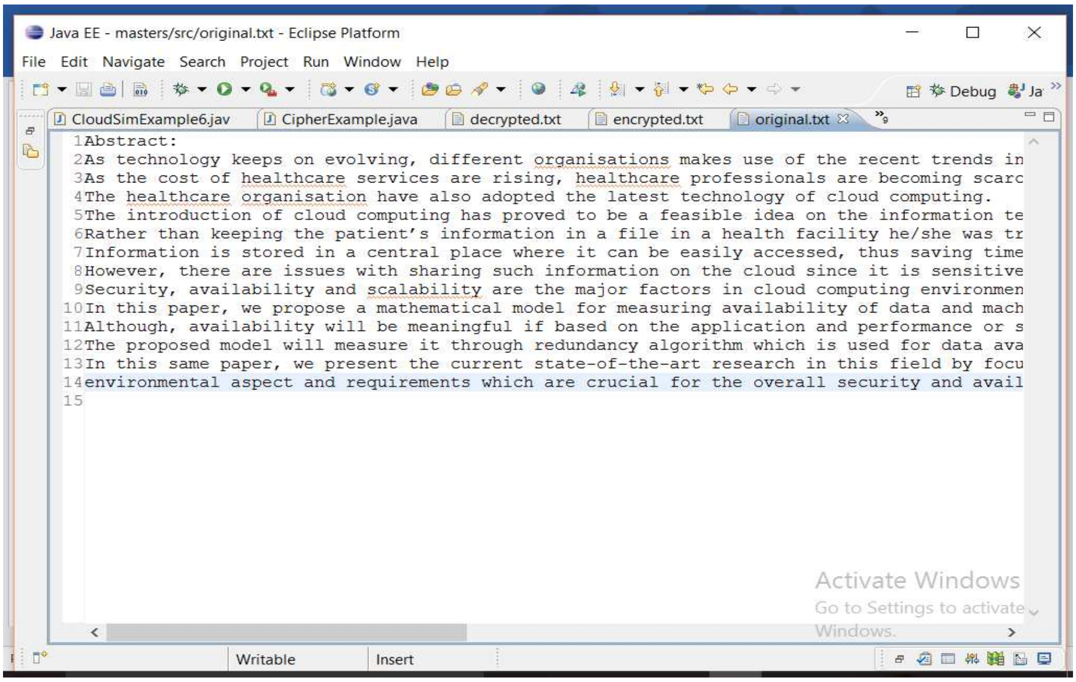
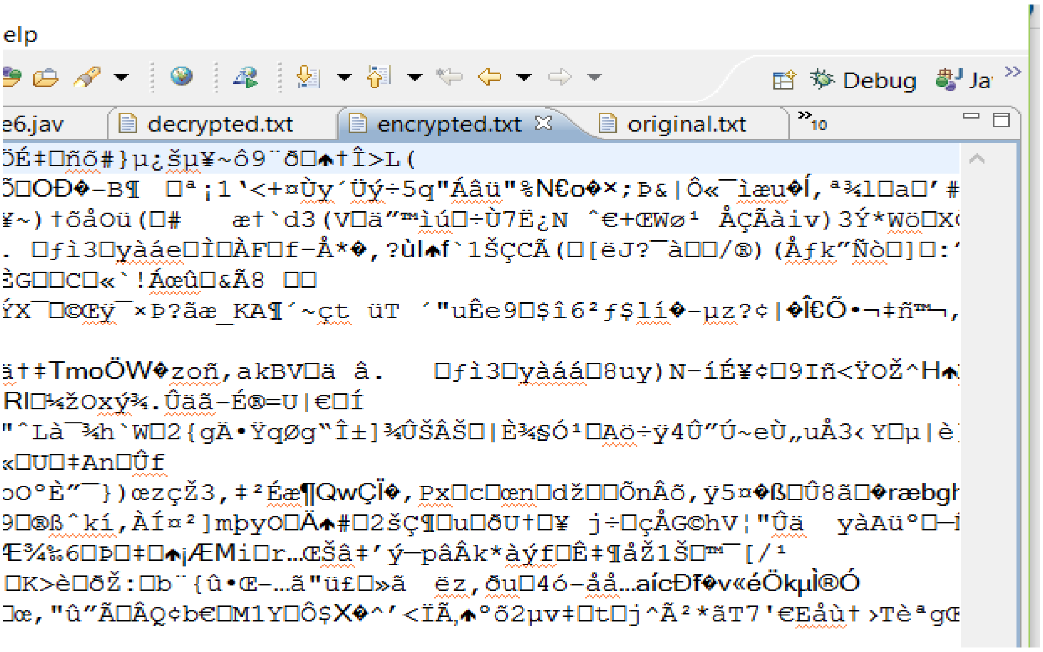


Fig. 10. Flowchart for uploading and encrypting data


Java EE - masters/src/original.txt - Eclipse Platform
File Edit Navigate Search Project Run Window Help
Debug
Ja
CloudSimExample6.jav
CipherExample.java
decrypted.txt
encrypted.txt
original.txt
Activate Windows
Go to Settings to activate Windows.
Writable
Insert

```
Abstract:
As technology keeps on evolving, different organisations makes use of the recent trends in
As the cost of healthcare services are rising, healthcare professionals are becoming scarc
The healthcare organisation have also adopted the latest technology of cloud computing.
The introduction of cloud computing has proved to be a feasible idea on the information te
Rather than keeping the patient's information in a file in a health facility he/she was tr
Information is stored in a central place where it can be easily accessed, thus saving time
However, there are issues with sharing such information on the cloud since it is sensitive
Security, availability and scalability are the major factors in cloud computing environmen
In this paper, we propose a mathematical model for measuring availability of data and mach
Although, availability will be meaningful if based on the application and performance or s
The proposed model will measure it through redundancy algorithm which is used for data ava
In this same paper, we present the current state-of-the-art research in this field by focu
environmental aspect and requirements which are crucial for the overall security and avail
```

Fig. 11. An original file to be encrypted



```
ÕÉ‡□ñõ#}µ¿šµ¥~ô9¨õ□♠†Î>L(
Õ□OÐ�–B¶  □ª¡1'<+¤Ùy´Üý÷5q"Áâü"%N€o�×;Þ&|Ô«¯ìæu�Í,ª¾1□a□'#
¥~)†õåOü(□#    æ†`d3(V□ä”™ìú□÷Ù7Ë¿N ^€+ŒWø¹ ÅÇÃàiv)3Ý*Wö□X
. □fì3□yàáe□Ì□ÀF□f–Å*�,?ùl♠f`1ŠÇCÃ(□[ëJ?¯à□□/®)(Åƒk”Ñò□]□:'
ÈG□□C□«`!Áœû□&Ã8 □□
ÝX¯□©Œý¯×Þ?ãæ_KA¶´~çt üT ´"uÊe9□$î6²ƒ$lí�–µz?¢|�Î€Õ•¬‡ñ™¬,

ã†‡TmoÖW�zoñ,akBV□ä â.   □fì3□yàáá□8uy)N–íÉ¥¢□9Iñ<ŸOŽ^H♠
RI□¼žOxý¾.Ûäã–É®=U|€□í
"^Là¯¾h`W□2{gÄ•Ÿqøg“Î±]¾ÛŠÂŠ□|È¾§Ó¹□Aö÷ÿ4Û”Ú~eÙ„uÅ3‹Y□µ|è
«□U□‡An□Ûf
ÞO°È“¯})œzçŽ3,‡²Éæ¶QwÇÏ�,Px□c□œn□dž□□ÕnÂõ,ÿ5¤�ß□Û8ã□�ræbgh
9□®ß^kí,Àí¤²]mþyO□Ä♠#□2šÇ¶□u□õU†□¥ j÷□çÅG©hV¦"Ûä  yàAü°□–i
Œ¾‰6□Þ□‡□♠¡ÆMi□r…ŒŠâ‡'ý—pâÂk*àýf□Ê‡¶åŽ1Š□™¯[/¹
□K>è□õŽ:□b¨{û•Œ–…ã"ü£□»ã  ëz,õu□46–åå…aícÐf�v«éÖkµÌ®Ó
Œœ,"û“Ã□ÂQ¢b€□M1Y□Ô$X�^'<ÏÃ,♠°õ2µv‡□t□j^Ã²*ãT7'€Eåùt›Tèªg
```

Fig. 12. An encrypted result of the file in Fig. 11

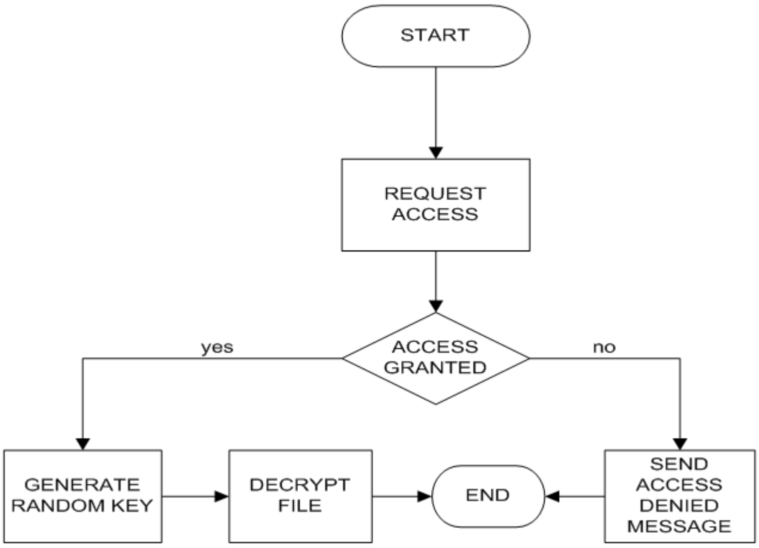


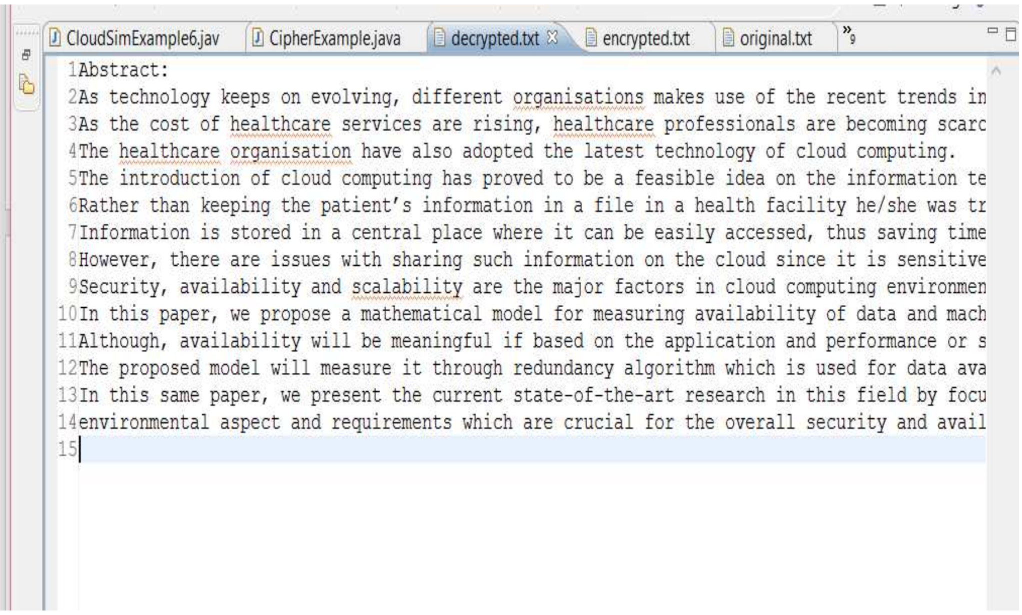
Fig. 13. Flowchart for requesting access to data

Flowchart for Requesting Data

The flowchart in Fig. 13 shows the process of the data user in getting access to the information. This involves access granting, random generation of keys and the decryption of the needed information. The algorithmic descriptions as well as the pseudo-code are also shown for better understanding of the data user part of the proposed system as:

- Registers with the cloud
- Requests data access from the data owner
- Get the random key
- Decrypts data

```
Pseudocode-2 (Data User)
START
SENDS a request to the data owner
IF request accepted
RECIEVES access key
DECRYPT data
ELSE access denied
EXIT
```



```
Abstract:
As technology keeps on evolving, different organisations makes use of the recent trends in
As the cost of healthcare services are rising, healthcare professionals are becoming scarc
The healthcare organisation have also adopted the latest technology of cloud computing.
The introduction of cloud computing has proved to be a feasible idea on the information te
Rather than keeping the patient's information in a file in a health facility he/she was tr
Information is stored in a central place where it can be easily accessed, thus saving time
However, there are issues with sharing such information on the cloud since it is sensitive
Security, availability and scalability are the major factors in cloud computing environmen
In this paper, we propose a mathematical model for measuring availability of data and mach
Although, availability will be meaningful if based on the application and performance or s
The proposed model will measure it through redundancy algorithm which is used for data ava
In this same paper, we present the current state-of-the-art research in this field by focu
environmental aspect and requirements which are crucial for the overall security and avail
```

Fig. 14. Shows the file after decryption

Results after Decryption

The image in Fig. 14 shows the decrypted file. This is basically what the user will be able to see after granted access to the secured information via random key generation. The result is produced in the CloudSim software.

Conclusion

In recent years, cloud computing has become the buzzword in the information technology community. Cloud computing has not only benefited the information technology community, even the health care organisations are benefiting from this technology. The sharing of health information on the cloud had made it easy for health professionals to access patient's information from anywhere around the world. Treatment of patients has now been made easy because the patient history is now available on the cloud. Although the whole world is greatly benefiting from this technology, there are also some issues with the security of data in the cloud. Strong security measures should be implemented so that data does not fall on the wrong hands. A mathematical model is proposed in this study for computing availability of information and servers on cloud computing. This model considers both data and node availability parameters which some of them are static during the cloud lifetime and others have dynamic nature. That means they can change based on the resource capacity or can be varying based on the different algorithm that the systems use. The paper also present the current state-of-the-art research in this field by focusing on several shortcomings of current healthcare solutions and standards and we further proposed a system that will encrypt data before it is being sent to the cloud. The system is intended to be linked to the cloud in such a way that, before the client submits the data to the cloud the data will go through that system for encryption. The paper presents the steps to achieve the proposed system and a sample of the encrypted and decrypted file using our proposed method is given.As a future work the input function for the graph and weigh of graph need more attention for achieving the complete availability model, also, we have intended to work on security model which will be responsible for securing data on the client side. Outside these, there is need to compare our proposed security solution with other existing ones, which is another step to see the performance of our design.

Author's Contributions

All authors equally contributed in this work.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Al-Khanjari, Z., A. Al-Ani and S. Al-Hermizy, 2014. A proposed security architecture for establishing privacy domains in e-health cloud. Eur. Scientific J., 2: 322-330.

Alshehri, S., S. Radziszowski and R.K. Raj, 2012. Designing a secure cloud-based EHR system using ciphertext-policy attribute-based encryption. Proceedings of the DMC, (DMC' 12), pp: 21-25.

Barua, M., X. Liang, R. Lu and X. Shen, 2011. ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing. Int. J. Security Netw., 6: 67-76. DOI: 10.1504/IJSN.2011.043666

Bowers, K.D., A. Juels and A. Oprea, 2009. HAIL: A high-availability and integrity layer for cloud storage. Proceedings of the 16th ACM Conference on Computer and Communications Security, Nov. 9-13, ACM., Chicago, Illinois, pp: 187-198. DOI: 10.1145/1653662.1653686

Calheiros, R.N., R. Ranjan, A. Beloglazov, C.A.F.D. Rose and R. Buyya, 2011. CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Pract. Exp., 41: 23-50. DOI: 10.1002/spe.995

Deshmukh, P.M., A.S. Gughane, P.L. Hasija and S.P. Katpale, 2012. Maintaining file storage security in cloud computing. Int. J. Emerg. Technol. Adv. Eng., 2: 576-580.

Fakhrul, A.O. S.S. Salman-Al-Musawi, A. Khairul and N. Rashid, 2012. A secured cloud based health care data management system. Int. J. Comput. Applic., 49: 24-30.

Gavrilov, G. and V. Trajkovik, 2012. Security and privacy issues and requirements for healthcare cloud computing. Proceedings of the CT Innovations Web, (IW' 12), pp: 143-152.

Hernandez-Ramirez, E.M., V.J. Sosa-Sosa and I. Lopez-Arevalo, 2012. A comparison of redundancy techniques for private and hybrid cloud storage. J. Applied Res. Technol., 10: 893-901.

IHCS, 2013. An overview of cloud security issues facing healthcare organisations and Intel technologies for securing the healthcare cloud. Intel Healthcare Cloud Security.

Ikuomola, A.J. and O. Arowolo, 2014. Securing patient privacy in e-health cloud homomorphic encryption and access control. Internal J. Comput. Netw. Commun. Security, 2: 15-21.

Jouini, M., A.B. Aissa, L.B.A. Rabai and A. Mili, 2012. Towards quantitative measures of information security: A cloud computing case study. Int. J. Cyber-Security Digital Forens., 1: 248-262.

Kaur, P.D. and I. Chana, 2014. Cloud based intelligent system for delivering health care as a service. Comput. Meth. Programs Biomed. 113: 346-359. DOI: 10.1016/j.cmpb.2013.09.013

Khan, M.A., 2016. A survey of security issues for cloud computing. J. Netw. Comput. Applic., 71: 11-29. DOI: 10.1016/j.jnca.2016.05.010

Lohr, H., A. Sadeghi and M. Winandy, 2010. Securing the E-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium, Nov. 11-12, ACM., Arlington, Virginia, USA., pp: 220-229. DOI: 10.1145/1882992.1883024

Mar, K.K., 2011. Secured virtual diffused file system for the cloud. Proceedings of the International Conference for Internet Technology and Secured Transactions, Dec. 11-14, IEEE Xplore Press, pp: 116-121.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing. National Institute of Standards Technology.

Menascé, D.A., 2004. Performance and availability of internet data centers. IEEE Internet Comput., 8: 94-96. DOI: 10.1109/MIC.2004.1297280

Sen, J., 2013. Security and privacy issues in cloud computing. Innovation Labs, Tata Consultancy Services Ltd., Kolkata, India.

Sharma, Y., B. Javadi, W. Si and D. Sun, 2016. Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. J. Netw. Comput. Applic., 74: 66-85. DOI: 10.1016/j.jnca.2016.08.010

Singh, S., Y.S. Jeong and J.H. Park, 2016. A survey on cloud computing security: Issues, threats and solutions. J. Netw. Comput. Applic., 75: 200-222. DOI: 10.1016/j.jnca.2016.09.002

Thilakanathan, D., S. Chen, S. Nepal, R. Calvo and L. Alem, 2014. A platform for secure monitoring and sharing of generic health data in the cloud. Future Generat. Comput. Syst., 35: 102-113. DOI: 10.1016/j.future.2013.09.011

Zhang, R. and L. Liu, 2010. Security models and requirements for healthcare application clouds. Proceedings of the IEEE 3rd International Conference on Cloud Computing, Jul. 5-10, IEEE Xplore Press, pp: 268-275. DOI: 10.1109/CLOUD.2010.62