EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Towards Secure, Flexible and Efficient Role Based Hospital's Cloud Management System: Case Study

Shilpi Harnal[1,*], R.K. Chauhan[1]

[1]Department of Computer Science and Application, Kurukshetra University, Kurukshetra, India

Abstract

INTRODUCTION: Many organizations of health care have recognized that quality of service can be improved by maintaining e-records of patient's reports, medical histories, surgeries recordings, etc. over the multimedia cloud servers. But, the data breach is always a matter of stake for an organization as well as for the patients.
OBJECTIVES: This work has considered a qualitative scenario related to multimedia e-content management for a multi-forte hospital's cloud server.
METHODS: An End-to-End Encryption with the cryptographic algorithm is applied along with an access control framework for secure transmission and storage of e-records.
RESULTS: The results are presented in the form of bar graphs for the time taken to perform encryption/decryption of various media files and combo graphs for different scenarios of access control.
CONCLUSION: This can provide prevention from many attacks/threats, ensures authentication and privacy along with limiting the server usage and cost.

Keywords: Cloud Computing, Role-Based Access Control, Access control, Security, DDOS, Multimedia cloud computing, Hospital, e-Health.

Received on 11 January 2020, accepted on 17 June 2020, published on 22 June 2020

doi: 10.4108/eai.13-7-2018.165497

1. Introduction

To maintain a trade-off between the low capacity mobile devices and the requirement of accessing heavy resources, now numerous users are moving towards the cloud usage. So, cloud computing has become a necessary and most required state particularly for mobile users which provides access to a wide variety of services and resources at any time and from any place [1]. Thereby, the cloud reduces the user's burden to many folds [2]. Nowadays, the maximum of contents shared, stored, produced, and processed via different sources like computers, satellites, smartphones, sensor networks, other medical records, and data, etc. are of multimedia category which includes video, images, gif, and audio contents. This constitutes a major section of the network traffic [3]. Mobile gadgets with minimum required configuration and less processing power stand nowhere and are unable to cope up with the huge manipulations and computing required by other expensive media software. This resulted in the demand for Multimedia Cloud Computing (MCC) [4]. Not only this, multimedia kind of data needs immense computing power and storage capacities but also it presents security as a major concern. Since, the computing, storage and security constraints for the multimedia content are different, this field has drawn a lot of attention and became a popular area of research. It has been also proposed by many researchers to have a separate architecture for multimedia content handling over cloud [5].

But cloud providers and cloud users are in the distinct security domains and are having a dynamic relationship between them. Usually, the major concerns for any service providers are confidentiality, integrity, access control and security of secret and private media objects [6] [7] [8]. Thus, security issues related to multimedia objects require

*Shilpi Harnal. Email:shilpi13n@gmail.com

special attention and solution to maintain the faith and interest of users. Because the integrity of the user's private multimedia files is really a matter of stake for them always. Among various challenges with multimedia cloud computing, the crucial concerns are:

i. *End-to-End Cryptography:* End-to-End Cryptography is the most appropriate and widely approved solution for multimedia cloud security concerns to detect and protect the person's data from unauthorized access [9]. Based on the problems raised while dealing with multimedia data over cloud servers, there are some drawbacks with the existing schemes of security. Based on these limitations, the need for a fast and secure improved cryptography algorithm was raised, as only a strong end-to-end encryption technique can play a major role in the security of sensitive media data.

ii. *Role-Based Access Control:* As in the cloud, users are not legendary by their predefined identities. Therefore identity-based security mechanisms are not of much use. Instead, they are providing accesses based on their characteristics and attributes to achieve confidentiality and authentication [10] [11].

In order to fulfil above concerns for the private and crucial medical records of any patient, this work has applied an improved cryptography procedure for the multimedia record's storage along with End-to-End Encryption while transferring e-records to/from the hospital's cloud server [12]. Also, to deal with the requirement of proper authentication and access control techniques, an efficient and flexible role-based access control (EF-RBAC) model has been suggested [13]. The significance of the improved cryptography algorithm and of EF-RBAC for the enhancement of multimedia cloud technology can easily be illustrated by relating them with any real-world qualitative scenarios. These qualitative scenarios are better known as case studies. This paper presents a possible practical scenario or case study where the suggested cryptography algorithm and access control model can be deployed for performance enhancement. The case study has considered how sensitive e-records of patients can be maintained securely by applying these techniques and how practice sessions for the medical interns can be managed properly at a multi-forte hospital to achieve confidentiality, authentication, integrity, and security.

The following sections include the motivation for the case study, related work, methodology applied and the detailed case study for the hospital e-record - cloud management system. The further section includes the results in the form of combo graphs followed by the benefits & limitations of the proposed scenario.

2. Motivation for Case Study

For an organization, the data breach is always a matter of stake and can be a matter of life for an individual if any personal or sensitive multimedia content is leaked or misused. For any issue of a data breach, the organization has to face various legal issues and sometimes they have to pay high compensations. Some of the recent incidents of security breaches that came into notice are discussed below:

- Outlook: The Microsoft admitted that hackers had succeeded to access many accounts of Outlook.com between January 2019 and March 2019 [14]. Microsoft confessed that they were able to view emails also. The company notified the users whose credentials were infected, but there was no clear picture for an actual number of accounts compromised.
- Skype, Cortana: Another incident is where Microsoft has accepted that personal and sensitive audio conversations of consumers over Cortana virtual assistant and Skype have been listened by third-party contractors [15]. The New FAQ of Skype said that they may have audio recordings transcription, but the user's privacy is protected. They admitted that audio recordings have listened to quality checks only.
- Biostar-2: One of the biometrics company Biostar-2, whose security systems are deployed all over the world was found storing the data in unencrypted form. Such biometric data as records of face recognition, fingerprint scans along with other details of more than one million people have been found in a database that is publicly accessible [16]. A team of security researchers from Israel has succeeded easily by altering the search criteria of URL to gain access to Biostar 2's database including a total of 23GB of multimedia records. This retrieved information belongs to several organizations of many countries such as India, Finland, Sri Lanka, the US, and Indonesia.
- Facebook: According to a report of cyber-security (a research firm) Facebook records of about 540 million users were exposed to the service cloud of Amazon's computing [17]. This was because some of the third-party developers of the Facebook app uses plain sight to post their records.
- Facebook again: Facebook confirmed that data of around 50 million users were at risk, as a vulnerability was exploited by the attackers in July 2017 to access the user's personal content [18]. But this was revealed later in Sep 2018. So they were unaware of how many user's data were compromised from this long time. Later in Nov 2018, a group of unknown hackers hit some other vulnerability of the website and succeeded in capturing tokens of secret access for accounts of millions of Facebook users [19].
- Apple iCloud: Around 500 private and sensitive pictures of many celebrities were disseminated on the image-board 4chan from the iCloud i.e. Apple's services suite cloud [20] [21]. Most of these celebrities were women and many of the pictures posted were having nudity. After that, these were also posted to

other social networks by other users. This was happened because of some security breach at the iCloud suite to allow unlimited attempts of passwords.

- Twitter: According to the author, [19], the multiple vulnerabilities hit twitter. The company revealed the incident and also informed all the affected users.
- Yahoo: As disclosed by Yahoo in 2013, accounts of their 3 billion email holders were likely compromised. The breach was revealed during mid-2016 and it was the largest ever data breach incident [22].
- Google+: After admitting two security flaws or vulnerabilities in the Google+ platform, Google had finally shut down Google+ or G+ in April 2019. These flaws in the API had exposed data of many subscribers through the friends of users using the G+ app to third-party developers [19] [22].
- Amazon: Because of the misconfiguration of Amazon's S3 buckets over the storage server of Amazon, the customer's data were set for anyone's access in public [23]. Even analysts at cybersecurity firm claim that elastic block storage (EBS) of Amazon they can access customer's database easily.

Apart from the above-mentioned cases, a survey by Techworld also claims the breach of security at some other service providers as well, such as T-Mobile, TalkTalk, Zomato, Uber, Pizza Hut, FIFA, British Airways and Microsoft Office 365, etc. Also one of the media company Cultura Colectiva of Mexico exposed a total of 146 GB of various user's data. Another database exposed by an app named as At the Pool, includes user IDs, photos, friends, various check-ins, etc. for about 22,000 users. All these scenarios raise the need for secure end-to-end encryption during transmission and storage of sensitive e-media records of patients. Also, a strong access control mechanism is always required for providing protection against unauthorized accesses. This work fulfills both the requirements with the earlier proposed cryptography algorithm [12] and efficient & flexible role-based access control mechanism (EF-RBAC) for a hospital's cloud server [13].

3. Related Work

It is also important to note here that, this necessity of generating, accessing, sharing, storing, editing and transmitting media contents over unsafe internet source by millions of clients' raises issues like bandwidth, jitter, delay throughput in terms of Quality of Experience (QoE) and Quality of service (QoS). Here, another major concern is the security of sensitive and crucial media objects of clients to ensure integrity and confidentiality. Such requirements can become a kind of bottleneck for the traditional cloud providers and can lead to an unsatisfactory experience for clients [24] [25].

Akter, Gani et al. (2018) have analyzed that the use of multimedia applications and services for e-health is getting popular day by day. By this people can access their personal health records (PHRs) such as health history X-ray reports, MRI, EEG/ECG data, clinical audio-visual reports, insurance policy, and ultrasound reports electronically at any time from any location through any handheld electronic devices. It's the responsibility of health care providers to manage uploads and security of such crucial/sensitive information over the cloud. Thus, authors have proposed the usage of personal storage service over the cloud for managing these records, such as OneDrive, Dropbox and Google Drive, etc. [26].

The authors Stergiou, Psannis et al. (2018), have proposed a network of a new type that could provide more appropriate multimedia data transfer facilities. They have also discussed the use of various analysis tools and simulators tools that could be used for the study of the collection, the management, the analysis, the processing and of the storage for the rich media data of large volumes. They have measured the performance of the network with CloudSim [27].

Noura et al. (2018), have stated that while handling multimedia objects the major pronounced effects were the impact of privacy, integrity and confidentiality breaches for a media service provider. According to them, the application of encryption is the proven technique to handle these threats. They have analysed two recent cipher techniques based on the two rounds for the protection of image contents [28].

Joseph, Vazhacharickal et al. (2017), have analysed that security of multimedia contents while in storage or transmission has become extremely important with the growing demand for multimedia keeping, computation, and sharing. The authors believe that traditional techniques of encryption using DES and AES are difficult to use for encryption of multimedia data. This is because of certain features of rich multimedia contents like high redundancy is possible, large in volume and requirement of real time functioning [4].

Shankar (2018) has stated that cryptography can be the best approach to maintain availability, integrity, and confidentiality of sensitive digital data. The author has proposed an optimized RSA algorithm to ensure the secure transmission of images with high secrecy and confidentially among the sender and the intended receiver [29].

Nowadays, some application providers like WhatsApp, TextSecure and Gmail, etc. have started providing E2EE. Similar to other providers of email, the Gmail application also supports end-to-end encryption based only on Transport Level Security (TLS), according to which data is available to the server only but not accessible during transmit. Thus, many cloud users are forced to use some applications from third-party vendors to perform encryption/decryption for their critical and private information before sending it over the cloud. Such applications are well known as domain client (DC) applications. Song et al. (2014) have suggested an Encrypted Cloud i.e. EnCloud, which involves a mechanism for achieving end-to-end encryption among the service providers and cloud users, to maintain user's trust by facilitating their tasks. Hence, it proves that cloud

applications and services could be compromised anytime without providing encryption at the end-to-end level. Anyhow, a user could not afford to lose their crucial and sensitive multimedia data at any cost [30].

According to authors Bethencourt et al. (2007), the traditional access control schemes such as mandatory or discretionary access control models cannot be applicable for an open cloud environment [31]. Role-based access control (RBAC) scheme, assigns roles to users based on their least privileges and functions required to perform a job. The Goyal et al. (2006), said that Task Role-based access control model (TRBAC) is considered as a viable scheme for the cloud computing environment. According to authors, in TRBAC access permissions can be validated dynamically based on the user's role and the task assigned to the user [32].

Another proposed variant for cloud computing by Yang et al. (2012), is the Attribute-role-based access control (ARBAC) model. For this scheme, data objects are assigned with some attributes and values. To access these object's attributes, the user has to provide that particular value and access is provided by the cloud server only after this validation is complete [33]. Some other authors as Ristenpart et al. (2009), have proposed a fine-grained key-based ARBAC model with the provision of preserving the privacy of the attribute's values corresponding to an object using the symmetric/private key encryption schemes to protect its privacy [34].

Shafiq et al. (2005), have suggested that certain roles should be fixed and static in some applications, while permissions and users for roles might be assigned dynamically [35]. Ruj et al. (2011), have proposed the involvement of a certified third party for assigning roles to users. They have also proposed to inculcate certain parameters (such as all possible timings and locations of access) to each user's profile to maintain the trust/authentication of users [36].

Thus the discussion has shown the work done by various authors in the field of security measures for multimedia cloud computing. The work in this paper has presented an improved solution for these security issues in terms of security, attacks prevention, cost, auditing, server response time and operational efficiency as discussed in further sections.

4. Methodology Applied for Case Study

Thus, it is clear from the above literature that the security of confidential and private data over the cloud is always an issue of stake for clients and only a strong cryptography technique with End-to-End Encryption can manage the integrity and confidentiality of data both at cloud storage and during transmission. Otherwise, the cloud will always be vulnerable to users and organizations. Also, it is clear from the literature that an effective access control mechanism can mitigate the chances of security breaches by unauthorized users and untrusted insiders.

4.1. Improved Cryptographic Framework Applied [12]

This framework applies a secure and improved symmetric procedure with the provision of randomly generating the secret key for media contents cryptography. The applied hybrid procedure is an advanced and improved version of the blowfish algorithm for better security while storing/retrieving text and other multimedia objects (like gifs, audio, images, video or any other sort of media contents) to and from the media aware cloud server. Primarily blowfish algorithm was applicable for the text files only. This proposed framework works with end-to-end encryption (E2EE) policy. Thus, before transmitting any content to the server, encryption for the same is performed at the client's site and after retrieval of any content from the cloud server, the decryption is also performed at the client's end. This proposed approach guarantees a high level of privacy and security for the personal multimedia contents of patients and also it is efficient to apply over various types of multimedia objects. The general framework for the scheme is presented in figure 1 shown below:

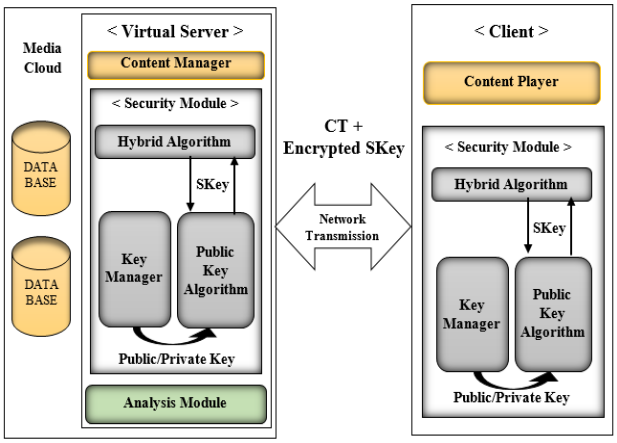

Figure 1. E2EE based proposed framework for multimedia cloud computing [12]

The Sequence of steps for this framework are as follows:

1. The client raises a request for any multimedia object.
2. Content manager verifies the request.
3. Analysis module verifies the availability of servers and other parameters.
4. Key manager is responsible for the availability of both asymmetric and symmetric (Skey) keys.
5. Skey is used for the encryption/decryption of media object (CT) using the improved hybrid symmetric algorithm and asymmetric encryption is used for encrypting Skey for secure transmission over the network.
6. Both encrypted object (CT) and the encrypted Skey is transmitted to another end (client or server) to maintain E2EE.

The detailed description and comparison of the applied improved blowfish hybrid algorithm are presented by us in the referred paper and the pictorial representation is shown in figure 2.

This improved hybrid algorithm was developed using JAVA and executed using the command-line interface. The setup was applied and tested by encrypting multimedia files of various types and sizes. Further, the encrypted files were also tested over the cloud

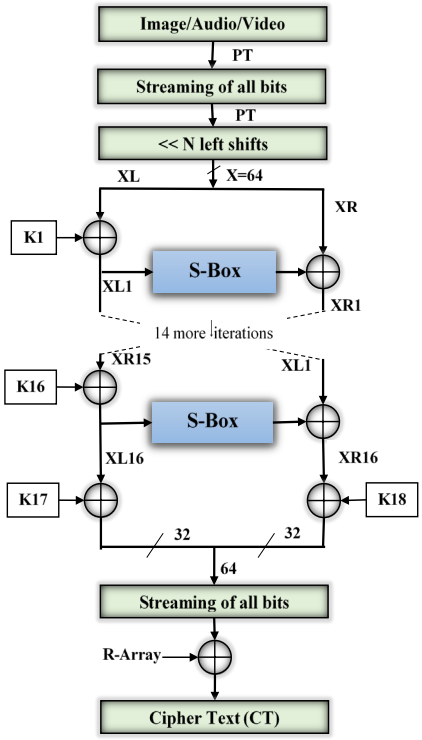

Figure 2. The Steps of Improved Hybrid Algo. [12]

4.2. EF-RBAC Framework Applied [13]

With Efficient and Flexible Role-based access control (EF-RBAC) framework system users are dynamically provided with some roles as needed and as per the policy of the organization. Accesses/Permissions are applied for the specific roles and the same permissions automatically get applied to all the users of that category or with the same role. The roles are chosen very carefully by the authorities as per the organization's requirements. Every new user is assigned with a minimum one role and one user can have multiple roles as well. The roles are assigned based on the least privilege policy. The roles and their respected users are applied with some constraints such as each user is provided with a limited number of required transactions based on their role in a day. If the user's transaction count reaches predefined threshold value, then the user's limit exceeds and the server stops listening from that user.

This scheme has added provision of gifting/borrowing transactions to/from one another (within authenticated registered users having the same role only). So that if some users do not need more number of transactions in a day, he/she can gift or borrow his/her transactions with other users of the same role to implement security mechanism to the roles of the system.

Role-based access control (RBAC) is a methodology of proscribing network accesses, which support only the roles of individual users within an enterprise. Consequently, the number of requests to the server decreases and encompasses a limit, as each user has a count on its access to cloud servers. This leads to improved/reduced response time and decreases the overhead of servers. Additionally, it provides prevention against distributed denial of service (DDoS) attacks. The detailed description of this framework is shown in figure 3 given below.

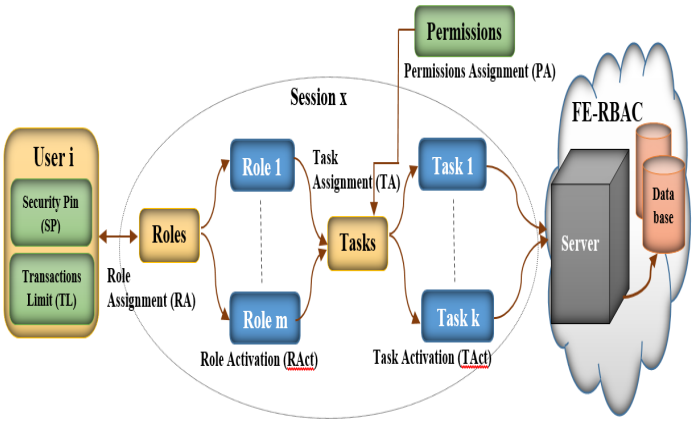

Figure 3. Proposed Efficient and Flexible Role Based Access Control Model [13]

Figure 3 is depicting how a User 'i' is assigned with one or multiple active roles in the organization and one or multiple tasks are activated accordingly. Tasks are executed within their boundary of permissions for accessing cloud services and resources. The main features of the Efficient and Flexible Role Based Access Control framework (EF-RBAC) are defined as follows:

- Multiple active sessions are possible at a constant time; however, there is just one active session for one active user at a time.
- Each user entered in the organization is assigned with a role (Multiple roles can be allocated to a user similarly) and each role has a limit over the number of transactions that can be used.
- Among the numerous roles outlined for an organization, every role has some predefined rules, attributes and transaction limits.
- Every role has a specific number of tasks and every task is associated with certain permissions specific to roles.
- Each user manages a personal security PIN number and also keeps a record of his/her transactions used till now.
- Once transactions limit exceeds for a user, e.g. if the user 'A' makes a request for a transaction from another user 'B' having the same role, firstly user 'A' will have to seek permission from user 'B' for his/her one-time

security PIN (Because user 'A' is required to provide security PIN of user 'B' before accessing transaction from user B's account). After the transaction of 'A' is over, the secure PIN is autogenerated again.

- Once this limit exceeds (e.g. of user 'A'), either the user can request a transaction from another user with the same role or the server stops taking further requests from that user's side for that specific role.
- Further if any suspicious behavior is detected like a user is trying to make repetitive attempts after his limit is exceeded or if the user is trying to access a file that he/she is not authorized to access or if the user is trying to make an unauthorized update, etc., then the Role-Based access control mechanism will analyze and report the attempt to authorities.

Steps of EF-RBAC Algorithm:

1. Start
2. Create R Roles, N Users, P Transactions
3. Limits the transactions (T_Limit) for each Role
4. Assign Role and T_Limit to each user
5. Initially Set T_Used = 0 for each user
6. Submit array of VMs to DataCenter Broker.
7. **Repeat While (User i has some task to execute)**
8. {
9. **If (T_Used[i] < T_Limit[i] AND User[i] has task)**
   -Submit Cloudlet to Broker
   -Broker assigns Cloudlet to available VM
   -VM executes the Cloudlet and send response
   -Set T_Used[i] = T_Used[i]+1
10. **Else If (T_Used[i]=T_Limit[i] AND User[i] has task)**
    -Notify the User about the Limit Exceed
    -If (User wants to request Transaction from j User)
        -Make a request for security PIN to user j
        -Submit security_PIN[j] and Cloudlet to Broker
        -Broker assigns Cloudlet to available VM
        -VM executes the Cloudlet and send response
        -Set T_Used[j] = T_Used[j]+1
        -Auto-generate security_PIN[j] for user j
11. **Else If (T_Used[i]=T_Limit[i] AND User[i] has no task)**
    -Notify the User about the Limit Exceed
12. Notify the server about users limit, where N=Total number of users
13. } [End of while loop of step 7]

This work has implemented proposed Efficient and Flexible Role-Based Authentication Control (EF-RBAC) over the cloud using CloudSim (version 3.0) simulator tool to limit the number of accesses a user can have in a day and to add the provision of gifting or borrowing transactions from other users. Cloudsim tool provides an extensible and generalized seamless modeling framework.

5. Hospital E-Record - Cloud Management System

According to many health care organizations around the world, the quality of medical service can be improved by maintaining electronic records of patient's reports, medical histories, video recordings of surgeries, etc. over the multimedia cloud servers. This enables a patient and a doctor to access these records from any location in a cost-effective manner for better health and effective resource utilization [39]. But it's been a challenging decision and task to migrate to complete electronic cloud medical systems for managing sensitive and crucial medical records of patients.

5.1. Overview

Chiang et al. (2018), have performed a study to discuss advanced practices in medical technology and self-consciousness among people regarding them [37]. Because of these factors, the usage of tools to support e-medical records has been promoted by the World Health Organization (WHO). These e-medical records facilitate the patients, doctors and medical interns to access the records online. By this efficiency of the medical system is enhanced.

This case study is taking an example of a multi-forte hospital that incorporates specialists/doctors, patients, and several medical interns. Patients having any sort of sicknesses visit the concerned doctor and get a complete check-up from them. The complete database of the patient's records is maintained over the cloud servers. By this, patients and concerned doctors can access their crucial health records (PHRs) such as health history X-ray reports, MRI, EEG/ECG data, clinical audio-visual reports, insurance policy, and ultrasound reports electronically at any time from any location through their electronic smartphones or any handheld electronic devices [26].

This case study includes a number of appointed medical interns at a multi-forte hospital. The medical intern is the one who has completed his/her medical school (degree of MBBS) of four and a half years to serve as a professional doctor in India. But these medical interns cannot practice medicine in an unsupervised manner as they do not yet have a complete license as a physician. According to the Medical Council of India to get a permanent license to practice as a primary care doctor, they have to go through a compulsory internship of one year in various fields of specialties. These medical interns are associated with experienced doctors during their one year of training.

This case study provides a better provision for managing sensitive e-Records of patients and arranging practice sessions for medical interns as well. This works with the practice of uploading videos of any surgeries performed by the specialists and private medical histories for reference to the cloud server, but only with the patient's consent. These reports and videos of any patient are very sensitive and it's the responsibility of their health care provider or administrator to manage uploads and security of such crucial information over the cloud.

5.2. Challenges with Ordinary System

Cloud has greatly relaxed the users from the burden of storage, heavy computations, etc. through its services [38]. Now users or patients, in this case, prefer to store their crucial data over the cloud servers only in encrypted formats. The major challenges with ordinary media service providers are:

- If the patient's credentials and multimedia records of their reports, videos are stored in plain text format, then there is always a risk to security.
- The problem arises when some other unauthorized entities desire to access the data of patients they are not authorized to access.
- There may be chances that even an authorized user tries to access the data of patients they are not authorized to access.
- Another problem grows when data is transmitted between cloud users and servers in an unencrypted format through untrusted networks. This can raise chances of man-in-the middle attack and also can affect the integrity and confidentiality of the data.
- Also a problem of non-availability of service or denial of service (DoS) grows if any malicious user forges as an authentic user and floods the server with dummy requests.
- The Problem of non-availability of service or denial of service (DoS) can also generate even if any authentic user intentionally floods the network to disturb the normal service.

Trust is the crucial factor for data sharing, storage, and transmission, as it can avoid potential risks and can overcome uncertainties. There is still a lack of proper access control and security policies over the ordinary cloud to maintain reputation and trust. Thus, this work addresses the above issues of access control, integrity, confidentiality, and security for any patient's personal and sensitive medical records.

5.3. Entities Involved with Proposed Case Study Solution

This solution work towards providing a system with flexible access with secure transmission & storage on the basis of policies/permissions decided by the hospital authorities and patient's consents. The least entities required to flexibly participate for such a secure system control are shown through the UML use case diagram in figure 4 and are described as follows:

i. *Patients:* The person undergoing any treatment in the hospital. They can access their medical records anytime from cloud storage.
ii. *Doctors:* A doctor is a person who performs checkups of patients and starts their treatments accordingly. Each doctor is associated with a department and can supervise/assist many medical interns. A doctor can access the records of their respective patients only.
iii. *Medical Interns:* They are associated with doctors of their respective departments. They are like medical trainees and appointed after their medical degree completion. They will be certified physicians only after completion of their internship.
iv. *Hospital Cloud Server:* It's the third-party multimedia service provider cloud server. It provides storage, sharing, editing, security and backups for all the multimedia records discussed above and other credentials all the entities.

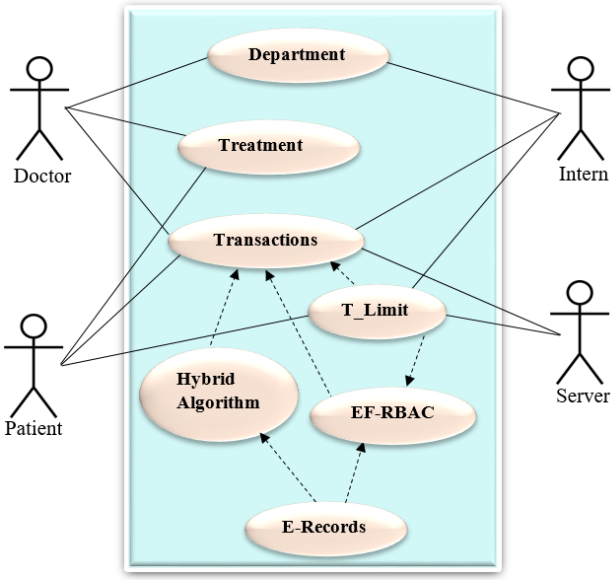

Figure 4. Entities for Case Study

The UML use case diagram of figure 4 has depicted the major functionalities of the purposed case study system for hospital cloud along with entities involved in the system. Here T_Limit represents the Transaction limit defined for any of the users belonging to a specific role. The detailed description of functionalities is covered in further sections.

5.4. Description of Proposed Solution

The general model of the proposed solution for the Hospital e-Record Cloud Management system with all the above defined entities is presented in figure 5. Here both client and server-side modules are having EF-RBAC and projected improved cryptography algorithm. The transmission of multimedia contents between the two parties is secured with E2EE using the improved algorithm [12]. Access control is provided with EF-RBAC and every access is provided based on the roles defined per entity and permissions defined for each role [13].

The steps and rules involved in the normal functionality of the Hospital e-Record Cloud Management System are shown in figure 5 and a relational schema for this system including all entities is depicted with the help of an ER Diagram in figure 6.

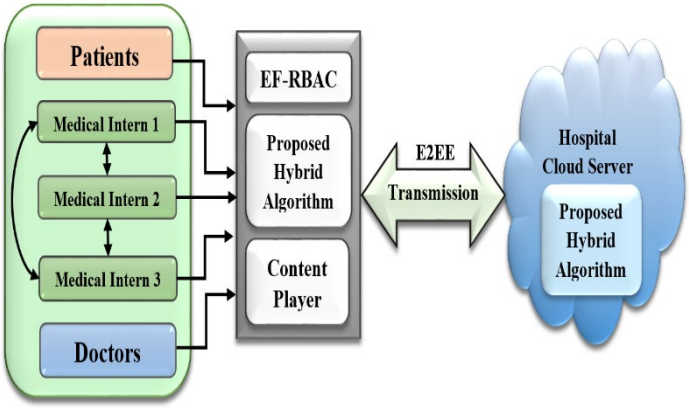

Figure 5. Hospital e-Record Cloud Management System

The rules are defined as follows:

- Roles are defined as per entities involved except server that means the system has three defined roles as Patients, Doctors and Medical Interns. Each entity is defined by a particular ID, as included in the ER Diagram depicted in figure 6.
- Each doctor and the medical intern is associated with one department, such as Pathology, Orthopedic, Dental, Emergency, Gynecology, Anesthetics, Laboratory, Cardiology, Cancer, Neurology, etc. The departments are not shown in figure 5 for the sake of simplicity, but they are part of the ER Diagram of figure 6 as essential content.
- Each patient is getting treatment and concerned with one doctor only. But one doctor can treat multiple patients at the same time. Patients can upload and access their medical records to/from the media cloud server. Doctors can only be able to access the records of their specific patients only.
- As per the proposed EF-RBAC scheme, the users are provided with limited transactions (T-Limit) for a day to limit the load at the server. Any limit can be decided for doctors and patients. Because generally, they are never going to exceed their transaction limit.
- The problem is mainly associated with the transaction limit of medical interns. As they can overload or flood the server fully if a hospital has thousands of interns. This can result in the unavailability of servers for others and also it will increase the rental cost for the hospital. Medical interns use the Hospital e-Record for the study of medical histories, reports and to view videos of live surgeries for their self-reference.
- Thus to limit the server's load and to reduce the usage cost of the rented server, here the proposed work has limited the number of transactions to be allowed per day for each medical intern.
- Assuming the limit is five for each user with a medical intern role. Side by reducing cost, this will also minimize the misuse of the system. If the limit exceeds for an intern, he/she can borrow a transaction from any other medical intern by sharing a secure PIN or the server stops answering their requests.

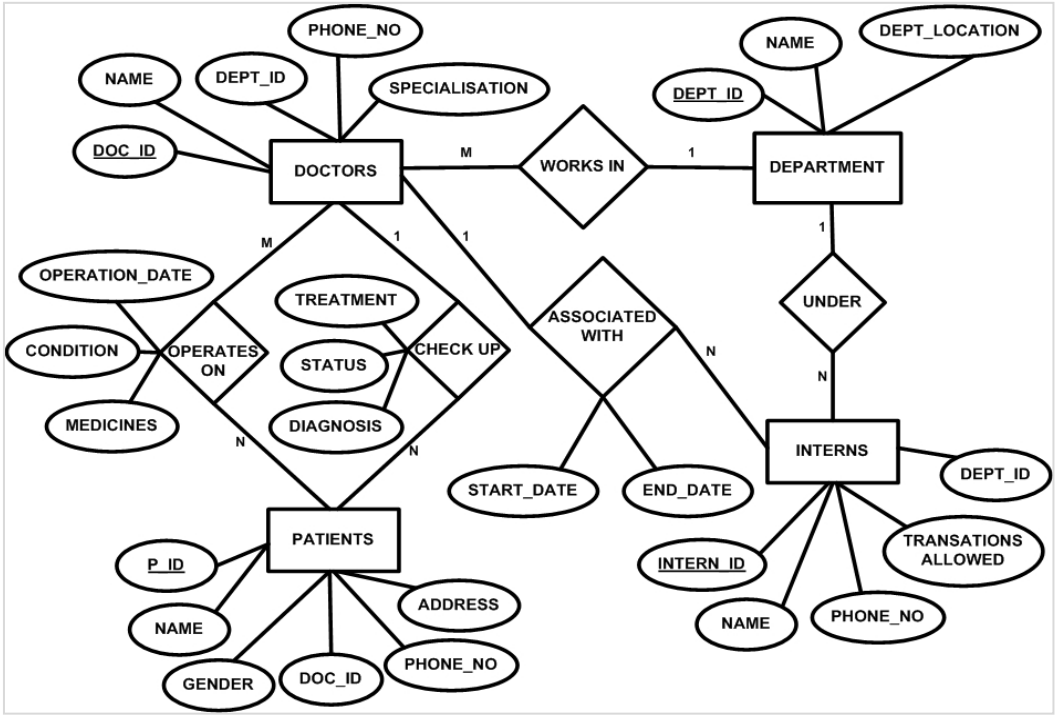

Figure 6. ER-Diagram for Hospital e-Record Management System.

- At last, for privacy and data breach preservation, data is encrypted with the fast and secure improved algorithm for storage as well as for transmission in encrypted form i.e. E2EE.

As discussed a case study describes the real experience of users/organizations with a cloud server. Here, the study has considered a qualitative scenario for the understanding of practical applications of discussed improved hybrid algorithm and EF-RBAC model. That is related to multimedia content management for a Hospital e-Record Management System. This can guarantee privacy and security with E2EE and helps to reduce cost by limiting server usage. It also provides prevention from many attacks and threats as discussed in further sections. Thus, it is clear from the case study that the work can be very useful if deployed with cloud applications and the advantages are very appealing.

5.5. Steps of Proposed Solution

The steps of the procedure to execute each transaction corresponding to each user with encryption/decryption of multimedia object using the hybrid algorithm are as follows:

1. Start
2. Create R Roles, N Entities, P Transactions
3. Limits the transactions (T_Limit) for each Role
4. Assign Role and T_Limit to each entity
5. Initially Set T_Used = 0 for each entity
6. Submit array of VMs to DataCenter Broker.
7. **Repeat While (Entity i has transaction to execute)**
8. {
9. **If (T_Used[i] < T_Limit[i] AND Entity[i] has task)**
   -Submit Cloudlet/Transaction to Broker
   -Broker assigns Cloudlet to available VM
   -VM executes the Cloudlet with hybrid algorithm
   -Set T_Used[i] = T_Used[i]+1
10. **Else If (T_Used[i]=T_Limit[i] AND Entity[i] has task)**
    -Notify the Entity about the Limit Exceed
    -If (Entity requests Transaction from j Entity)
      -Make a request for security PIN to entity j
      -Submit security_PIN[j] and Cloudlet to Broker
      -Broker assigns Cloudlet to available VM
      -VM executes the Cloudlet with hybrid algorithm
      -Set T_Used[j] = T_Used[j]+1
      -Auto-generate security_PIN[j] for user j
11. **Else If (T_Used[i]=T_Limit[i] AND User[i] has no task)**
    -Notify the Entity about the Limit Exceed
12. Notify the server about entities limit, where N=Total number of entities
13. } [End of while loop of step 7]

6. Results and Discussion

6.1. Complexities of the Proposed Solution

As the improved hybrid algorithm is block cipher algorithm and usually works with a block of fixed size (here, each block is equivalent to 64 bits), thus the hybrid procedure is independent of the input and takes approximately the same time, i.e. O(1). But, as the input multimedia files are bigger in size and divided into M blocks during the procedure. So here, the complexity is O(M) of the hybrid algorithm, for data of M blocks to be encrypted [12].

For ordinary access control systems where there is no limit over the number of transaction's usage for users, the complexity will be difficult to measure, as the usage may vary always. But, the complexity analysis by applying the EF-RBAC scheme (embedded with the hybrid algorithm) having the limit over transactions is always possible and defined in table 1 as follows:

Here, N: Number of entities/interns, M: Number of blocks in a file to encrypt and P: Number of transactions.

Table 1. Complexity analysis for EF-RBAC scheme

Sr. No.	Scenario	Complexity
1.	Role assignment to users	O(N)
2.	Task assignment to users	O(N)
3.	Execution of one Transaction or Cloudlet with one object of M blocks	O(M)
4.	Looping through all the users for task execution	O(N*P)
5.	Looping through users to find the users of the same role, in case of request	O(N)
6.	Looping through users for task execution and then looping to find the users of the same role, in case of request	O(N*P*M)

6.2. Simulation Results of Proposed Solution for medical e-records [12]

Firstly, this section analyses and compares the rate i.e. the time consumed by the proposed improved procedure to perform encryption and decryption of multimedia e-records of various sizes and types. Thus, the proposed algorithm found to be working perfectly with a variety of files of various types and sizes such as audio, images or video files. The algorithm has shown hopeful results for every input file. The time consumed for performing encryption and decryption excluding the time of key generation, for sample media files of various types and sizes are presented in table 2.

Table 2. Sample data and time taken by the hybrid cryptography algorithm [12]

Sr. No.	File Type	File Size in KBs	Encryption Time (MS)	Decryption Time (MS)
1	Image	3233	208	165
2	Image	4830	295	235
3	Image	6308	383	287
4	Audio	4209	264	193
5	Audio	6374	392	291
6	Video	7289	419	320
7	Video	9171	524	401
8	Video	11305	662	516

The input media file's size is measured in kilobytes (KBs) units and the corresponding time taken for decryption and encryption has been measured in milliseconds (MSs). The resultant cipher text files have tested successfully over the cloud server by uploading and retrieving from the cloud without any error. The complete procedure of implementation is carried out over Pentium dual-core processor with 2GB of RAM, the results are expected to be improved with more advanced processors.

Further, this section presents the results of the simulation in the form of tables generated at the end of every transaction or cloudlet execution by medical interns/users. For resultant tables, the headings are represented in the first column for clarity of facts, such as User-IDs, Roles-Assigned, Transactions-Limit (T-Limit), Transactions-Used (T-Used), Transactions-Left (T-Left), Transactions-Rejected (T-Rejected), Transactions-Borrowed (T-Borrowed), Transactions-Gifted (T-Gifted), and User-Blocked. These headings are the same as the parameters used with the algorithm. The rest of the cells are depicting the value corresponding to each user. Here, the simulation has taken the following parameters:

- **Us: {u1, u2, u3, u4, u5, u6, u7}**
  // N=7 users are defined for the system
- **Ro: {r1, r2, r3}** // R=3 roles are defined
- **Ts: {t1,…, tm}**
  // P=70 transactions are defined
- **Transactions-Limit (T-Limit):** 5 for each user with r1, 10 for r2 and 15 for r3
- **Transactions-Used (T-Used):** Transactions used by the user till then, Initially zero
- **Transactions-Left (T-Left):** Transactions left with user till then, Initially zero
- **Transactions-Borrowed (T-Borrowed):** Transactions borrowed from another user with same role
- **Transactions-Gifted (T-Gifted):** Transactions gifted to other users with the same role
- **Transactions-Rejected (T-Rejected):** Number of attempts by the user once the limit exceeds
- **User-Blocked:** yes/no, whether the user is blocked for the day or not

Table 3 shows the simulation status after the execution of 57 transactions/cloudlets with CloudSim simulator. The illegal transactions are rejected by the EF-RBAC algorithm. There could be two possibilities of rejection, that is if the user tries to execute any task after the limit exceeded or secondly, if the user tries to gain access for some record for which he/she was not permitted.

Here, according to table 3 for scenario-1:

- user1 (i.e. u1) with role1 (i.e. r1) is blocked after the limit exceeded and also u1 has tried 2 illegal attempts after that.
- The user3 (i.e u3) has borrowed 2 transactions after limit exceeded, one from u4 and another from u5 and get blocked after that.
- Figure 7 is depicting the combo graph (Bar graph along with the Line graph) for the complete scenario of table 3.
- The 3 bars i.e. sky blue, light green, and orange are showing Transactions-Limit, Transactions-Used, Transactions-Left for each user respectively.
- The red line represents the illegal attempts corresponding to Transactions-Rejected, the black line represents the Transactions-Borrowed and green line represents the Transactions-Gifted.
- The users with illegal attempts or with rejected transactions are blocked for the day.

Table 3. Simulation Status Scenario 1

User-IDs :	u1	u2	u3	u4	u5	u6	u7
Role-Assigned :	r1	r1	r2	r2	r2	r3	r3
T-Limit :	5	5	10	10	10	15	15
T-Used :	5	2	10	7	9	11	13
T-Left :	0	3	0	3	1	4	2
T-Borrowed :	0	0	**2**	0	0	0	0
T-Gifted :	0	0	0	**1**	**1**	0	0
T-Rejected :	**2**	0	0	0	0	0	0
User-Blocked :	**yes**	no	**yes**	no	no	no	no

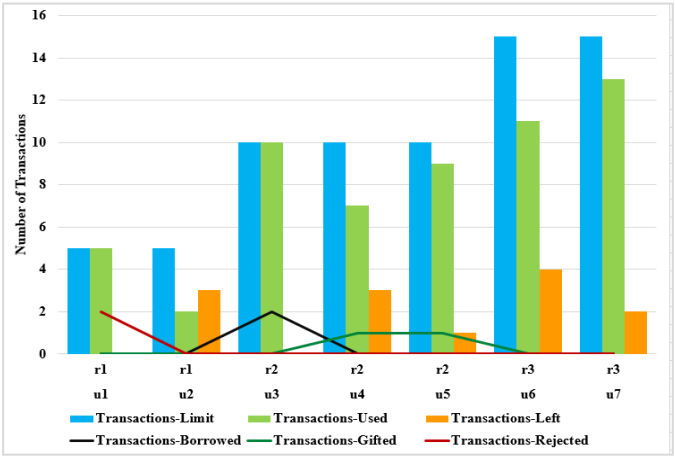

Figure 7. Simulation Status Scenario 1

Here, according to table 4 for scenario-2:

- user1 (i.e. u1), user3 (i.e. u3), user4 (i.e. u4) and user5 (i.e. u5) are initially same as of table 3.
- But user4 (i.e. u4) has made 4 illegal attempts and user6 (i.e. u6) has tried 5 illegal attempts. Thus, u4 and u6 were blocked by the server even if they were left with transactions.
- The red line in the graph is depicting illegal attempts.

Table 4. Simulation Status Scenario 2

User-IDs :	**u1**	**u2**	**u3**	**u4**	**u5**	**u6**	**u7**
Role-Assigned :	**r1**	**r1**	**r2**	**r2**	**r2**	**r3**	**r3**
T-Limit :	5	5	10	10	10	15	15
T-Used :	5	2	10	8	9	12	13
T-Left :	0	3	0	2	1	3	2
T-Borrowed :	0	0	**2**	0	0	0	0
T-Gifted :	0	0	0	**1**	**1**	0	0
T-Rejected :	**2**	0	0	**4**	0	**5**	0
User-Blocked :	yes	no	yes	yes	no	yes	no

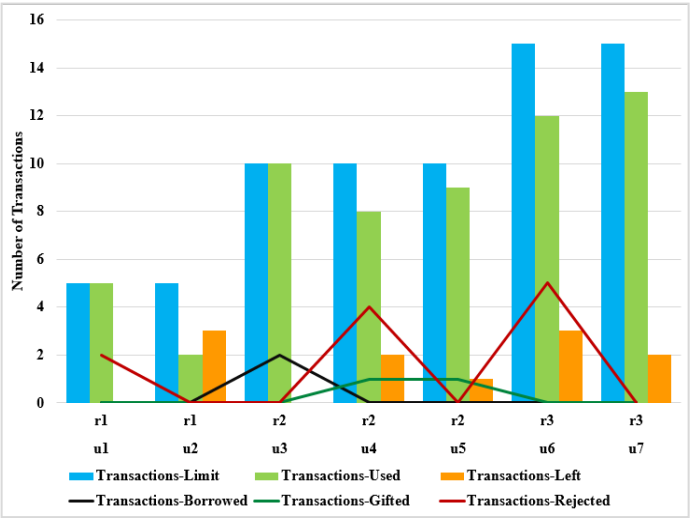

Figure 8. Simulation Status Scenario 2

7. Benefits & Limitations of the Proposed Framework

7.1. Benefits

The proposed approach works on providing end-to-end encryption (E2EE) to end-users of multimedia service cloud of a multi forte hospital. Also, users are assigned roles based on the least required privileges for an object. Every access is tracked and any practice of unauthorized accesses is also captured. In nutshell, this can be said that this scheme is scalable, dynamic and support active and passive workflow in the system. Apart from these, the proposed mechanism can also provide the following benefits:

- *Authenticated Access only:* The proposed framework assures an entity for authenticated access to their personal media records, as only an authentic entity will be able to decrypt and encrypt the secret key by applying their own private key for E2EE.
- *Integrity and Confidentiality:* The proposed scheme also addresses the most critical and required factors for every cloud service provider that is integrity and confidentiality. Only authorized users can view the information which provides confidentiality and no access is possible during transmission of data to preserve integrity.
- *Accessibility and Scalability:* The scheme suggested here is quite flexible and scalable enough based on the client's requirements on a pay as you use basis.
- *End-to-End Encryption (E2EE):* E2EE is the primary feature of the proposed framework for protecting the confidential, critical and personal multimedia information of clients during transmission.
- *Protection against Distributed Denial of Service Attacks (DDoS):* With limited accesses scheme this will also provide protection against distributed denial of service (DDoS) attacks. As no attacker can control the services with limited accesses.
- *Decreased threats on the server:* It will minimize the risk of information access by the intruders by limiting the accesses for users. Also, it reduces the chance of information misuse by even authentic users, as only required information is available to them under the least privilege policy.
- *Reduces the cost of organization:* As the model is scalable enough, the cost of management, operations, and maintenance also varies according to services availed with time.
- *Improved server response time & operational efficiency:* It reduces server workload by limiting the per day accesses as per users/roles, unlike ordinary access control methods. This leads to higher operational potency and better response time for the servers.
- *Separation of duties and auditing*: This model reduces conflicts by separating each permission for tasks, tasks specific to roles and roles for each user. The auditing process gets simplified by this approach.
- *Delegation of tasks:* This policy leads to easy auditing and visibility of tasks for administration. Thus if any user is overloaded with tasks, then the administration has the choice to delegate his/her duties to different users.
- *Improved security as it follows the least privilege principle:* As data is a valuable asset nowadays, this scheme is surely enhancing the security from suspicious attempts from internal and external users. So

it is decreasing the risk of data leakage and breaches by intruders.

- *Limited network usage if the organization has numerous employees:* No matter the number of employees an organization hires, the network usage will always be limited. The network cost and server cost will always be measurable with the proposed scheme.
- *Compliance enhancing:* As most of the costs are countable, it gives the ability to easily verify all the policies and activation compliances.
- *Safeguard against attacks:* Framework presented here is efficient to apply for any media cloud service environment as it can provide complete prevention and acts as a safeguard against various attacks such as brute force attack, side-channel attacks, non-repudiation, man-in-middle attack, etc.

7.2. Limitations

Sometimes if the roles of users are changing dynamically, it may create confusion regarding which user is associated with which privileges. Roles are assigned on the basis of the least privilege principle, but still, if roles are changed frequently then some confusion may arise.

8. Conclusion and Future Scope

Ultimately it can be said with the firm belief that the only cloud has the potential to handle and manage the future needs of accessing media contents of any organization. Although, at the same time cloud servers and clients also have a number of security and privacy-related issues of concern that require special handling. This work has discussed a case study scenario related to multimedia content management for a Hospital e-Record Management System to describe the actual experience of users/organizations with cloud server after deployment of the improved E2EE cryptography scenario and EF-RBAC model.

It is clear from the case study that it can greatly help to reduce cost, limit server usage, guarantees privacy and security, prevention from many attacks and threats, etc. Thus, it can be concluded that the work can be very useful if deployed with cloud applications and the advantages are really very appealing. The future research is possible in the area to develop an efficient and secure indexing method to quickly locate a required image or any other multimedia objects from the huge amount of encrypted multimedia files by the cloud servers.

References

[1] Zhu, W., Luo, C., Wang, J. and Li, S. (2011). Multimedia Cloud Computing. IEEE Signal Processing Magazine, 28(3), pp 59-69.

[2] Rong, C., Nguyen, S.T. and Jaatun, M.G. (2012). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, Elsevier, ScienceDirect, 39(1), pp 47-54.

[3] Harnal S. and Chauhan R.K. (2016). Multimedia Support from Cloud Computing: A Review. In International Conference on Microcom-2016, IEEE, NIT, Durgapur.

[4] Joseph, S.K., Thomas, G. and Vazhacharickal, P.J. et al. (2017). Multimedia encryption in cloud computing: an overview. IEEE 13th International Workshop on Multimedia Signal Processing, pp. 1-13.

[5] Varghese, B. and Buyya, R. (2018). Next generation cloud computing: New trends and research directions. Future Generation Computer Systems 79, ScienceDirect, Elsevier, pp. 849–861.

[6] Ning, J., Cao, Z., Dong, X., Liang, K., Wei, L. and Choo, K.K.R. (2017). CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage. IEEE Transactions on Services Computing, IEEE, pp 1-14.

[7] Alani, M.M. (2016). Security Threats in Cloud Computing. Elements of Cloud Computing Security, Chapter, Springer Briefs in Computer Science, DOI 10.1007/978-3-319-41411-9_3, pp 25-39.

[8] Zhong, H., Zhu, W., Xu, Y. and Cui, J. (2016). Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. Springer-Verlag Berlin Heidelberg 2016.

[9] Tekeoglu, A. and Tosun, A.S. (2015). A Closer Look into Privacy and Security of Chromecast Multimedia Cloud Communications. IEEE International Workshop on Multimedia Cloud Communication (MMCloudCom 2015), pp. 121-126.

[10] Meghanathan, N. (2013). Review of Access Control Models for Cloud Computing. In proceedings of the third International Conference on Computer Science, Engineering & Applications, 3(1), pp. 77-85.

[11] Wang, W., Han, J., Song, M. and Wang, X. (2011). The Design of a Trust and Role Based Access Control Model in Cloud Computing. In proceedings of the 6th International Conference on Pervasive Computing and Applications, IEEE, ICPCA-2011, pp. 330-334.

[12] Harnal S. and Chauhan R.K. (2019b). Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing. International Journal of Innovative Technology and Exploring Engineering (IJITEE), Scopus, Elsevier, Vol. 8, Issue 10, pp. 918-924.

[13] Harnal S. and Chauhan R.K. (2019a). Flexible and Efficient Role-Based Access Control (FE-RBAC) Mechanism for Cloud. EAI Endorsed Transactions on Scalable Information Systems, Thomson Reuters-ESCI, Web of Science Database, pp. 1-10.

[14] ANI (2019). Outlook security breach: Microsoft admits that hackers accessed email accounts, content for six months. Article, Economic Times.

[15] IANS (2019). Microsoft contractors listening your Skype, Cortana chats. Article, Economic Times.

[16] Ganjoo, S. (2019). New data breach exposes fingerprints and face recognition records of millions of users. Article, Technology news.

[17] Silverstein, J. (2019). Hundreds of millions of Facebook user records were exposed on Amazon cloud server. Article, CBS NEWS.

[18] Perez, S. and Whittaker, Z. (2018). Everything you need to know about Facebook's data breach affecting 50M users. Article, TechCrunch.

[19] Kumar, M. (2019). iCloud Possibly Suffered a Privacy Breach Last Year That Apple Kept a Secret. Article.

[20] Arthur and Charles (2014), "Naked celebrity hack: security experts focus on iCloud backup theory". The Guardian Retrieved.
[21] Charlton, A. (2015). "iCloud accounts at risk of brute force attack as hacker exploits 'painfully obvious' password flaw". Article
[22] Techworld, Staff (2019). The most infamous data breaches. Survey, TechWorld.
[23] Whittaker, Z. (2019). Hundreds of exposed Amazon cloud backups found leaking sensitive data. Article, TechCrunch.
[24] Zhang, Q., Ji, Z., Zhu, W. and Zhang, Y.Q. (2002). Power-minimized bit allocation for video communication over wireless channels. IEEE Trans. Circuits Syst. Video Technol., 12(6), pp. 398–410, June 2002.
[25] Kilkki, K. (2008). Quality of experience in communications ecosystem. J. Universal Computer Sci., 14(5), pp. 615–624, 2008.
[26] Akter, M., Gani, A., Rahman, M.O. and Hassan, M.M. (2018). Performance Analysis of Personal Cloud Storage Services for Mobile Multimedia Health Record Management. IEEE Access, 6, pp 52625-52638.
[27] Stergiou, C., Psannis, K.E., Plageras, A.P., Ishibashi, Y. and Kim, B.G. (2018). Algorithms for Efficient Digital Media Transmission over IoT and Cloud Networking. Journal of Multimedia Information System, 5(1), pp 27-34.
[28] Noura, H.N., Noura, M., Chehab, A., Mansour, M.M. and Couturier, R. (2018). Efficient and secure cipher scheme for multimedia contents. Multimedia Tools and Applications, Springer, 78(11), pp 14837–14866.
[29] Shankar, K. (2018). An Optimal RSA Encryption Algorithm for Secret Images. International Journal of Pure and Applied Mathematics, Scopus, 118(20), pp. 2491-2500.
[30] Song, Y., Kim, H. and Mohaisen, A. (2014). A PrivateWalk in the Clouds: Using End-to-EndEncryption between Cloud Applications in a Personal Domain. C. Eckert et al. (Eds.): TrustBus 2014, LNCS 8647, Springer International Publishing Switzerland 2014, pp. 72–82.
[31] Bethencourt, J., Sahai, A. and Waters, B. (2007). Cipher text-Policy Attribute-Based Encryption. Proceedings of the IEEE Symposium on Security and Privacy, pp. 321-334.
[32] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006). Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data. Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98.
[33] Yang, K. and Jia, X. (2012). Attribute-based Access Control for Multi-Authority Systems in Cloud Storage. Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, pp. 536-545.
[34] Ristenpart, T., Tromer, E., Shacham, H. and Savage, S. (2009). Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds. Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, USA, pp 199-212.
[35] Shafiq, B., Joshi, J.B.D., Bertino, E. and Ghafoor, A. (2005). Secure Interoperation in a Multi-domain Environment Employing RBAC Policies. IEEE Transactions on Knowledge and Data Engineering, 17(11), pp. 1557-1577.
[36] Ruj, S., Nayak, A. and Stojmenovic, I. (2011). DACC: Distributed Access Control in Clouds. Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. pp. 91-98.
[37] Chiang, D.L., Huang, Y.T. and Chen, T.S. (2018). Applying time-constraint access control of personal health record in cloud computing. Enterprise Information Systems, Article, pp 1-16, DOI: 10.1080/17517575.2018.1522452.
[38] Yan, Z., Li X., Wang, M. and Vasilakos, A.V. (2017). Flexible Data Access Control based on Trust and Reputation in Cloud Computing. IEEE Transactions on Cloud Computing, 5(3), pp 485-498.
[39] Almulhim M., Islam N. and Zaman N. (2019). A Lightweight and Secure Authentication Scheme for IoT Based E Health Applications. International Journal of Computer Science and Network Security, 19(1), pp 107-120.