Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 3715–3724, DOI 10.12694/scpe.v25i5.3113

# A SECURE DATA STORAGE APPROACH FOR ONLINE EXAMINATION PLATFORM USING CLOUD DBAAS SERVICE

SRINU BANOTHU[*], G. JANARDHAN[†], G. SIRISHA[‡], SRINIVASULU SHEPURI[§], MADHAVI KARNAM[¶], AND ALLAM BALARAM[‖]

**Abstract.** For the time being, many government or private organizations for recruitment of staff or educational institutions moving towards online based tests. The online examination system is a software application used for conducting examination using computer systems. It helps to the recruitment agency or any govt. or private organizations for conducting any job recruitment examinations transparently. Due to this system results are processed without delay and efficiently evaluated to assess the candidate's abilities. But the biggest challenge for online examination system is data integrity, security and privacy. The current system is resolving the privacy issue by providing authentication credentials such as user name, password to the candidates. So that only authorized users with proper credentials can login to the system and attempt the exam. But the data confidentiality and integrity are biggest challenges for the system. As the data stored in system database is in plain text format, hence it may be modified or misused by the internal staff of the organization. This paper presents the frame work for secure storage and management of candidate's data using encryption scheme, distributed databases in cloud database system. The proposed framework enhances the data confidentiality, integrity and avoids any cheating by internal staff or third party institutions. This paper conducts experimental work on proposed framework and analyses the results of the system.

**Key words:** online examination system, data security, cloud database, encryption, distributed database

## 1. Introduction.

Now a day's most of the recruitment agencies such as government or semi government are conducting online examination as part of recruitment process for faster evaluation and recruitment process [1]. Many recruitment agencies are gradually replacing paper examinations by online examination systems due to various information technologies and rapid evolution of network technology. Online examination systems improve the efficiency and quality of the examination and make the examinations not limited to places and regions [2]. Existing online examination system modes consist mainly of Client/Server (C /S) and Browser/Server (B /S) structure [3,4]. For the C /S examination system, examination center is autonomous. During the examination, examination questions and examination information are pushed down to examination center by the administrator. The examinee is able to take the examination at examination center. This type of structure is mostly distributed in local area network. Candidates can only take the exams within the prescribed environment that is limited to some extent in terms of time and space. In addition, this type of system has a low carrying capacity, it is not easy to scale up, it is easy to lose candidates' answers in emergency situations and there are some issues like disconnected examination systems and problems with data synchronization which make it difficult for B/S based examination systems to be widely used, which is why a new technology is needed to solve this dilemma [5].

The emergence of cloud computing is the result of the rapid evolution of the next generation Internet technology. It is a new form of neural computing mode [6–8] that allows computing to be distributed on many distributed computers instead of on local computers or on remote servers. It is a result of the integration of distributed computing and utility computing technologies, virtualization technologies, web services technologies, grid computing technologies, and others. The purpose of CC is to enable users to utilize virtual resource pools

[*]Dept. of CSE, Vignan Institute of Technology and Science, Deshmukhi(v), Yadadri Bhuvanagiri Dist, Telangana, India, 508284
[†]Dept. of CSE, Vignan Institute of Technology and Science, Deshmukhi(v), Yadadri Bhuvanagiri Dist, Telangana, India, 508284
[‡]Dept. of CSE, CVR College of Engineering, Mangalpally(V), Ranga Reddy Dist, Telangana, India, 501510
[§]Dept. of CSE (AIML), AVN Institute of Engineering and Technology, Hyderabad, Telangana state, India, 501505
[¶]Dept.of CSE, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India, 500090
[‖]Department of CSE, MLR Institute of Technology, Hyderabad, Telangana - 500043. (bmadhaviranjan@yahoo.com)

as much as possible at any time, anywhere on the network to solve large scale computing problems. One of the services offered by CC is Software as a Service (SaaS). SaaS is a type of software application mode which provides software services on the Internet and is the latest trend in software technology development [9, 10].

In addition to SaaS, double cache and adapter technologies are used to solve the problem of examinees answer loss and the problem of data synchronization between the examination systems in unexpected circumstances. As a result, CC offers a technical solution to the current design of the online examination system.

Conducting examination through online platform is having many advantages: it avoids the major issues of recruitment process such as paper leakage, recently it became biggest issue in telangana state(India), the internal staff of the Telangana State Public Service Commission soled the Group-I, Assistant Executive Engineering examination papers and earned the lot of black money. With this many people's life whoever were sincerely prepared for getting job got spoiled. And also completes the recruitment process smoothly without any delays. Hence, many recruitment agencies are moving towards online examination platform. Besides advantages of this system, it also facing some issues related to user authentication and secure storage of candidate marks data. The marks obtained by the candidate plays a vital role in recruitment process, so biggest challenge is security and integrity of the marks data stored in database system. It became so significant to solve security issues; otherwise many qualified candidates lose opportunities. With these things in mind, a frame work for secure storage of marks data in cloud database system is proposed. [11] Cloud computing is a technology that provides data processing and storage services through internet on rental basis. One of cloud computing services is Database as a Service (DBaaS). The cloud Database as a Service (DBaaS) enables users to outsource data in cloud database system and access whenever required through any devices connected to internet. DBaaS provides organizations with unlimited data storage services cost-effectively with higher availability and easy deployment. Now a day's most of the organizations or individuals are outsourcing their databases to the cloud environment.

The objective of this research is to develop a secure data storage and management system in cloud for online examination system using distributed databases and data encryption algorithms to meet the challenges facing by recruitment agencies.

**2. Literature Survey.** Any recruitment organization can plan, administer, and oversee exams in an online setting with the help of an online examination system. It helps the inspector by lessening the workload associated with administering tests, examining answer sheets, and generating results [12]. In light of this, online tests have become increasingly common in recent years. Although many young students disclose personal information on social media, Okada et al. [13] noted that their attitudes change when it comes to e-assessment since they are more worried about data privacy, security, and safety.

Cluskey et al. [14] studied all the feasible approaches to conduct online examinations without supervision. This paper presented the detail discussion about cheating scenarios used by students and also measures to avoid cheating by students. Authors have guided few methods for building an online testing plan and few online examination control techniques such as taking tests at one set time using Respondus Lockdown Browser (RDL), checking student ID, and so on.

Authors [15] proposed an approach to identify student's movement in online examination using Convolution Neural Networks (CNN). The problem with this approach is that the position and orientation of students cannot be analyzed and requires much data to preview the data. And this approach is not focused on the security of data stored in database.

Mukta et. al. [16] worked on Adaptive Test Sheet Generation in E-Learning using Fuzzy Logic Approach. Authors guided the employing of an ambiguous technique of assessing students favorite tests in the e-learning.

Jung and Yeom [17] discussed about how to secure an online examination system using cryptography group. However, it needs the use of higher quality webcams and microphones. This is a disadvantage of the system. They have not concentrated about the protection of data from insider attackers.

Paul et al [18]. proposed a system where in the production manager of the questionnaire selects a percentage of complexity for questions that must be met. The program can generate papers in accordance with the format indicated by the administrator and subsequently save it in PDF format, enabling colleges to receive it upon clicking send.

Zhen and Su [19] suggested a methodology for designing a question paper template based on the input

requirements.

The paper [20] proposed a few strategies for the face identification system on this respect. The authors have defined how neural networks (NN), Support Vector Machines (SVM), and Algebraic characterization may be utilized in face reorganization systems. The colleagues and jain presented the significance of a blockchain technology network in the online examination system. Authors introduced blockchain based online examination system. They employed the 'Smart contracts', it is one of the better applications and a 'Ethereal' public blockchain platform [21]. They have additionally compared the general effectiveness of the blockchain-based method with the cloud-based scheme.

Lee and et al. developed in [22] a system that classifies student's VFOA information by capturing their head pose estimates and eye movement estimates using advanced technologies artificial intelligence approaches.

The papers [23, 24] proposed the approaches for user authentication and prevention of malpractices by users. Authors also proposed approaches for identification of misconduct of users during examination.

The authors of [24, 25, and 26] proposed the approaches for secure storage of data in cloud environments and performances of various database encryption algorithms for ensuring the confidentiality of data stored in cloud database systems. An unauthorized user cannot access data in an e-learning system. Only students who have been authenticated and granted permission can view exam data uploaded by teachers. One common technique for access control is encryption.

A session key establishment protocol was presented by Kausar et al. [27] for a predetermined duration, such as a class, seminar, or exam. The session key, which encrypts messages using symmetric cryptography, is distributed using a public key infrastructure, and message integrity is ensured by a hash-based message authentication code.

To properly finish the login procedure in Al-Hawari and Alshawabkeh's study [28], students must enter the exam instance session password correctly; the exam instance session password was produced automatically by the examination management system, and it wasn't made public until the instructor revealed it at the start of the relevant class. Few prior investigations [27, 28] have reported the possibility of a single point failure, the inability to prevent communication parties' repudiation actions, and the inability to resolve internal conflicts. In order to efficiently upload and download data in cloud-based systems, Sahaya et al. [29] presented a strategy that first encrypts the message using DES and then encodes it using Reed Solomon code in the data centers. However, it doesn't have precise access control.

The common problem identified from the above literature is that there are no approaches focused on security to the marks data stored database system. The marks obtained by the candidate may be modified by the internal staff of the organization by miss using authentication credentials. Instead our proposed model focuses on security and integrity of the data stored in database systems

**3. Proposed System.** To address security issues of marks data in online examinations systems and for better availability and scalability of the system. This work proposes a new framework using cloud services, cryptographic algorithms and data distribution. It is hopeful that proposed work overcomes the issues of data confidentiality, integrity and availability. These are three key measures of data security. Here a brief overview of proposed approach is presented with figure 1for secure data storage and management of online examination systems using one of cloud service such as Cloud Database as a Service, data distribution and cryptographic algorithms. The objectives of proposed system are also discussed.

**3.1. System Model.** This system is having three major modules such as 1) users 2) administrator and 2) Cloud databases.

*Users:* The users are candidates who write the examination, every user is having authentication credentials such as username and password for login into the system. Once users are signed in they will write and submit examination. After submission users marks data and personal information will be stored in local database servers of the system.

*Administrator:* An administrator is a person who is responsible for whole data management such as data encryption, data outsourcing to cloud database servers, key generation, ensuring data privacy and security. An administrator plays a vital role and should be a main responsible person for ensuring privacy and security to online examination data.

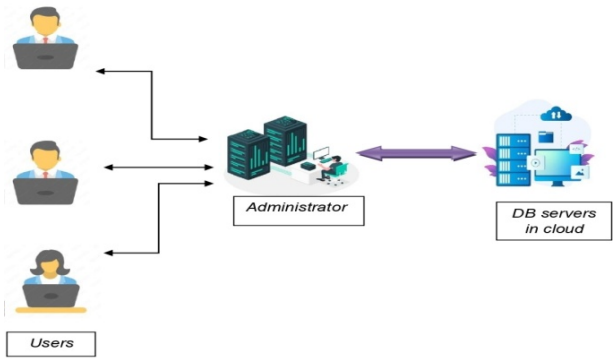


Fig. 3.1: Cloud based secure data storage system for storing online examinations marks data.

*Cloud Database Servers:* The proposed system uses the cloud DBaaS service for secure storage of candidate's data. Data storage in cloud provides many benefits such higher data availability, security and scalability etc.

**3.2. Design Objectives.** *Access Control:* The question paper submitted by any recruitment agency can be accessed by authenticated users only during given time period. Answer sheet and score obtained by candidates are accessible to administrator only. The administrator can provide access policies when cipher text of data is generated and stored in distributed data storage servers. Only the users who satisfy the access policy can view the data.

1) *Data Confidentiality:* System keeps data highly confidential from unauthorized people access.
2) *Data Tampering resistance or Ensuring Data Integrity:* Data integrity is a key issue for online examination system. Any unauthorized entity in the cloud environment or local servers should not modify the data. Otherwise, it violates the transparency of the online examination system.
3) *Collision Resistance:* when one key is not enough for data decryption, 2 or more unauthorized entities may try to combine their keys for decryption of data. System ensures that combine keys cannot decrypt correct plain text.
4) *Data availability:* As data is outsourced to cloud environment, cloud service providers always keeps data available to be accessed by authorized persons whenever needed. It provides higher scalability.

**4. Methodology.** This section presents the methodology of proposed system. Proposed approach achieves key elements of data security such as data confidentiality, data integrity and data availability. The aim of this approach is to securely outsource and manage the data of online examination using cryptography algorithms, data distribution and cloud services. The proposed approach uses cryptographic algorithms and vertical fragmentation feature of distributed database to achieve data confidentiality and data integrity. In this approach vertical fragmentation plays a vital role for achieving data confidentiality. Vertical fragmentation is a technique to split the database table vertically into two or more sub table fragments with chosen columns. As database tables are partitioned vertically with selected columns into two or more sub tables and distributed data into multiple database servers in cloud, the internal staff of the cloud service provider cannot get complete information about a record. So it keeps the data secure from insider attack in cloud environment. The cloud services are used for proving better data availability and scalability. Proposed system uses the Cloud Database as a Service (DBaaS) for storing data in cloud environment, Advanced Encryption Standards (AES) algorithm for cryptographic operations (i.e encryption and decryption of data) on data. As AES is more secure and robust algorithm, it is chosen for cryptography operations. AES uses keys of variable length such as 128,192 and 256 bits length keys, for 128 bit key, about 2128 attempts are required to break the cipher. This is very difficult task for the hacker to hack the data. The framework consists of two major modules: users and Administrators.

*Users:* users login to the online examination system using authorization credentials and attempt the test, after test is over submit the test. This test data will be stored in systems local database servers.

*Administrator:* Administrator is an owner of the data stored in systems local database servers, performs tasks such as data encryption and outsourcing to cloud environment for ensuring data privacy and security. For achieving data security issues, the proposed framework consists of two phases

*Setup Phase.* In this phase, administrator does the data pre-processing, outsourcing and user authorization

1. Administrator encrypts the database table attribute values using advanced encryption standard algorithm (AES) with a secret key (this key only knows to the administrator). Administrator uses SHA 256 authentication algorithm for generating 256 bit secret key.
2. Splits the table vertically into 2 or more sub tables with selected columns (i.e. vertical fragmentation). While splitting tables, in each sub table columns are included using a factor called key and data sensitivity. The maximum number of possible sub tables depends on number of columns of a table. Each sub table must includes at least two columns
3. Add row index column in each sub table and insert row index value in index column, it should be the same value for a row in every sub table. This helps to identify each sub records of a row of actual table (i.e. before splitting of table) and merge the records of fragmented tables into a record of original table (i.e. before partition). Row index column values are unique and not in encrypted form.
4. Finally, upload the vertically partitioned table data into multiple database server platforms of the same cloud environment. Choose different locations of data centres to store the data of partitioned table fragments. This makes very difficult to an attacker or internal staff to get complete record information of a table as records are partitioned and stored in different data centres.

*Retrieval Phase.* In this phase, the administrator sends the data retrieve request to all database servers where fragmented data is stored in cloud. The key attribute to select the records from fragmented tables is row index value. The cloud database server returns requested records data in encrypted format from multiple sub table fragments. An application merges the records data into a record of original table (before fragmentation). Then administrator gives input as secret key and then decrypted results are shown to the user. Only one key is used for data decryption The algorithms for secure data uploading to the cloud environment and retrieval are shown in Algorithm 1 and 2.

## 5. Implementations and Results.

*Experimental Setup.* For experimental results we have used the cloud service from cloudcluster.in and software technology PHP (Hypertext Preprocessor) for application development and MySQL database server for backend data store. For testing the results of our proposed model, initially we have created a account in cloudcluster.io, cloud cluster provides a complete managed open source application cloud service on kubernetes cloud for cloud DBaaS service. In which we have deployed two MySQL database servers with configurations of servers on cloud platform are:3(core) Processors, 4GB RAM, 100GB SSD and chosen data centers at two different locations for storing the fragmented table data. Then developed a small application in PHP and installed MySQL database server on local system for storing dataset. The data set is created with random values of marks in the range from 0 to 50. Data set includes fields such as candidate id, test id, marks scored. XAMPP server is installed on our local system to run an application. Our system is configured with Intel core i5 processor, 10GB RAM and 360GB hard disk space. System is connected to the internet of 150mbps Network speed. The results are shown in below figures.

For experimental purpose, we have created a database table named as testscore with fields such as id, candidateid, testid and testscore, in our local machine.

Figure 5.1 shows the records inserted into the testscore table in local system. The records in the database table are stored in plain text format or readable format. Then created two table fragments, one with fields id, candidateid, testid and other with id, testscore in two different cloud database servers. Here attribute id is a row index added in both table fragments. Later, run our application on our machine to encrypt, split and insert encrypted records into cloud database servers as shown in figure 5.2, in which records with selected columns are stored in encrypted format. Finally, figure 5.3 shows the encrypted data stored in fragmented table. Both table fragments are having same values for every row for row index attribute id.

### 5.1. Performance Analysis.

*Performance Evaluation.* The performance of proposed scheme is evaluated by considering the parameters such as time taken to encrypt, split and upload data into cloud environment and time taken to retrieve the

**Algorithm 1** Database upload to cloud

```
Procedure databaseupload(dbname, tablename, secretkey )
{

Inputs: local database name, table name, secret key as inputs
Output: encrypted and vertically partitioned table
segments uploaded to database servers in cloud        ▷ generate the 256 bit hash code of secret key using SHA256
algorithm and save key in local database system

Hashed_key=sha256(secret_key);
                                          ▷ Select the table data to be outsourced from local database server

if(num_of_rows≥ 0)
{

while (all rows are processed)
{
      ▷ Select one row and encrypt all column values of selected row using AES256 algorithm with hashed secret key.

C1=encrypt (column-1)
C2=encrypt (column-2)
C3=encrypt (column-2)
C4=encrypt (column-2)
.
.
Cn= encrypt (column-n)
Insert (row-index, C1) into tablefragment1 in cloud
Insert (row-index, C2) into table fragment 2 in cloud
Insert (row-index, C3) into table fragment 3 in cloud
Insert (row-index, C4) into table fragment 4 in cloud
Insert (row-index, C5) into table fragment 5 in cloud
.
.
Insert (row-index, Cn) into table fragment
N in cloud
} } }
```

data from cloud database and view results to the users. The time to upload data (UT) considered the time of AES algorithm for data encryption (ET), communication cost (CC) and query execution time (QET).

$$UT = ET + CC + QET \tag{5.1}$$

The time to retrieve the data (RT) from cloud database servers, considered the time of AES algorithm for data decryption (DT), communication cost (CC) and SELECT query execution time (SQET). Here SELECT query without predicate is used for retrieving all the records from database.

$$RT = DT + CC + SQET \tag{5.2}$$

The performance of data upload time and retrieval time are tested by considering the data sets with variable number of records. The performance of the system in terms of time in seconds to upload data and retrieval data are shown in figure 5.4.

*Security Alalysis.* The security of our proposed approach is analyzed against to insider attacks and outsider attacks. The data is strongly protected against the insider and outsider attackers in such a way that as data is encrypted and distributed into multiple database systems if attacker compromises the data in one fragment,

**Algorithm 2** For Secure retrieving of data from the cloud DB

```
Procedure database_ retrieve (dbname, tablename, secretkey )
{
                                        ▷ Cipher text can be from your MySQL data or from a user input via a web form.
                                                    ▷ This example will use user input cipher text to decrypt.
    ▷ generate the 256 bit hash code of secret key using SHA256 algorithm and compare with saved key in database

Hashed_key=sha256(secret_key);
                                                                        ▷ compares decryption key

if (decryption key matches with encryption key)
{
                                                ▷ retrieve the records from table fragment1 in cipher text format

Sql1=SELECT * from fagment1;

if (num_rows_of_fragment1 ≥ 0)
{                                                                       ▷ select one record from fragment1

While (all rows of fragment1 are processed)
{              ▷ select records from table fragment2 matching id with id of record selected from table fragment 1
                                                        ▷ merge records retrieved from fragment 1 and 2

$ row= $ row1+$ row2;          ▷ decrypt all column values using AES decryption algorithm and secret key

P1= decrypt (column-1)
P2= decrypt (column-2)
P3= decrypt (column-2)
P4= decrypt (column-2)
.
.
.
Pn= decrypt (column-n)
    } } } }
```

cannot get the complete information and inside attackers also unaware about data format stored in database. The proposed scheme achieves data integrity such a way that as data is encrypted using symmetric encryption scheme using a secret key if any modification is done on cipher text, it cannot be decrypted properly.

As data is stored in one cloud vendor, the approach requires less cost and less communication delay for data upload and retrieval operations. So our model is more efficient and secure with less cost than available state of art models in literature.From literature, authors have focused on user authentication of online examination system to prevent from masquerade attacks, in this study we focused on confidentiality and integrity of marks data of the users after storing in database servers. This study ensure to protect data from internal staff of the organization, because internal staff may misuse their credentials and do update the marks. This is huge loss for the candidates those who prepare sincerely and write the examination.

Our proposed scheme, in addition to offering a higher security level,our scheme preserves better communication and computation performance while uploading data and retrieval phase. This is particularly important when it comes to privacy-preserving and avoiding single-point failure.

**6. Conclusion and Future scope.** In this paper, we propose a scheme for secure data storage and management of online examination systems using symmetric key cryptography algorithms, data distribution and cloud database as a service (DBaaS). In proposed scheme for preserving data confidentiality and integrity, database table records are encrypted using cryptographic AES-256 algorithm with 256 bit secret key generated

SELECT query execution time on UCA: 311.95521354675 Milliseconds

| id | Candidate_id | Test_id | Score |
|---|---|---|---|
| 48193 | cand_00001 | Test_01 | 34 |
| 48194 | cand_00002 | Test_01 | 28 |
| 48195 | cand_00003 | Test_01 | 38 |
| 48196 | cand_00004 | Test_01 | 27 |
| 48197 | cand_00005 | Test_01 | 24 |
| 48198 | cand_00006 | Test_01 | 22 |
| 48199 | cand_00007 | Test_01 | 38 |
| 48200 | cand_00008 | Test_01 | 34 |
| 48201 | cand_00009 | Test_01 | 23 |
| 48202 | cand_00010 | Test_01 | 37 |
| 48203 | cand_00011 | Test_01 | 27 |
| 48204 | cand_00012 | Test_01 | 34 |
| 48205 | cand_00013 | Test_01 | 32 |
| 48206 | cand_00014 | Test_01 | 39 |
| 48207 | cand_00015 | Test_01 | 37 |
| 48208 | cand_00016 | Test_01 | 29 |
| 48209 | cand_00017 | Test_01 | 34 |
| 48210 | cand_00018 | Test_01 | 34 |
| 48211 | cand_00019 | Test_01 | 30 |
| 48212 | cand_00020 | Test_01 | 22 |

Fig. 5.1: Data stored in local database system before encryption

SELECT * FROM `Test_Score1`

| id | Candidate_id | Test_id |
|---|---|---|
| 48193 | L3JPZGFhSFVTWUVjZW03N0pPMVd6QT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48194 | MDhtc0RtT0ExQ2cwN0t2SEY1andkZz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48195 | NDMvUXZyYStGTG5UbUNseXZmNlJEQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48196 | VmN5dGhzSTdEd2tMTkdROHdneS91dz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48197 | NUI4OVRDQzVRRGJid1FNUDY2UEJwZz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48198 | TmpQWkhIbk0vdWtKNWk4ZndlbHkxUT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48199 | aTh6S25xRXBmb0R3c3NuQytvZEs0dz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48200 | RnBzYUpQcGgzUXRkcUt0dkNnYmRrUT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48201 | R2JLS1E1ZDFjVVN5VjNLbDRSamhzQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48202 | Z1VWZmZWZnpXdFpsTXRndmE0SW1TQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48203 | cHhMa2JmQjVONFE1Z2pzN0Vlak1uZz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48204 | ME1TYW5lWlFoZ0YrUzdRTDJCenN0Zz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48205 | eDRUN0txT3lyU1FmWFg5SmdUZ2dZUT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48206 | b2F2bnY0NUF2cVZWczYybmc1L1htdz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48207 | NG5PM2xkN1BmbnpTVldPRFViMENxZz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48208 | OUNUa1Fjdk43bljWElSRXZueXdjQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48209 | UlZlSFZyYTNIc2hiQUdKSTd5MVg2Zz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48210 | d05SWmNsQUVkQWI4bFE2Y2ZqeFdldz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48211 | YXI4czdiZGNldTdvTVdCRS9razAxQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48212 | MTJ6OUE0Y2VwSk55VlhVYUZxa2gwUT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48213 | emIraFRjQ1NIRUw5L2RBTmZJSXpSQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48214 | bHU2VU1GWG5abXE5d0ZYbTI6RWIxQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48215 | UC9adm45UHlIMGo0WVNvR293WmFNZz09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48216 | cm9oN2U1STZTU1B3V0hiWFZlbGVYUT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |
| 48217 | V0VrOUZDUURybDMxeVhNN3NBeG5rQT09OjowZDA4MDY3YTM4MD... | OVdiMFFteVl3L1lzeVJ3dlFyM0hEZz09OjowZDA4MDY3YTM4MD... |

Fig. 5.2: Data stored in database after encryption and fragmentation (Table fragment1)

using SHA256 algorithm, and then table is vertically partitioned with selected columns into multiple small table fragments. These small table fragments are inserted and stored in different database servers in cloud environment. As data is stored in cipher text format and only part of the entire record is stored in each database servers, the internal staff of the organization also cannot know what data is. So the proposed scheme

```
SELECT * FROM `Test_Score2`
```

| id | Score |
|---|---|
| 48193 | cFllSmM0Z2piakNUdVJJRHI3T1IzZz09OjowZDA4MDY3YTM4MD... |
| 48194 | am1MTG1uZDgwOTJvd1p4RVdyNnl2Zz09OjowZDA4MDY3YTM4MD... |
| 48195 | N3pLeHRJSFgvM05oM2g2NlVFWm1qZz09OjowZDA4MDY3YTM4MD... |
| 48196 | K2kydmphTWZZU1hiVFhJa3lyblRyZz09OjowZDA4MDY3YTM4MD... |
| 48197 | b3lZT3NDNllreVFCWFdHWFZmMHY4Zz09OjowZDA4MDY3YTM4MD... |
| 48198 | Y2pXVmlHOFNZZ2NpcE5lNVhTTFZQUT09OjowZDA4MDY3YTM4MD... |
| 48199 | N3pLeHRJSFgvM05oM: No row selected. |
| 48200 | cFllSmM0Z2piakNUdVJJRHI3T1IzZz09OjowZDA4MDY3YTM4MD... |
| 48201 | MW5WK2d5K3VvVHdyYkJSeXhnNktYZz09OjowZDA4MDY3YTM4MD... |
| 48202 | QnhZYzNVK3dYY1AwMFkrNElnMXprZz09OjowZDA4MDY3YTM4MD... |
| 48203 | K2kydmphTWZZU1hiVFhJa3lyblRyZz09OjowZDA4MDY3YTM4MD... |
| 48204 | cFllSmM0Z2piakNUdVJJRHI3T1IzZz09OjowZDA4MDY3YTM4MD... |
| 48205 | Z3YwN0MzOHRkcVRMTFlMMEViUmJwQT09OjowZDA4MDY3YTM4MD... |
| 48206 | L0F5Zk01bWEyOC95THJJSWlWRXdLQT09OjowZDA4MDY3YTM4MD... |
| 48207 | QnhZYzNVK3dYY1AwMFkrNElnMXprZz09OjowZDA4MDY3YTM4MD... |
| 48208 | aW0xYTBhelkvUjlLWFVrUnk4Vjh4QT09OjowZDA4MDY3YTM4MD... |
| 48209 | cFllSmM0Z2piakNUdVJJRHI3T1IzZz09OjowZDA4MDY3YTM4MD... |
| 48210 | cFllSmM0Z2piakNUdVJJRHI3T1IzZz09OjowZDA4MDY3YTM4MD... |
| 48211 | ell3R21XZVI4NVN1Z2UzSVJFT1BmZz09OjowZDA4MDY3YTM4MD... |
| 48212 | Y2pXVmlHOFNZZ2NpcE5lNVhTTFZQUT09OjowZDA4MDY3YTM4MD... |
| 48213 | QnhZYzNVK3dYY1AwMFkrNElnMXprZz09OjowZDA4MDY3YTM4MD... |
| 48214 | am1MTG1uZDgwOTJvd1p4RVdyNnl2Zz09OjowZDA4MDY3YTM4MD... |
| 48215 | dDdlRDk5Sm5DbWp2NkNWQStPbE12UT09OjowZDA4MDY3YTM4MD... |
| 48216 | K2kydmphTWZZU1hiVFhJa3lyblRyZz09OjowZDA4MDY3YTM4MD... |
| 48217 | aW0xYTBhelkvUjlLWFVrUnk4Vjh4QT09OjowZDA4MDY3YTM4MD... |

Fig. 5.3: Data stored in database after encryption and fragmentation (Table fragment2)

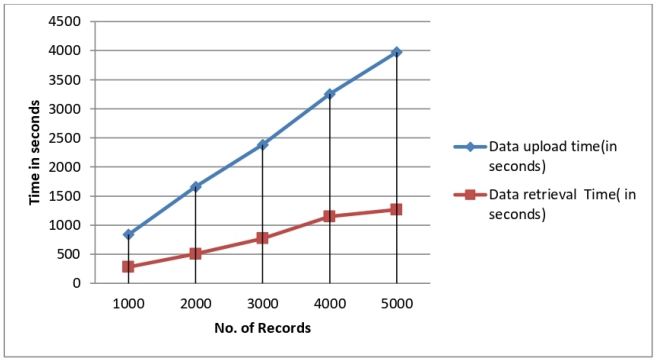


Fig. 5.4: Data upload and retrieval time of proposed scheme

preserves the data confidentially and integrity. As cloud is rental basis service, the cloud services providers always takes care about the security of physical infrastructure and keeps it always available. As cloud vendors maintain the infrastructure suitable for variable sized data, good scalability can be achieved with this approach. In our future research, scheme will incorporate other encryption algorithms and evaluate the performance.

## REFERENCES

[1] Sattar, M. R. I., Efty, M. T. B. H., Rafa, T. S., Das, T., Samad, M. S., Pathak, A., and Ullah, M. H..*An advanced and secure framework for conducting online examination using blockchain method*, Cyber Security and Applications,2023.

[2] Al-Aqbi, A. T. Q., Al-Taie, R. R. K., & Ibrahim, S. K. *Design and Implementation of Online Examination System based on MSVS and SQL for University Students in Iraq.* , Webology, 18(1). 2021.

[3] Mistry, B., Parekh, H., Desai, K., & Shah, N. *Online Examination System with Measures for Prevention of Cheating along with Rapid Assessment and Automatic Grading.* ,In 2022 5th International Conference on Advances in Science and Technology (ICAST) (pp. 28-34). IEEE. 2022.

[4] Semlambo, A., Almasi, K., & Liechuka, Y. Perceived *Usefulness and ease of use of online examination system: A case of Institute of Accountancy Arusha.* , International Journal of Scientific Research and Management (IJSRM), 10(04),

851-861. 2022.
[5] Qianhuazhu, *Design and testing of online examination system based on MyEclipse* , Software Engineering and Applications, vol. 08, no. 3, pp. 99–103, 2019.
[6] Garima Verma *Blockchain-based privacy preservation framework for healthcare data in cloud environment*, Journal of Experimental & Theoretical Artificial Intelligence, 36:1, 147-160, DOI: 10.1080/0952813X.2022.2135611, 2024.
[7] Z. Huang, Y. Zhang, Q. Li et al., *Unidirectional variation and deep CNN denoiser priors for simultaneously destriping and denoising optical remote sensing images,* , International Journal of Remote Sensing, vol. 40, no. 15, pp. 5737–5748, 2019.
[8] X.-B. Jin, W.-Z. Zheng, J.-L. Kong et al., *Deep-learning temporal predictor via bidirectional self-attentive encoderdecoder framework for IOT-based environmental sensing in intelligent greenhouse*, Agriculture, vol. 11, no. 8, p. 802, 2021.
[9] H. Shi, H. Zhang, J. Huang, and Z. Xu, *Design of examination system based on LabVIEW for pesticide detection staff,*, Modern electronic technology, vol. 042, no. 2, pp. 49–53, 2019.
[10] H. ru Zhang*Application of cloud computing technology in the university's information construction and development*, Software Engineering and Applications, vol. 8, no. 2, pp. 32–37, 2019.
[11] Banothu, S., Govardhan, A., & Madhavi, K. *A Fully Distributed Secure Approach for Database Security in Cloud Computing* , In Computational Intelligence and Data Analytics: Proceedings of ICCIDA 2022 (pp. 523-531). Singapore: Springer Nature Singapore, 2022.
[12] D. V. Kotwal, S. R. Bhadke, A. S. Gunjal et al., *Online examination system,* , International Research Journal of Engineering and Technology (IRJET), vol. 3, no. 1, pp. 115–117, 2016.
[13] A. Okada, D. Whitelock, W. Holmes et al., *E-authentication for online assessment: a mixed-method study*, British Journal of Educational Technology, vol. 50, no. 2, pp. 861–875, 2019.
[14] Cluskey Jr, G. R., Ehlen, C. R., & Raiborn, M. H. *Thwarting online exam cheating without proctor supervision.* , Journal of Academic and Business Ethics, 4, 1.,2011.
[15] Kavish Garg, et al., *Convolutional neural network-based virtual exam controller*, 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2020.
[16] Mukta Goyal, Divakar Yadav, Alka Choubey, *Fuzzy logic approach for adaptive test sheet generation in e-learning*, 2012 IEEE International Conference on Technology Enhanced Education (ICTEE), IEEE, 2012.
[17] Im Y. Jung, Heon Y. Yeom, *Enhanced security for online exams using group cryptography*, IEEE Trans. Educ. 52 (3) 340–349.,2009.
[18] Mojitha Mohandas, et al., *Automated question paper generator system*, Int. J. Adv. Res. Comput. Commun. Eng. 4 (12) 676–678.,2015.
[19] Dimple V. Paul, et al., *Use of an evolutionary approach for question paper template generation*, 2012 IEEE Fourth International Conference on Technology for Education, IEEE, 2012.
[20] Chenggang Zhen, Yingmei Su, *Research about human face recognition technology*, 2009 International Conference on Test and Measurement, IEEE, Vol. 1,2009.
[21] Apoorv Jain, et al., *Smart contract enabled online examination system based in blockchain network*, 2021 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2021.
[22] Kyungmee Lee, Mik Fanguy, *Online exam proctoring technologies: educational innovation or deterioration?* , Br. J. Educ. Technol.,2022.
[23] Qurotul Aini, et al., *Digitalization online exam cards in the era of disruption 5.0 using the DevOps Method*, J. Educ. Sci. Technol. (EST) 7 (1) 67–75.,2021.
[24] Banothu, Srinu, A. Govardhan, and Karnam Madhavi. *A Fully Distributed Secure Approach Using Nondeterministic Encryption For Database Security in Cloud.* , Journal of Theoretical and Applied Information Technology 100.7, 2022.
[25] Karanam, Madhavi, et al. *Performance Evaluation of Cryptographic Security Algorithms on Cloud.* , E3S Web of Conferences. Vol. 391. EDP Sciences, 2023.
[26] Banothu, Srinu, A. Govardhan, and Karnam Madhavi. *Performance evaluation of cloud database security algorithms.* , E3S Web of Conferences. Vol. 309. EDP Sciences, 2021
[27] S. Kausar, X. Huahu, A. Ullah et al., *Fog-assisted secure data exchange for examination and testing in E-learning System*, Mobile Networks and Applications, pp. 1–17, 2020.
[28] F. Al-HawariM. Alshawabkeh et al., *Integrated and secure web-based examination management system*, Computer Applications in Engineering Education, pp. 994–1014, 2019.
[29] G. Sahaya Stalin Jose and C. Seldev Christophe, *Secure cloud data storage approach in e-learning systems*, Cluster Computing, vol. 22, pp. S12857–S12862, 2019.

*Edited by:* Anil Kumar Budati
*Special issue on:* Soft Computing and Artificial Intelligence for wire/wireless Human-Machine Interface
*Received:* Jan 1, 2024
*Accepted:* Mar 29, 2024