International Journal of Science and Engineering Applications
Volume 9 - Issue 06, 68 - 78, 2020, ISSN:- 2319 - 7560

# An Improved Data Masking Security Solution Using Modulus Based Technique (MOBAT) for Data Warehouse System

Kefas Suwa Larson
M.Sc. Student, Comp. Science
Dept. of Mathematical Science
Abubakar Tafawa Balewa University (ATBU),
Bauchi, Nigeria

Souley Boukari
Professor, Computer Science
Dept. of Mathematical Science
Abubakar Tafawa Balewa University (ATBU),
Bauchi, Nigeria

**Abstract**: Protecting Data Warehouse (DW) is very important, since it consists of sensitive data used in many business models for decision support processes. Data masking and encryption techniques have been recommended in academic literatures for DW, however, most of the previous works considered only the numeric data types. This research proposes an improved Modulus Based Technique (MOBAT) that supports string data with numeric and non-numeric attributes. Java with NetBeans and MySQL were used in developing the solution. The experimental results show that our suggested technique achieves low storage space overhead, loading time overhead and better processing time performance as compared to the existing system. While existing system consumed 102MB storage space after MOBAT was applied to the data (8% storage space overhead), the proposed methodology maintained the same storage space (1172mb) when data was without encryption and when MOBAT was applied. This means that no extra space is added. Also, loading time overhead for existing system was 7%, but the new scheme achieved 6%. Based on the experimental results obtained, our technique is more efficient, making it a valid alternative for protecting data stored in DWs.

**Keywords**: Data Warehouse Security; Data Warehousing; Data Security; Data Masking; Data Encryption

## 1. INTRODUCTION

Although many studies have been conducted on security issues in Data Warehouse (DW), attacks are increasing every year in numbers and complexity, and none of the security solution proposed so far by researchers has proffered a permanent and all-inclusive answer to the data damage, breaches, malicious attacks, etc.

Security concerns have been an important subject in the corridor of DW system and it remains totally unresolved up to date **[1]**. The data stored in warehouse is extracted from various operational databases. So, security has always been the critical issue in DW for protection of essential and useful data **[2].** Due to the widespread use of confidential data in Data Warehousing systems, security is a major concern **[3]**.

According to **[4],** the main concept of DW Security is about Confidentiality, Integrity and Availability (CIA). Confidentially means only authorized users should access the data from the DW. Integrity means originality of the data. Availability means information is available all the time**.** Authors in **[5],** indicated that to comply with the CIA attributes, many techniques have been submitted. These can be classified into two broad categories: preventive and reactive techniques. Preventive data security techniques protect the data in advance from security breaches or attacks. They used data masking, encryption, and data access policies to tackle the preventive category. Reactive data security techniques effectively respond after a security attack or security problem has occurred**.**

Granting that a variety of standard encryption algorithms are available to secure DW, but as a consequence, they do reduce the performance of the DW system due to their required large computational overheads **[6].** Most of the DW Security approaches used encryption and masking methods that tried to provide strong data privacy. However, these types of encryption method make them inefficient for DW use owing to their high computational overheads. Therefore, a data masking technique is needed that can provide strong data privacy with less computational effort and also maintains high performance **[7].**

Furthermore, researchers in the past have used masking and encryption techniques to protect data in DW, however, most of the previous researches applied the masking and encryption techniques to sensitive numeric attributes only. In this study, an improved Modulus Based Technique (MOBAT) that supports string data with textual, alphanumeric, numeric and special character attributes specifically designed for DW system is proposed.

The rest of this paper is organized as follows: Section **2** describes review of related works. Section **3** presents the new MOBAT methodology. Section **4** presents the results of the implementation of new MOBAT and the simulation conducted, and finally, Section **5** concludes the study and highlights future research directions.

## 2. REVIEW OF RELATED WORKS

This section provides a review of related works done by different researchers on DW Security, pointing out the strengths and weaknesses of each proffered solution.

The authors in **[8],** proposed a solution based on user profile, which considers the definition of access permissions according to the user role using the access rights defined in data sources, generate the level of sensitivity of each object in the DW according to these permissions, then trace the access and detect violation attempts of access rights on a sensitive data. They claim that this technique helps the owner of the DW to well manage the access control of the users. But this type of solution can only be suitable for applications with a

limited number of users and roles and where the user's roles seldom change, not for volume-centric data environment such as DW.

**[1]** presented a framework for securing a student DW by creating a hybrid technique using email and password, Token and CAPTCHA authentication to ensure that only registered students have access to the DW. However, their solution only restricts logging access to the DW, while data at rest is not masked, hence making it extremely vulnerable to a breach.

In their work, **[9]** evaluated a new schema that balances security and performance when outsourcing DW in the cloud. The schema is based on a simple privacy homomorphism using the MOD operator with 2 prime numbers p and q. The scenario is to encrypt data stocked in DW with the encryption function $\phi(x)= [x \bmod p, x \bmod q]$ *and* $m = pq$ (the product of these large secret primes). Unfortunately, the schema is not secure enough because the cloud provider can infer the two chunks of data and get the two secret parameters p and q. Malicious intruders can also break the security parameters of the cloud provider, get the encrypted data and the modulo m from the cloud provider and decrypt the data using the known clear text.

**[2]** discussed an enhanced security architecture for DW by combining One-Time Pad (OTP) encryption technique with Advanced Encryption Standard (AES) to encrypt the data before loading it into the DW. The OTP encrypts the input data with random key (k) using modular addition, mod26 which has tremendous properties that plays an essential part in cryptography for security. The OTP is unbreakable theoretically but practically it is weak.

In their paper**, [10**] considered a solution that uses a universal scheme for hiding data of various type fields of a row (tuple) of a database table based on the use of MOBAT public and private keys (K1, K2 and K3). Their method is based on random permutation of elements (bytes, characters) of data of a specific field of a different type (numeric, character strings, Binary Large Objects (BLOBs), Character Large Objects (CLOBs)) of table row, which used data shuffling technique. However, only 18,000 rows of data were subjected to the masking and encryption evaluation, thus, may not be sufficient for a DW that stores huge volume of data.

In **[11**], the authors discussed a framework to Identify, Map, Apply, Sign, Keep testing, and Utilize (IMASKU) and Content-Based Data Masking Technique to securely save sensitive data into an integrated DW to prevent the database from the risks of external and internal attacks. Their technique is claimed to protect data at rest within the enterprise data warehouse. However, further algorithm optimization method is needed to determine the acceptable execution time when a big size of data is to be used on the framework.

**[12]** presented a new and efficient Format Preserving Encryption (FPE) scheme for encrypting integer data of 16 digits by using AES, exclusive OR operation and a translation method to overcome the shortcomings of existing schemes. However, the technique only covers 16-digit numeric data and may not be feasible for DW system that contains various data types.

**[13]** considered a Multivalued-Homomorphic (MV-HO) encryption strategy that was compared with encryption strategies based on symmetric encryption, order preserving symmetric encryption and homomorphic encryption. They claim that their technique is the best solution as it is pareto-optimal with respect to other strategies investigated. But the technique was only tested with a small size of data, which is not characteristic of a DW that holds huge volume of data.

To deal with numeric and non-numeric data types, **[14**] proposed a technique to protect the confidentiality of numeric and non-numeric data by obfuscation and encryption before storing into the Cloud storage. They claim that their technique has reduced the service cost, minimized the data size and processing time while uploading into the cloud storage. However, there was no experimental evaluation carried out to ascertain this assumption.

**[15]** evaluated a new framework for implementing security issues in DWs named DW Signature (DWS). The DWS framework focuses on the triage of security issues, which are Confidentiality, Integrity and Availability (CIA). Their approach achieves high performance by using parallel computing through a middleware named View Manager Layer (VML). However, the method lacks performance evaluation of (i) finding the query memory buffer for the VML middleware, and (ii) evaluating the high performance when the number of executors increases in the VML middleware.

In **[16],** the authors advanced an integrated data security framework that enables the use of data masking, encryption and intrusion detection in a single workflow for DW environment. The framework discusses the feasibility issues involving solutions that promote data confidentiality and deal with intrusions against DWs at the database level, focusing on data masking, encryption and database intrusion detection systems (DIDS). However, both the data masking and encryption techniques presented were specifically designed to mask and encrypt numeric values only. This is because of the believe that in most DWs the main portion of sensitive data is numerical. Thus, the solution does not cover all the sensitive data that may be stored in DW.

**[17]** presented "An Effective DW Security Framework" which highlights the usage of modulus operator in data security for DW system. They replaced the original set of data with another set of data that is not real but realistic. The numeric data is masked using a mathematical formula that makes use of the modulus operator. They also injected false rows onto the database which uses up extra space but helps in increasing the randomness in the database that can mislead the hackers. Their technique was compared with standard encryption algorithms such as AES128 and 3DES168. The results gotten were highly favorable with balanced system performance in storage space overheads, loading time overheads and response time overheads. However, there is need to design a masking technique for respective data domain (since DW is made of data from different sources) so that it can apply to all data types instead of the numeric data only.

**[18]** proposed a Specific Encryption Solution for DW (SES-DW) using only standard SQL operators such as eXclusive OR (XOR) and modulo (MOD, which returns the remainder of a division expression), together with additions and subtractions. Their technique shows a better database performance than standard and state-of-the-art encryption solutions with security based on DW perspective. However, its major shortfall is that it can only secure sensitive data with numeric data types. It does not cover other data types such as textual or alphanumeric characters.

The authors in **[19**], presented a lightweight encryption technique based on a cipher using alternating sets of eXclusive OR (XOR) and bit switching operations sequence

which focuses on leveraging security-performance tradeoffs that can make it feasible for DW environments. But, the viability and feasibility of the technique could not be guaranteed since the method was not tested in a real-world DW environment.

**[20]** implemented a model for securing data in DW based on log implementation. They noted that, data stored in DW need to be transformed to other form which should be unreadable to attackers. Thus, to increase data security the authors have suggested a technique called data masking, which is a process to convert original data to some other form. For this, a MOD function/operator is used in SQL such that whenever a user sends request stored in a log, it is verified in the log and resent. But their data masking method introduced large overheads, making it unfeasible for DW environment.

**[21]** introduced a Big Data Security mechanism using the MOBAT technique, wherein they first selected only certain attributes that have higher values than the rest and secure them, which in turn provided security to the whole of the Big Data. To mask the numeric data in the Big Data they made use of the mathematical formula with MOD (modulus) operator (which returns the remainder) and a set of other basic arithmetic operators. However, the technique covers only numeric data. There is need to extend the focus to securing the character data as well.

**[22]** reviewed the security measure to prevent sensitive data from malicious attacks. He provided a log-based security system architecture to prevent the data from attackers. But the critical problem is on how to automatically coordinate the access rights of the DW with those of the data from the different sources.

**[23]** presented a paper on how to balance Security and Performance for Enhancing Data Privacy in DWs using MOdulus-BAsed method. Their proposal uses the MOD operator and simple arithmetic operations to mask data and provide a significant level of apparent randomness for the masked values. The solution also uses one of the masking keys for injecting false data into the DW in order to mislead attackers and increase the overall security level, making them unable to distinguish true from false data. But their masking technique is also only tailored to numeric kind of data.

In **24]**, the authors presented the best database encryption solutions to protect sensitive data. They proposed a data masking solution for numerical values in DWs based on the mathematical modulus operator, which can be used with an extra software application layer. However, this technique needs to be expanded to cover masking of alphanumeric values, so that it can provide a complete data protection solution.

# 3. PROPOSED METHODOLOGY

This section presents the expected methodology used in securing the data in a DW system.

In our proposed solution, we have designed a model to implement one of the future works of **[16]**, in which the data protection was only for numeric data type. The extension of the existing techniques to cover all the data types is imperative because DW stores huge amount of sensitive data types that must be guarded against from both inside and outside attackers.

The main contribution of our research work is the expansion of the existing MOBAT technique to ensure all sensitive data with different data types in DW can be encrypted, and to prevent unauthorized access. This was designed and extended using the 95-Printable ASCII codes for alphanumeric characters and symbols, while maintaining the existing MOBAT formula for the numeric data type. Figure 1 depicts the framework of the improved security solution.

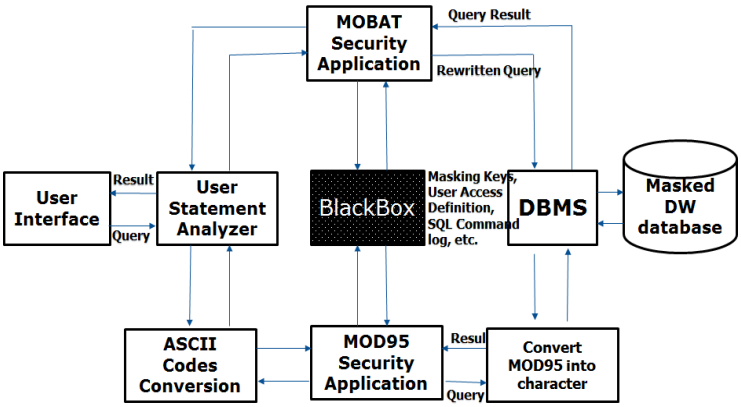



**Figure 1. Proposed MOBAT and MOD95 system with extended components**

## 3.1 Working Principle of the Proposed System

This research proposes an improved MOBAT for securing data in Data Warehouses based on **[16]**. Our technique is a hybrid of MOBAT and MOD 95 which uses the 95 printable ASCII codes table that contains all the input on a normal computer keyboard. This provides for easy conversion of almost all English characters you can find on most computer systems, and enables encrypting all data types. The considered structure is mainly divided into two modules, numeric and non-numeric data masking.

### *3.1.1 Numeric data masking*

To better understand the working of the numeric data masking technique, let us consider a table 'T' with a set of 'm' rows and 'n' columns, where rows are given by (R1, R2,……,Rm) and columns are given by (C1, C2,……,Cn). Let the value that has to be masked be represented as a pair of (Ri, Cj) where 'Ri' is the row and 'Cj' is the column which contains the data that has to be masked. In order to mask the data, we must have three masking keys:

- K1, a 128-bit randomly generated number which remains constant for the table T.
- K2, a 128-bit randomly generated number which remains constant for a particular column Cj. This is represented as K2, j.
- K3, a random number between 1 and $2^{128}$ that remains constant for a row. The value depends on the data of that particular row. It is represented as K3, i.

K1 and K2 are stored in the Black Box, while K3 will be stored in the masked table along with the other data. Thus, every row of a table will compulsorily have a public key K3.

Now, let's suppose a value to be masked as (Ri, Cj). Then the new masked value (Ri, Cj)` is given by the formula:

$$(Ri, Cj)' = (Ri, Cj) - ((K3, i \bmod K1) \bmod K2, j) + K2, j \quad (1)$$

To retrieve the original value, we used the following formula:

**(Ri, Cj) = (Ri, Cj)' + ((K3, i Mod K1) Mod K2, j) - K2, j (2)**

### *3.1.2 Non-numeric data masking*

For the non-numeric data types, we use a simple linear algebraic function with the private key (K2) to encrypt them by employing the formula stated in **[25]**:

**E(x) = ((x - 32 + K2 + 95) mod 95) + 32 (3)**

where x is the equivalent value of each character to mask/encrypt as contain in ASCII table, while the randomly generated key K2, is column dependent. We are subtracting 32 from every element of x because the printable characters have ASCII codes in the range of 32 to 126, while mod 95 represents the ASCII values in the range 0 to 94.

To reverse any of the encrypted characters, we have to reverse the steps used in encrypting it to recover the original values.

**D(E(x)) = ((x - 32 - K2 + 95) mod 95) + 32 (4)**

Thus, to reverse any of the encrypted characters, we have to reverse the steps used in encrypting it to recover the original values.

### *3.1.3 Proposed program design*

The main algorithm of the submitted solution is as shown in Figure 2, while details of the split algorithms are numbered 1 to 6 subsequently.

**Begin algorithm**
1. For each table n in the target DW database TDW(1….N)
2. Fetch K1 private key common for the entire table(n)
3. For each attribute j in the table
4. Fetch K2,j private key common for entire attribute(j)
5. For each sensitive data item (Ri, Cj) selected from the table(n)
6. Fetch K3,i public key common for a tuple (i)
7. **If Data item selected is NOT numeric**
8. **Convert each character to its ASCII equivalent and store in E(x)**
9. **Encrypt/ Decrypt E(x) with MOD95 masking formula**
10. **Translate E(x) to its character equivalent (ciphertext)**
11. **Append E(x) to (Ri, Cj)**
12. **end for**
13. else
14. for each pair of digits selected in (Ri, Cj)
15. encrypt/ decrypt digit value with MOBAT masking formula and store in numb
16. append numb to (Ri, Cj) //every loop appends with previous values
17. end for
18. end for
19. end for
20. end algorithm.

**Figure 2. Algorithm for DW Security using MOBAT and MOD95**

**1. Algorithm for Encryption with MOBAT and MOD95**
Step 1: Identify sensitive Data to mask
Step 2: If data is Numeric Then
Step 3: Encrypt data using MOBAT algorithm
Step 4. Go to Step 9
Step 5: If Data is Non-numeric THEN
Step 6: Convert character to ASCII code
Step 7: Encrypt data using MOD95
Step 8: Convert the MOD95 into character to produce ciphertext
Step 9: Store Data in DW database

**2. Algorithm for Decryption with MOBAT and MOD95**
Step 1: Identify encrypted Data to unmask
Step 2: If data is Numeric Then
Step 3: Decrypt data using reverse formula of MOBAT algorithm
Step 4: Go to Step 9
Step 5: If Data is Non-numeric THEN
Step 6: Convert ciphertext to ascii code
Step 7: Decrypt data using the reverse formula of MOD95
Step 8: Convert the MOD95 into character to produce plaintext
Step 9: Store Data in DW database
Step 10: Display result (original data) to user

**3. MOBAT Encryption Algorithm for Numeric Data types**
Step 1. Select Numeric data fields to encrypt, in our case (l_quantity, l_extendedprice, l_discount and l_tax)
Step 2: Fetch masking keys (k1, k2)
Step 3: Generate k3 for each row
Step 4: Apply MOBAT formula to data
Step 5: Store record in DW masked database
Step 6: Repeat steps 2 to 5 for each row until end
Step 7: Calculate execution time (in second).
Step 8: Display result to user

**4. MOBAT Decryption Algorithm for Numeric Data types**
Step 1. Select Numeric data fields to decrypt, in our case (l_quantity, l_extendedprice, l_discount and l_tax)
Step 2: Fetch masking keys (k1, k2)
Step 3: Generate k3 for each row
Step 4: Apply reverse MOBAT formula to data
Step 5: Repeat steps 2 to 4 for each row until end
Step 6: Calculate execution time (second)
Step 7: Display results to user

**5. MOD95 Encryption Algorithm for Non-Numeric Data types**
Step 1: Select non-numeric data to encrypt, in our case (l_shipmode)
Step 2: Fetch k2 for each column
Step 3: Convert data to ascii code equivalent
Step 4: Apply MOD95 formula to data
Step 5: Convert MOD95 into character to produce Ciphertext
Step 6: Store record in DW masked database
Step 7: Repeat steps 2 to 6 for each row until end
Step 8: Calculate execution time (in second)
Step 9: Display results to user

**6. MOD95 Decryption Algorithm for Non-Numeric Data types**
Step 1: Select non-numeric data field to decrypt, in our case (l_shipmode)
Step 2: Fetch k2 for each column
Step 3: Convert data to ascii code equivalent
Step 4: Apply MOD95 reverse formula to retrieve original data
Step 5: Convert MOD95 into character to produce Plaintext
Step 6: Repeat steps 2 to 5 for each row until end
Step 7: Calculate execution time (in second)
Step 8: Display results to user.

### *3.1.4 Functional flowchart of the proposed work*

The working of the improved MOBAT is further depicted by the Flowchart in Figure 3.

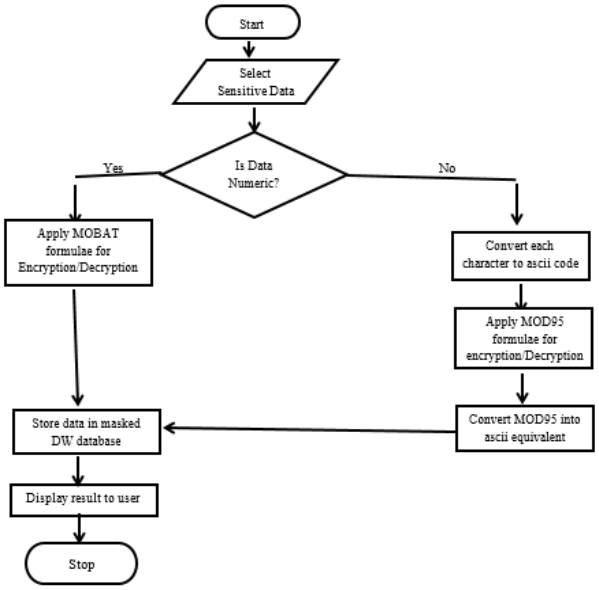



**Figure 3. Flowchart of the Proposed System**

### *3.1.5 Evaluation metrics*

The evaluation of the masking /unmasking process is conducted using a dataset downloaded from the TPC-H database. Two data masking metrics are considered:

**Storage Growth –** The change in the size of new masked LineItem data table in comparison with the original one measured in megabytes (MB).

This is measured as follows:

$$\text{Storage Size Overhead (\%)} = \frac{\text{Storage size in MOBAT (MB)} - \text{Storage size in MySQL (MB)}}{\text{Storage size in MySQL (MB)}} \times 100$$

**Performance –** Loading time overhead (%) and the processing speed of the encryption/decryption algorithms in seconds. A time measurement is performed to evaluate the execution cost of data loading operation in standard application compared to loading time in the proposed approach (MOBAT).

This is measured as follows:

$$\text{Loading Time Overhead (\%)} = \frac{\text{Loading execution time with MOBAT (Sec)} - \text{Loading Time in MySQL database (sec)}}{\text{Loading Time in standard database (sec).}} \times 100$$

### *3.1.6 Masking key management*

A DW encryption solution is only as secure as the protection of its encryption keys. Therefore, the way in which encryption keys are accessed, restricted and stored is critically important. As stated in **[16]**, the public key K3, is stored in the fact table, so only keys K1 and K2 need to be cracked in MOBAT. K1 is a 16-byte integer, that is, a set of 128 bits. K2 depends on maximum storage size defined for each column, but variable between 1 and 128 bits. This means our technique is a minimum of $2^{129}$ key combinations for K1 and K2 together (at least 16 bytes+1 bit), and roughly needs an average number of $2^{128}$ tests (half of the total possible brute force tests – 50% chance) for discovering the keys using brute force, for each masked column in the table, since K2 is column dependent. For example, the minimum number of combinations needed to discover all key values for an $i^{th}$ number of columns is $i * 2^{129}$, resulting in an average of $i * 2^{128} \approx i * 3.4 \times 10^{38}$ brute force tests to discover the keys. As stated in **[11]**, the maximum time needed to crack these masking keys versus the 128-bit key combination is $1.02 \times 10^{18}$ years (1 billion years). This is a very difficult and time-consuming effort given the high number of possible brute key values to crack. Also, the MOBAT algorithms use dual moduli for the encryption and decryption process, thereby providing strong security against Brute-force attacks **[26].**

## 4. RESULTS AND DISCUSSION

In this section, we analyzed and discussed the contemplated data masking solution which is specifically designed to improve data confidentiality in DWs.

### 4.1 Simulation Environment

The work is implemented using Java programming language with Java development kit (JDK) 1.8 and NetBeans IDE 8.2 connected to XAMPP-MySQL DBMS on an intel Pentium N3540 Processor, 2.16GHz CPU with a 500GB hard disk and 4GB RAM. Various data sample testing was conducted to determine the execution time of the algorithms, and to know the storage space consumed when different size of data is loaded into the DW database**.**

### 4.2 Experimental Data

To assess performance of the new masking technique, we used dataset of a DW Fact table called LineItem that was extracted from the Transaction Processing Council ad-hoc (TPC-H) decision support benchmark to test the encryption/decryption algorithms. A brief description of the LineItem Fact table can be found in Appendix A.

### 4.3 Dataset

The dataset used in this research work was downloaded from the TPC-H decision support benchmark [TPC-H]. The data schema of TPC-H is created as sales DW with one fact table (LineItem), joint by seven-dimension tables on a standalone laptop.

From the sample dataset, we selected four sensitive numeric attributes and one non-numeric attribute and applied MOBAT and MOD95 algorithms respectively (L-Quantity, L_ExtendedPrice, L_Discount and L_Tax) and L_Shipmode). Also, for the experimental encryption, we tested one scenario, namely: the results for MOBAT where the public key K3, i columns are added to the fact table (LineItem) before encrypting any of the sensitive column, named as MOBAT AddCol. Finally, the results of the application of MOBAT and MOD95 masking formulae (1 & 3) on normal data and encrypted data are compared based on the scenario stated in Table 1.

**Table 1. Experimental encryption /masking scenario**

| Reference/ Label | Description |
|---|---|
| MOBAT AddCol | Data masked with MOBAT formulae (1 & 3) in which a column for masking key k3,i has been added to the fact table |

## 4.4 Presentation and Analysis of Results

This section discusses the operation performed and the time it takes to encrypt and decrypt data using the proposed MOBAT and MOD95 algorithms. After conducting four (4) test cases of simulation, the summary of results obtained are shown in Table 2. The complete set of test results and respective statistical measures can be seen in Appendix B.

**Table 2. Comparison of experimental results**

| Test Case | No. of Records | Data Size (MB) | Operation | MOBAT Algorithm (Sec) | MOD95 Algorithm (Sec) |
|---|---|---|---|---|---|
| Case 1 | 500,000 | 78 | Load Time (sec) | 44 | |
| | | | Encryption Time (sec) | 43 | 37 |
| | | | Decryption (sec) | 34 | 30 |
| Case 2 | 1,000,000 | 144 | Load Time (sec) | 90 | |
| | | | Encryption Time (sec) | 87 | 76 |
| | | | Decryption (sec) | 80 | 79 |
| Case 3 | 1,500,000 | 223 | Load Time (sec) | 139 | |
| | | | Encryption Time (sec) | 152 | 134 |
| | | | Decryption (sec) | 147 | 133 |
| Case 4 | 3,000,000 | 440 | Load Time (sec) | 273 | |
| | | | Encryption Time (sec) | 321 | 295 |
| | | | Decryption (sec) | 282 | 261 |

### *4.4.1 Analysis of experimental results*

#### *4.4.1.1 Test case 1 using 78mb data*

Figure 4 shows the graphical representation of the storage space used, loading time of the extracted data and the processing time while encrypting 78MB of data.

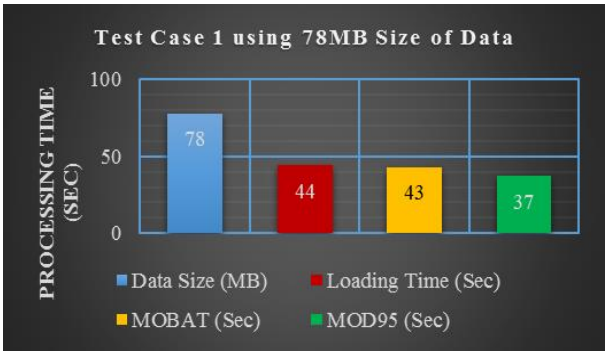



**Figure 4. Processing time executed in Test case 1**

#### *4.4.1.2 Test case 2 using 144mb data*

Figure 5 shows the graphical representation of the storage space used, loading time of the extracted data and the processing time while encrypting 144MB of data.

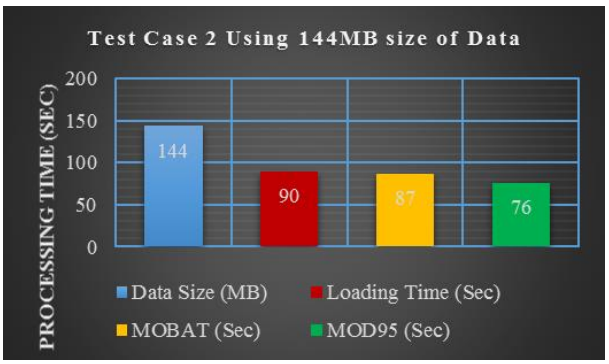



**Figure 5. Processing time executed in Test case 2**

.

#### *4.4.1.3 Test case 3 using 223mb data*

Figure 6 shows the graphical representation of the storage space used, loading time of the extracted data and the processing time while encrypting 223MB of data.

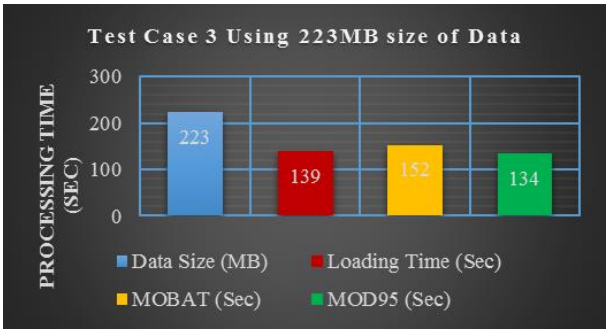



**Figure 6. Processing time executed in Test case 3**

#### *4.4.1.4 Test case 4 using 440mb data*

Figure 7 shows the graphical representation of the storage space used, loading time of the extracted data and the processing time while encrypting 440MB of data.

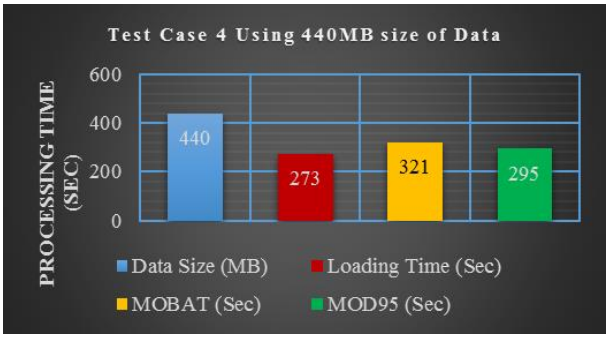



**Figure 7. Processing time executed in Test case 4**

### *4.4.2 Analysis of storage space*

This section describes the total data storage space used (in MB) and the percentage storage overhead after loading the TPC-H 1GB LineItem Fact table into the DW. We analyzed both the standard storage space used by the LineItem fact table when it is without any sort of encryption and when the columns of the fact table have been masked, as can be seen in Table 3. This is to find out whether the application of MOBAT and MOD95 processes will write additional data that may take up extra storage space in the DW database.

**Table 3. Storage size and overhead for the TPC-H 1gb tables.**

| | Proposed MOBAT | | Existing MOBAT | |
|---|---|---|---|---|
| Test Case | Standard MySQL | MOBAT (MB) | Standard SQL Server | Existing MOBAT |
| Test Case 1 | 78 | 78 | 1237 | 1339 |
| Test Case 2 | 144 | 144 | 1237 | 1339 |
| Test Case 3 | 223 | 223 | 1237 | 1339 |
| Test Case 3 | 440 | 440 | 1237 | 1339 |
| Dimensions | 287 | 287 | 1237 | 1339 |
| Total Storage Size (MB) | **1172** | **1172** | **1237** | **1339** |
| Storage overhead (%) | | 0% | | 8% |

Additionally, from Table 3, the existing system takes up 1237mb of storage space when it is without any encryption. But when MOBAT was applied to the data it consumed 1339mb of storage space**.** This means there is an increase of 102MB storage space after the MOBAT was applied to the data, leading to 8% storage space overhead.

However, in our considered MOBAT the storage space consumed when data was loaded without any encryption and when MOBAT/MOD95 was applied is the same, 1172mb. This means that no extra space is added when the proposed MOBAT was applied to the data.

Another key observation worth noting is the significant difference between the total data storage space sizes of SQL Server (1237MB) and MySQL (1172MB) as can be seen in Figure 8. The huge difference in the standard data storage space sizes between these DBMS is because they have distinct ways of storing data [16]. Research has shown that MySQL with MariaDB can improve compression performance for flash devices, improves storage efficiency, and improve power efficiency and CPU utilization **[27].**

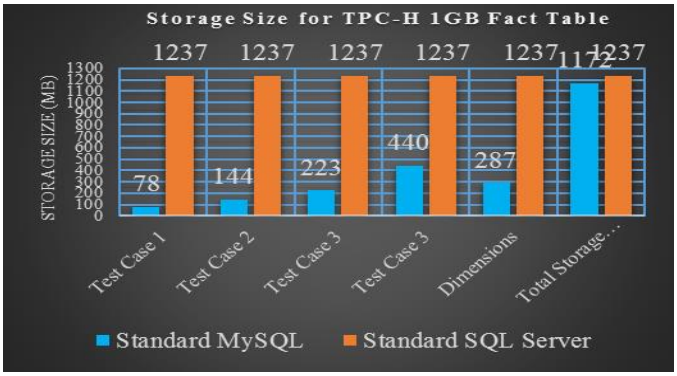



**Figure 8. LineItem fact table storage size (MB)**

Figure 9, shows that the improved MOBAT has incurred **0%** overhead in storage space when compared to the 8% recorded in the existing MOBAT. This means a huge cost savings in memory usage when using the novel solution. Figure 9, shows that the enhanced MOBAT has incurred **0%** overhead in storage space when compared to the 8% recorded in the existing MOBAT. This means a huge cost savings in memory usage when using the new MOBAT. The storage overhead is evaded by preserving each of the encrypted column's data type **[18].** This is achieved by retaining the original column-type and length of each encrypted column. This ensures the encrypted data is realistic but not real, and enables generating accurate but not factual results.

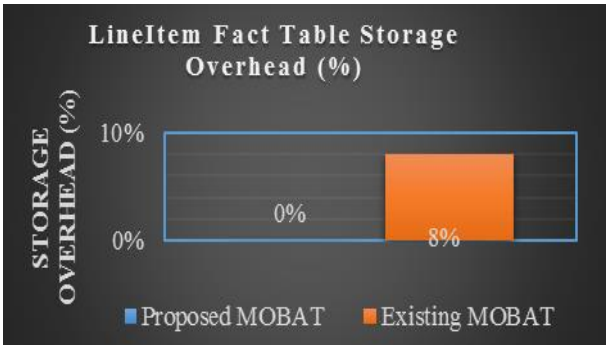



**Figure 9. LineItem storage space overhead (%).**

### *4.4.3 Analysis of load time*

In this section, we analyze the loading time taken when populating the fact table to know how long the execution of the data size by the MOBAT solution takes. Table 4 shows the Loading time of both the existing system and the improved MOBAT.

**Table 4. Lineitem fact table loading time (sec) and loading time overhead (%).**

| | Existing MOBAT | | Proposed MOBAT | |
|---|---|---|---|---|
| **Test Case** | **Standard SQL Server (Sec)** | **MOBAT Addcol (Sec)** | **Standard Mysql (Sec)** | **Proposed MOBAT (Sec)** |
| Test Case 1 | 212 | 227 | 34 | 44 |
| Test Case 2 | 212 | 227 | 84 | 90 |
| Test Case 3 | 212 | 227 | 134 | 139 |
| Test Case 4 | 212 | 227 | 262 | 273 |
| Total Loading Time | 212 | 227 | 514 | 546 |
| Loading Time Overhead (%) | | 7% | | 6% |

Figures 10 and 11 respectively show the results of the total loading time (in seconds) and the percentage of time overhead (%) for updating the TPC-H 1GB *LineItem* fact table. It can be observed that the total standard loading time for the LineItem fact table without using any sort of encryption solution is 212 seconds, and after MOBAT has been applied the loading takes 227 seconds as can be found in **[16]**. For the proposed system, total standard loading time takes 514 seconds, while the loading time when new MOBAT/MOD95 is applied takes 546 seconds.

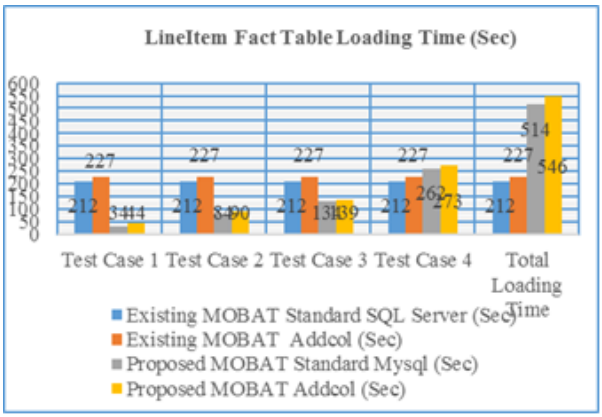



**Figure 10. LineItem fact table loading time (sec).**

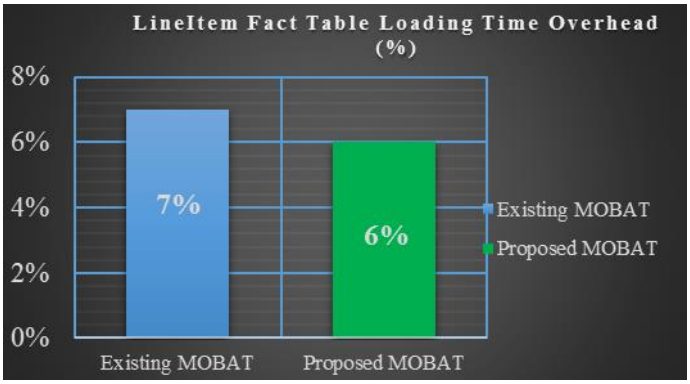



**Figure 11. LineItem fact table loading time overhead (%).**

A key observation that we can make from Figure 11 is the loading time overheads. While the existing system has loading time overheads as 7%, in the improved MOBAT it is 6%. This clearly shows that our MOBAT performs better than **[16].**

### *4.4.4 Analysis of processing time*

This section looks at the encryption and decryption speed for the four test cases to determine how long it takes MOBAT and MOD95 algorithms each to complete its masking task. Thus, the processing time of the encryption and decryption processes while updating the sensitive data is analyzed as shown in Figures 12 and 13.

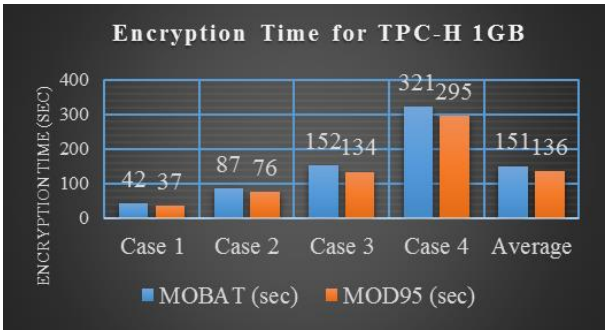



**Figure 12. Encryption time (sec) for the TPC-H 1gb fact table per algorithm.**

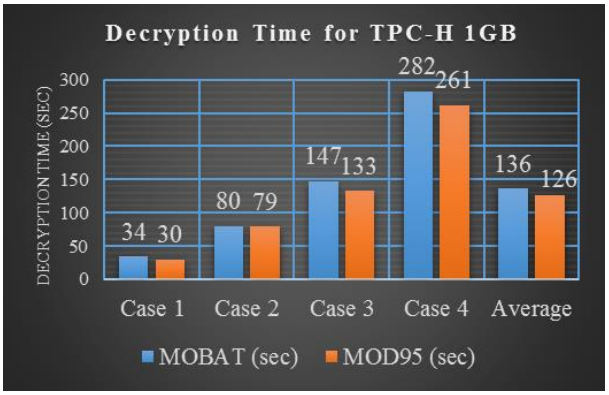



**Figure 13. Decryption time (sec) for the TPC-H 1GB fact table per algorithm.**

## 4.5 Discussion on the Experimental Results

### *4.5.1 Storage space overheads*

The 1172MB storage space consumed in the new system when data was loaded without any encryption and when MOBAT and MOD95 algorithms were applied shows that there is no extra space added to the system. This none increase in the storage size for the proposed system is explained by the fact that the improved MOBAT algorithm preserves the encrypted columns' data type format **[28]**. Thus, it avoids introducing storage space overhead and type conversions while running the encryption process.

Similarly, while the novel solution involves **0%** as storage space overhead, the existing system had 8% storage space overhead. This is because in the new entity the total storage space size did not change in both MySQL and when the data was masked with the new MOBAT. This signifies an efficient performance of the developed MOBAT.

### *4.5.2 Loading time overheads*

The loading time overheads of 6% achieved by suggested system is a significant improvement compared to the 7% recorded in **[16].**

### *4.5.3 Processing time performance*

#### *4.5.3.1 Encryption time when masking data*

As can be seen in Table 3 and Figure 12, each of the processing speed of MOBAT and MOD95 is directly proportional to the data size. That is, as the size of data increases so does the execution time of the algorithms. In the first, second, third and fourth test cases conducted, MOBAT algorithm took 42, 87, 152 and 321 seconds to encrypt data size of 78MB, 144MB, 223MB and 440MB, while MOD95 progressively took 37, 76, 134 and 295 seconds to encrypt the same size of data.

#### *4.5.3.2 Decryption time when unmasking data*

For the decryption process (Figure 13), the first, second, third and fourth test samples for MOBAT took 34, 80, 147 and 282 seconds, while MOD95 took 30, 79, 133 and 261 seconds to decrypt the same size of data.

A further observation from Figures 12 and 13, is that the processing time of MOD95 is lower than MOBAT. The MOBAT algorithm takes longer time to encrypt/decrypt data than MOD95 because in the experiment we chose four columns (l_quantity, l_extendedprice, (l_discount, and l_tax) to encrypt/decrypt with MOBAT while only one column (l_shipmode) was used to test the MOD95 algorithm.

## 4.6 General Observation

An improved data masking solution specifically designed for ensuring data confidentiality in DW was developed. The advanced data masking formulae are composed by a set of two consecutive moduli (division remainder) operations and some simple arithmetic operations.

Considering the results attained from the experimental tests, it is clear that the enhanced MOBAT is much more efficient. The recommended technique introduces low storage space overheads, low loading time overheads and better processing time performance in the system. Precisely, the proposed MOBAT is much faster than the existing solution, introducing 6% vs 7% of loading time and zero percent storage space overheads in the tested scenarios. The experimental results have demonstrated that the solution can effectively be used as a valid option for protecting sensitive data in Data Warehouses.

## 5. CONCLUSION AND FUTRE WORK

An improvement over existing MOBAT has been achieved, by allowing all string data types (textual, alphanumeric, special characters and numbers) to be masked, thus guaranteeing data privacy and confidentiality of data stored in data warehouses.

In this improved version of MOBAT, ASCII codes are used to encode all the 95 printable characters, thereby adding advantage of easy processing and implementation. That is, we have increased the scope of both data masking and encryption techniques to cover the protection of textual and alphanumeric attributes, apart from numerical attributes. The keys used in the encryption are randomly generated and so help to encrypt

the data that is required continuously by producing different values for different columns and rows of data.

The experimental results show that the improved MOBAT and MOD95 algorithms successfully encrypted all string data types in the sample data. This performance also comes without compromising the database size. The storage space overheads, loading time overheads and processing time performance introduced by our refined technique is lower than that in **[16].** This allows us to state that our improved MOBAT solution is a viable data security alternative that can be used to secure all string data in DW.

In the future, this approach can be expanded to cover all data types that may be stored in a DW such as metadata (XML), image, pdf, audio/video, etc. We also plan to

• implement and analyze the query performance of the encryption algorithms using some of the 22 TPC-H benchmark queries.

• simulate the practicability, efficiency and effectiveness of the new solution in a real-world Data Warehousing environment.

## 6. REFERENCES

[1] Kalio, Q. P., & Nwiabu, N. D. (2019). A framework for securing data warehouse using hybrid approach. International Journal of Computer Science and Mathematical Theory, 5(1), 44-55.

[2] Gupta, S., Jain, S., & Agarwal, M. (2019). DWSA: A secure data warehouse architecture for encrypting data using AES and OTP encryption technique. in soft computing: Theories and Applications (Vol. 742, pp. 505-514): Springer.

[3] Homayouni, H., Ghosh, S., & Ray, I. (2019). Data warehouse testing. in advances in Computers (Vol. 112, pp. 223-273): Elsevier.

[4] Kumar, S., Singh, B., & Kaur, G. (2016). Data warehouse security issue. International Journal of Advanced Research in Computer Science, 7(6).

[5] Divya, K., & Kurmi, J. (2017). A reassessment on security tactics of Data Warehouse and comparison of compression algorithms. Advances in Computational Sciences and Technology, 10(5), 847-854.

[6] Chandra, P., & Gupta, M. K. (2018). Comprehensive survey on data warehousing research. International Journal of Information Technology, 10(2).

[7] Phoghat, P., & Maitrey, S. (2015). Analysis of security techniques and issues in Data Warehouse. Paper presented at the 2015 1st International Conference on Next Generation Computing Technologies (NGCT).

[8] Elouazzani, A., Harbi, N., & Badir, H. (2018). User profile management to protect sensitive Data in Warehouses. *9*(1), 1-32.

[9] Karkouda, K., Nabli, A., & Gargouri, F. (2019). TrustedDW: A new framework to securely hosting data warehouse in the Cloud. Proceedings of 34th International Confer, 58, 397-406.

[10] Yesin, V. I., & Vilihura, V. V. (2019). Some approach to data masking as means to counteract the inference threat. Radio Engineering, 3(198), 113 -130.

[11] Ali, O. (2018). Secured data masking framework and technique for preserving privacy in a business intelligence analytics platform. Electronic Thesis and Dissertation Repository. 5995.

[12] Gupta, S., Jain, S., & Agarwal, M. (2018). Ensuring data security in databases using format preserving encryption. Paper presented at the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence).

[13] Lopes, C. C., Cesário-Times, V., Matwin, S., de Aguiar Ciferri, C. D., & Ciferri, R. R. (2018). An encryption methodology for enabling the use of data warehouses on the Cloud. International Journal of Data Warehousing and Mining (IJDWM), 14(4), 38-66.

[14] Yadav, S., & Tiwari, V. (2018). Encryption and Obfuscation: Confidentiality technique for enhancing data security in public cloud storage. Journal of Computer and Information Technology, 09, 33-39.

[15] Almeghari, M. J. (2017). Data Warehouse Signature: High performance evaluation for implementing security issues in Data Warehouses through a new framework. Journal of Computer Sciences and Applications, 5(1), 17-24.

[16] dos Santos, R. J. R. (2014). Enhancing data security in Data Warehousing. (Doctoral dissertation in Information Science and Technology). University of Coimbra. Retrieved from http://hdl.handle.net/10316/25230

[17] Vishnu, B., Manjunath, T., & Hamsa, C. (2014). An effective data warehouse security framework. International Journal of Computer Applications, 975, 8887.

[18] Santos, R. J., Rasteiro, D., Bernardino, J., & Vieira, M. (2013). A specific encryption solution for Data Warehouses. Paper presented at the International Conference on Database Systems for Advanced Applications.

[19] Santos, R. J., Vieira, M., & Bernardino, J. (2016). XSX: Lightweight encryption for Data Warehousing environments. Paper presented at the International Conference on Big Data Analytics and Knowledge Discovery.

[20] Singh, A. (2015). Implementation model for access control using log-based security: Practical approach. Paper presented at the 2015 International Conference on Advances in Computer Engineering and Applications.

[21] Achana, R., Hegadi, R. S., & Manjunath, T. (2015). A novel data security framework using E-MOD for big data. Paper presented at the 2015 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), BUET, Dhaka, Bangladesh.

[22] Rani, R. (2014). Data Warehouse security using log-based analysis: A review. In International Journal of Advanced Research in Computer Science and Software Engineering (Vol. 4, pp. 447-449).

[23] Santos, R. J., Bernardino, J., & Vieira, M. (2011a). Balancing security and performance for enhancing data privacy in Data Warehouses. Paper presented at the 2011IEEE 10th International Conference on Trust,

Security and Privacy in Computing and Communications.

[24] Santos, R. J., Bernardino, J., & Vieira, M. (2011b). A data masking technique for data warehouses. Paper presented at the Proceedings of the 15th Symposium on International Database Engineering & Applications.

[25] Brabson, B. (2004). How to Learn Visual Basic Programming. A step-by-step guide to tweaking your PC experience (There's no secret to writing good code). Maximum PC May 2004, 60-66.

[26] Manu, & Goel, A. (2017). Encryption algorithm using dual modulus. Paper presented at the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT).

[27] Tongkaw, S., & Tongkaw, A. (2016). A comparison of database performance of MariaDB and MySQL with OLTP workload. Paper presented at the 2016 IEEE Conference on Open Systems (ICOS), Langkawi, Malaysia.

[28] Chandrashekar, P., Dara, S., & Muralidhara, V. (2015). Efficient format preserving encrypted databases. Paper presented at the 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT).

[29] Sanchez, J. C. (2016). Investigating the star schema benchmark as a replacement for the TPC-H decision support system. Master's Thesis, East Carolina University.

## 7. APPENDIX A: TPC-H SCHEMA FOR LINEITEM.

The TPC-H consists of eight tables, namely, Supplier, Part, Partsupp, LineItem, Customer, Orders, Nation, and Region as can be seen in Figure 13. The schema represents a simple data warehouse dealing with sales, customers and suppliers. Customers order products, which can be bought from more than one supplier. Every customer and supplier are located in a nation, which in turn is in a geographic region. An order consists of a list of products sold to a customer. The list is stored in LineItem where every row holds information about one order line. There are several date fields both in LineItem and in Orders, which store information regarding the processing of an order (order date, ship date, commit date and receipt date). The central fact table in TPC-H is LineItem although Partsupp can also be considered another fact table.

The Scale Factor (**SF)** determines the ratio at which the data is loaded into a DW database. It is used to increase the size of the database throughout the benchmarking process. The value in front of SF is the number of rows of data for each table.

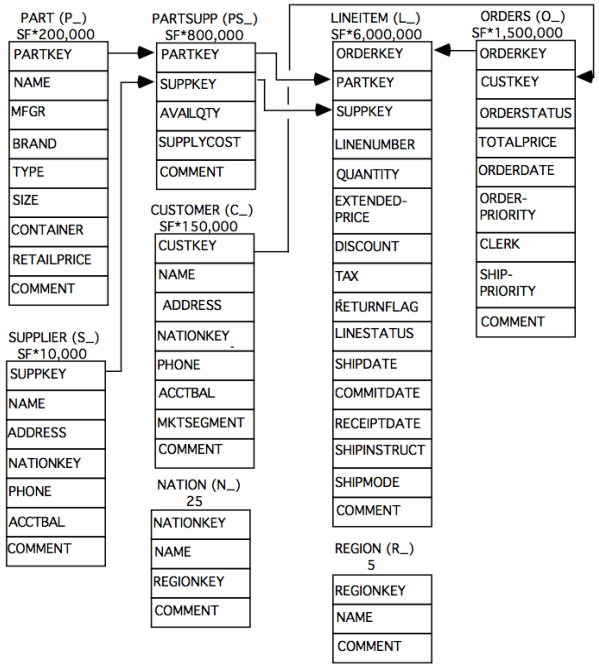



**Figure 14. TPC-H Schema. Source: [29]**

## 8. APPENDIX B: DATA MASKING AND ENCRYPTION EXPERIMENTAL RESULTS

In this appendix, we present the averages for the data masking and encryption experimental results. Each result is gotten from the execution of four rounds of experiments and shown in Table 5.

**Table 5: Sample Tests run per Test Case**

| Test 1 | | |
|---|---|---|
| Rows | 500,000 | |
| **Test case** | **Second** | **MB** |
| Case 1 | 44.5160 | 77.6 |
| Case 2 | 40.8673 | 77.6 |
| Case 3 | 44.5714 | 77.6 |
| Case 4 | 45.5383 | 77.6 |
| **Average** | **44** | **78** |

| Test 2 | | |
|---|---|---|
| Rows | 1,000,000 | |
| **Test case** | **Second** | **MB** |
| Case 1 | 90.3282 | 148.7 |
| Case 2 | 91.5370 | 142.7 |
| Case 3 | 89.8518 | 142.7 |
| Case 4 | 90.1704 | 143.7 |
| **Average** | **90** | **144** |

| Test 3 | | |
|---|---|---|
| Rows | 1,500,000 | |
| **Test case** | **Second** | **MB** |
| Case 1 | 134.8201 | 223.8 |
| Case 2 | 134.6162 | 225.8 |
| Case 3 | 131.4730 | 224.8 |
| Case 4 | 153.7349 | 218.8 |
| **Average** | **139** | **223** |

| Test 4 | | |
|---|---|---|
| Rows | 3,000,000 | |
| **Test case** | **Second** | **MB** |
| Case 1 | 281.3464 | 439 |
| Case 2 | 270.8838 | 459 |
| Case 3 | 277.3704 | 428 |
| Case 4 | 260.8134 | 432 |
| **Average** | **273** | **440** |

**Encryption Time for the TPC-H 1GB Fact Table per Solution**

| Test Case | No. of Rows | Data Size (MB) | MOBAT (sec) | MOD95 (sec) | Difference between the Algorithms |
|---|---|---|---|---|---|
| **Case 1** | 500,000 | 78 | 42 | 37 | 5 |
| **Case 2** | 1,000,000 | 144 | 87 | 76 | 11 |
| **Case 3** | 1,500,000 | 223 | 152 | 134 | 18 |
| **Case 4** | 3,000,000 | 440 | 321 | 295 | 26 |
| **Tot/Average** | **6,000,000** | **885** | **151** | **136** | **15** |

**Decryption Time for the TPC-H 1GB Fact Table per Solution**

| Test Case | No. of Rows | Data Size (MB) | MOBAT (sec) | MOD95 (sec) | Difference between the Algorithms |
|---|---|---|---|---|---|
| **Case 1** | 500,000 | 78 | 34 | 30 | 4 |
| **Case 2** | 1,000,000 | 144 | 80 | 79 | 1 |
| **Case 3** | 1,500,000 | 223 | 147 | 133 | 14 |
| **Case 4** | 3,000,000 | 440 | 282 | 261 | 21 |
| **Tot/Average** | **6,000,000** | **885** | **136** | **126** | **10** |

International Journal of Science and Engineering Applications
Volume 9 - Issue 06, 79 - 86, 2020, ISSN:- 2319 - 7560

# Introducing Geotourism Attractions in Toroud Village, Semnan Province, IRAN

Aref Shirazi
Amirkabir University of Technology
Tehran, Iran

Adel Shirazy
Shahrood University of Technology
Semnan, Iran

**Abstract**: Today, the role of tourism industry is more and more developed in any country and all countries try to have the maximum use of this industry, , as one of the important indicators of development, and the place of each country is identified in the optimal use of this important issue. In the meantime, despite the fact that Iran has received significant potential, Iran has not been able to use it as it needs to be. This matter is not focused solely on places and recreation centers, ancient and cultural, because we also have other well-known potentials in other natural arenas, which so far have received less attention in this regard. An important feature of ecotourism is one of these. But the tourism industry has stepped up in the last decade and has entered a much more serious and recent area of utilization and exploitation of the capabilities of geo-tourism. Along with the main pillar of the industry, the idea of creating geoparks by the UNESCO Organization is to protect and identify the 4 billion years old Earth heritage. Meanwhile, Iran, with a significant and very important history of geology, which has long been of interest to all foreign and domestic researchers and researchers, has a great potential and potential for creating geoparks. One of these areas is the Toroud village and its surroundings in the southern part of Shahroud city, Semnan province of Iran. In this article, in addition to introducing this very important area from the perspective of the writer as the center of decorative and semi-precious stones in Central Iran, it has tried to attract the attention of all governmental and non-governmental officials along with other interested researchers.

**Keywords**: Tourism; Ecotourism; Geotourism; Geopark; Toroud; Semnan; Iran

## 1. INTRODUCTION

Geotourism consists of two parts: geo and tourism. The first part includes geological attractions, geomorphology and mining heritage [1]. The second part, as a multidisciplinary theme, includes all the infrastructure of the tourism industry, including interpretation, management, accommodation, tours, and unlike ecotourism, which places the attractions of nature in the center of attention, the industry is generally attracted by attractions Inanimate nature deals [2]. Geotourism audiences are not only geologists and geomorphologists, but also ordinary tourists and nature enthusiasts. During the activities of geotourism, tourists, while visiting the beautiful phenomena and special geology and geomorphology, familiar with the foundations of their emergence, find their essential significance [3]. In China, due to the existence of geosites and beautiful landscapes, local authorities have focused on geo-tourism as one of the tools for new economic growth [4]. By creating each Geo site, the Chinese have created many jobs each year, and have more than 1 million visitors annually from geotourism [5]. Scientific tourism is another branch of tourism that can be attributed to scientific activities. For example, in mining, mineral processing, in which complex industrial methods are used. Or geological, archaeological or even mineral exploration (sampling, geochemistry, implementation of the results of statistical studies in field operations) can be used as scientific tourism goals for students and those interested in this field [6-12] .

The Geo-Parks Information System of Iran was established in 2004 with the assistance of the Geological Survey of Iran, based on the UNESCO Geo-Parks Network's International Geoscience Network Model, by the Geosciences Database of Iran. A serious effort has also been made to study geo-tourism since 2005 for a part of the western part of Qeshm Island, and now besides Qeshm Island, the geopark project of Sabalan region in Ardebil province is also being studied and compiled [13]. So here we will mention the number of countries and the number of geoparks created by them supported by UNESCO. China with 39 geoparks, and Germany with 5 geoparks, Spain 13 geoparks and Italy 10 geoparks [14]. Many geological structures can be identified by satellite imagery and remote sensing studies [15, 16] .

## 2. GEOGRAPHIC LOCATION AND GEOLOGY OF THE STUDY REGION

The Toroud village is located in the southern part of the Shahroud city, on the edge of the desert. The village is located in Semnan Province, Shahroud, in the central part of the Toroud rural district in terms of political-administrative divisions [17]. The geographical location of the village is located at 35 ° 25’ 38” N and 55 ° 00’ 55” E. Due to the geographical location of the village from the north to the Dolab rangeland, south to the Kavir desert, to the Kal Shor River (first Turan Wildlife Park) and the West to the Baamo rangelands. Distance from village to Shahrood city is more than 120 km (Figure 1,2) [18]. Its population is about 4500 people, and its relatively large area (20013 km2) has a large population dispersion. More than half of its population has migrated to cities such as Shahrood. The jobs of people in this region are livestock farming, including camel and sheep, and also agriculture. The agricultural products of the barley, wheat, cotton, garlic, turnips and tree products of those dates are limited to figs and pomegranates.

The agricultural lands are drunk by aqueduct. In 1953, an earthquake with 6.9 richter magnitude completely destroyed the Toroud village, and the current Toroud was built adjacent to the ruined village with clay and mud and wood. According to the quotations of the distant past, this area was the passageway of caravans, and along the southern edge of the desert, such as Khour, Biabanak, Jandagh and northern areas such as Shahrood, Damghan and Beyyrjmand, it was important in terms of distribution of goods. The carpet weaving has begun in the region about 40 years ago with the Naine design, and is now also popular. The area is rich in geology and minerals, and there are copper, lead, bentonite,

barite, manganese and some gemstones from the opal and agate family and gold minerals in it.

Fig1. Location Map of the Toroud village [18].

Fig 2. Torud location on the map

## 3. CENTRAL IRANIAN BLOCK GEOLOGY

In the constructional divisions of Iran, which was reported by Stocklin in 1968, Central Iran's unit includes all parts of the country that lies between the Alborz mountains in the north and the Esfandagh-Marivan in the south and the Loot block in the east as a triangle. According to this report, central Iran, like the adjacent regions in the first period, has a characteristic feature, but in the second and third period (the beginning of Alpine movements), it has been a very moving region for orthogonal movements. The intrusions and influences of the internal masses are witnessed, and eventually this zone is compressed in the last phase of the Alpine, in which folds, faults, and complex deformations have arisen. This area is introduced as a unit for geological characteristics. The whole central Iran zone is divided into four parts. The most important part that includes the plain of the desert and the study area is also the Neogene-Quaternary basin. Ofcourse, all the large inner basins of Central Plateau are formed in the late Miocene. The bottom of the basin in Quaternary and even now is gradually subsiding [19].

## 4. GEOTOURISTIC & TOURIST AREAS OF THE REGION

Major sources of water, such as Haj Aligholi Salt Lake, is one of the largest salt marshin Iran. The lake is a triangular state with its head in the north and the lake's water catchment area is about 2500 $Km^2$. The water of this lake is very salty and is very beautiful at sunset from the Siahkooh peaks. Salt Lake is the basin of many of the central rivers in Iran, and there are many marshes around it, although there are no aquatic species in the lake, but in the winter, a significant number of aquatic migratory birds come to this lake and the surrounding rivers. Years ago, in the summer, a number of flamingos were seen in its southern regions. Other ponds, such as the Abgirmakoosh, the Beerezard, the Asbeqadir are mostly dried up and the flood gathering place.

**The rivers of the region include:**

- **Bandalikhan river:** This river is the most important river in the protected area of the desert. It is the source of this river from the mountain of Khersang, which creates the Jajrood River. The river crossed the protected areas of Varchin, Jajrud and Khojir National Park in Parchin, which enters the Varamin Plain, has several branches and is used for irrigation, and drains the Jajroud River and the Tehran sewage system in the plain of Varamin Received in Bandalah Khan entered the protected area.
- **Gharechay river:** From Rasund Mountains in southern Arak, after passing from Arak and Saveh, the river Qomrood river into Salt Lake. The upper branch of the river near the unprotected deserts of the winter habitat is the habitat of various aquatic migratory birds, especially the cave, the ducks and green ducks, and dry ducks such as crests and winds in all seasons and it is important.

Ainorashid, Abmahale, Shekarab, Nakhjir, Cheshmeh Shahi, siahkooh are the most famous springs of Kavir National Park, which are currently supplying water to Ghasre Baharam. Cheshmeshahi Spring is a passionate water that has been driven by the tube to Ghasrebahram for public use. Around the fountain, the straw and cam tree are abundantly seen. The other springs that feed the cattle include: Ainorashid, Hozaghamohammad, Abmahale, Boz, Sorkh, Peyghambar, Abgole, Ghajariye, Shekarab, Talhe, Malekabad, Zanboori, Ab-barik, Lakab, Mirabderaz. In addition to having desert plant communities, semi-desert and vegetation communities of saline soils in mountainous parts with steppe plant communities. Many of the sandy and sandy beaches are characteristic of the most desert areas. Desert National Park plants are drought-tolerant (Xerophyte) and passionate (halophyte) species, which have been exposed to water scarcity as a live indicator of adverse ecological conditions for a fraction of the year, and for survival and adaptation to shortages Water and salinity of the soil find a special building that indicates the dryness and biological constraints of these plants to deal with dehydration, high temperatures, small leaves leading to thorns that indicate the dryness and biological constraints of these plants to deal with dehydration The heat of the small leaves leads to thorns.

## 5. BEAUTIFUL NATURAL AREAS FOR THE COMMON PEOPLE

In the Toroud village, considering the particular geological position, you can explore the beautiful developments of desert nature. One of these beautiful areas is deserts. (Figure 3,4)

Fig 3. A view of Alhagi bush in torud village.

Fig 4. Kooh Pineh area 18 km north of Trod

## 6. ATTRACTIONS IN THE REGION's GEOLOGY

**1- Gully erosion**

A gully is a landform created by running water, eroding sharply into soil. Gullies resemble large ditches or small valleys, but are meters to tens of meters in depth and width. When the gully formation is in process, the water flow rate can be substantial, causing a significant deep cutting action into soil [20]. According to the gully map (Figure 5), the surface of gully erosion in toroud basin is about 97.25 hectares [21].

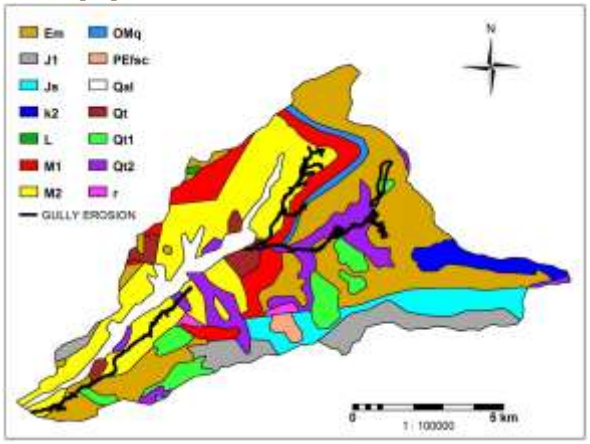



Fig 5. geology of toroud basin and gully erosion extension [21].

The research on the lithology and soil type in Toroud basin shows that most erodible sediments in this region are related to the age of Eocene and Miocene include Marl, Limestone, Shale, Sandstone, Conglomerate and etc. [21]. The high amount of gully surface is related to the Eocene period include, Marl, Marl stone, Limestone and tuff that is equal 41.65 percent of whole gully erosion in this region [21]. Pictures of gullies are shown in the **figures 6 and 7.**

Fig 6.Piping in the gully

Fig 7.Hole in the gully

There are many researchers that are interested to study

**2- ornamental and semi-precious stones**

Among the prominent features of this area are the existence of different mines that create the special ornamental and semi-precious stones. Some of the stones that have been harvested from this area and even sold by villagers:

Amethyst, turquoise, crystalline quartz (known as Dorrenajaf), Onyx (Soleymani agate), tree opal, varieties of agates (green and purple and red, etc.), moss agate and etc. (Figure 8).

- **Analcime** or analcite (from the Greek analkimos - "weak") is a white, gray, or colorless tectosilicate mineral. Analcime consists of hydrated sodium aluminium silicate in cubic crystalline form. Its chemical formula is $NaAlSi_2O_6 \cdot H_2O$. Minor amounts of potassium and calcium substitute for sodium. A silver-bearing synthetic variety also exists (Ag-analcite) [22].

- **Amethyst** is a violet variety of quartz. The name comes from the Koine Greek ἀμέθυστος amethystos from ἀ- a-, "not" and μεθύσκω methysko / μεθύω methyo, "intoxicate", a reference to the belief that the stone protected its owner from drunkenness[23]. The ancient Greeks wore amethyst and carved drinking vessels from it in the belief that it would prevent intoxication. Amethyst is a semiprecious stone often used in jewelry and is the traditional birthstone for February.

- **Barite** is a mineral consisting of barium sulfate ($BaSO_4$). Barite is generally white or colorless, and is the main source of the element barium [24].

- **Agate** is a common rock formation, consisting of silica, chalcedony and quartz as its primary components. the formation consists of a wide variety of colors and grain size. Agates are primarily formed within volcanic rocks and metamorphic rocks. These stones have been seen to have dated back as far as Ancient Greece, however with their mediocre durability, their everyday uses are most commonly as decorations or jewelry [25]. Lace agate is a variety that exhibits a lace-like pattern with forms such as eyes, swirls, bands or zigzags [26].

- **Cerussite** (also known as lead carbonate or white lead ore) is a mineral consisting of lead carbonate ($PbCO_3$), and an important ore of lead. The name is from the Latin cerussa, white lead [27].

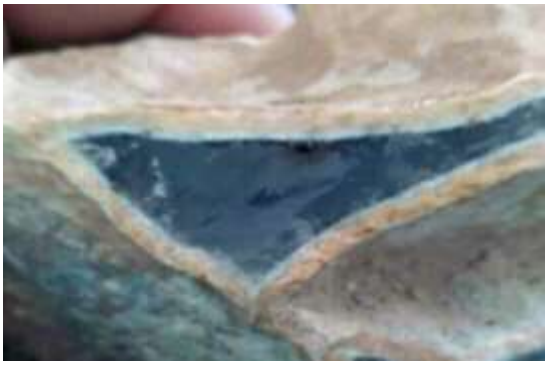
- **Calcite** is a carbonate mineral and the most stable polymorph of calcium carbonate ($CaCO_3$). Calcite is derived from the German Calcit, a term coined in the 19th century from the Latin word for lime, calx (genitive calcis) with the suffix -ite used to name minerals. It is thus etymologically related to chalk [27]. This mineral is found in most of areas of iran [28]

A

B

C

D



E

I

F

J

G

K

H

L

M

N

Fig 8. Common rocks and minerals found in the torud

(A: Analsim , B: Amethyst, C: Barite, D: Agate, E: Dendritic Agate, F: geod agate, G: Moss Agate, H: Silica, I: Jasper, J: Turquoise, K: Onyx, L: Jade, M: Cerussite ,N: calcite )

## 7. THE PUBLIC BEAUTIES OF THE AREA

The Toroud village, due to its historic history, has historical attractions as well as natural attractions. Specific species of this region, such as the camel of the desert, the Asian zebrafish (Khar Turan) and the Cheetah, and etc. are among the other natural charisma of the plain of Kavir desert (Figures 9-11).

Fig 9. Historic monuments and geological aesthetics around it

Fig 10. Palm trees in the Torud village

Fig 11. Some species of animals in the area

## 8. CONCLUSION

The Toroud village is located in the southern part of the city of Shahrood, on the edge of the desert. Due to the specific situation of the village and the opinion of the village around it, the village has geologically diverse attractions for geologists and others. In addition to geological features that include desert, mines, geological phenomena and zeinous rocks, this area also has vegetation coverings and a variety of animal life. The geopark potential of this region can be seen in the area. These studies are important to the attention of the more authorities, and it is hoped that the results will also lead to other parts of our beloved country.

## 9. REFERENCES

[1] R. K. Dowling, "Global geotourism–an emerging form of sustainable tourism," *Czech Journal of Tourism*, vol. 2, no. 2, pp. 59-79, 2013.

[2] N. T. Farsani, C. O. Coelho, C. M. Costa, and A. Amrikazemi, "Geo-knowledge management and geoconservation via geoparks and geotourism," *Geoheritage*, vol. 6, no. 3, pp. 185-192, 2014.

[3] J. Larwood and C. Prosser, "Geotourism, conservation and society," *Geologica balcanica*, vol. 28, pp. 97-100, 1998.

[4] Z. Xun and Z. Ting, "The socio-economic benefits of establishing National Geoparks in China," *Episodes*, vol. 26, no. 4, pp. 302-309, 2003.

[5] R. K. Dowling and D. Newsome, *Geotourism*. routledge, 2006.

[6] S. Alahgholi, A. Shirazy, and A. Shirazi, "Geostatistical Studies and Anomalous Elements Detection, Bardaskan Area, Iran," *Open Journal of Geology*, vol. 8, no. 7, pp. 697-710, 2018.

[7] S. Khakmardan, A. Shirazi, A. Shirazy, and H. Hosseingholi, "Copper Oxide Ore Leaching Ability and Cementation Behavior, Mesgaran Deposit in IRAN," *Open Journal of Geology*, vol. 8, no. 09, p. 841, 2018.

[8] A. SHIRAZI and A. HEZARKHANI, "Predicting gold grade in Tarq 1: 100000 geochemical map using the behavior of gold, Arsenic and Antimony by K-means method," 2018.

[9] A. Shirazi, A. Shirazy, S. Saki, and A. Hezarkhani, "Introducing a software for innovative neuro-fuzzy clustering method named NFCMR," *Global Journal of Computer Sciences: Theory and Research*, vol. 8, no. 2, pp. 62-69, 2018.

[10] A. Shirazi, A. Shirazy, S. Saki, and A. Hezarkhani, "Geostatistics Studies and Geochemical Modeling Based on Core Data, Sheytoor Iron Deposit, Iran," *Journal of Geological Resource and Engineering*, vol. 6, pp. 124-133, 2018.

[11] A. Shirazy, A. Shirazi, M. H. Ferdossi, and M. Ziaii, "Geochemical and Geostatistical Studies for Estimating Gold Grade in Tarq Prospect Area by K-Means Clustering Method," *Open Journal of Geology*, vol. 9, no. 6, pp. 306-326, 2019.

[12] A. Shirazi, A. Hezarkhani, A. Shirazy, and I. Shahrood, "Exploration Geochemistry Data-Application for Cu Anomaly Separation Based On Classical and Modern Statistical Methods in South Khorasan, Iran," *International Journal of Science and Engineering Applications*, vol. 7, pp. 39-44, 2018.

[13] A. G. Yalgouz-Agaj, L. Ardebil, and S. Karimdoust, "Identification of some of the geotourism sites in Iran," *World Applied Sciences Journal*, vol. 11, no. 11, pp. 1342-1347, 2010.

[14] UNESCO. "List of UNESCO Global Geoparks (UGGp)." http://www.unesco.org/new/en/natural-sciences/environment/earth-sciences/unesco-global-geoparks/list-of-unesco-global-geoparks/

[15] A. Shirazi, A. Shirazy, and J. Karami, "Remote Sensing to Identify Copper Alterations and Promising Regions, Sarbishe, South Khorasan, Iran," *International Journal of Geology and Earth Sciences*, vol. 4, no. 2, pp. 36-52, 2018.

[16] A. Shirazi, A. Hezarkhani, A. Shirazy, and I. Shahrood, "Remote Sensing Studies for Mapping of Iron Oxide Regions, South of Kerman, IRAN," *International Journal of Science and Engineering Applications*, vol. 7, no. 4, pp. 45-51, 2018.

[17] K. Roustaei, "Archaeo-metallurgical reconnaissance of ancient mines and slag sites on the northern edge of the Dasht-e Kavir Desert, Iran," *Iranica Antiqua*, vol. 47, p. 351, 2012.

[18] N. Ambraseys and A. Moinfar, "The sessmicity of IRAN: The Torud earthquake of 12th february 1953," *Annals of geophysics*, vol. 30, no. 1-2, pp. 186-200, 1977.

[19] J. Stoecklin, "Structural history and tectonics of Iran: a review," *AAPG bulletin*, vol. 52, no. 7, pp. 1229-1258, 1968.

[20] P. R. Christensen, "Formation of recent Martian gullies through melting of extensive water-rich snow deposits," *Nature*, vol. 422, no. 6927, pp. 45-48, 2003.

[21] F. Mousazadeh and K. O. Salleh, "The influence of lithology and soil on the occurrence and expansion of gully erosion, Toroud Basin–Iran," *Procedia-Social and Behavioral Sciences*, vol. 120, pp. 2014.

[22] C. S. Hurlbut and C. Klein, *Manual of mineralogy (after James D. Dana)*. Wiley, 1977.

[23] A. crystals from Mexico, "Mohs scale hardness."

[24] J. D. Dana and W. E. Ford, *Dana's manual of mineralogy for the student of elementary mineralogy, the mining engineer, the geologist, the prospector, the collector, etc*. J. Wiley & Sons, 1912.

[25] Y. Wang and E. Merino, "Self-organizational origin of agates: Banding, fiber twisting, composition, and dynamic crystallization model," *Geochimica et Cosmochimica Acta*, vol. 54, no. 6, pp. 1627-1638, 1990.

[26] R. Simmons and N. Ahsian, *The book of stones: Who they are and what they teach*. North Atlantic Books, 2015.

[27] J. W. Anthony, *Handbook of mineralogy*. Mineral Data Publishing, 1990.

[28] Shirazy, A., Shirazi, A., Ferdossi, M. H., & Ziaii, M. (2019). Geochemical and Geostatistical Studies for Estimating Gold Grade in Tarq Prospect Area by K-Means Clustering Method. *Open Journal of Geology*, *9*(6), 306-326.

International Journal of Science and Engineering Applications
Volume 9 - Issue 06, 87 - 90, 2020, ISSN:- 2319 - 7560

# Metal Filled Carbon Nanotubes for Targeted Radiation Therapy: A Feasibility Study

| S. Ashmeg | M. Rodriguez | D. Gregory | A. Parbatani | E. Eienbraun |
|---|---|---|---|---|
| SUNY Polytechnic Institute | SUNY Polytechnic Institute | SUNY Polytechnic Institute | SUNY Polytechnic Institute | SUNY Polytechnic Institute |
| Albany, NY 1220 | Albany, NY 1220 | Albany, NY 1220 | Albany, NY 1220 | Albany, NY 1220 |

**Abstract**: This research involves demonstrating the viability of filling the nanotubes with copper and characterizing its effectiveness as a vehicle for transport of radionuclide. A two-step filling method has been adopted in this study. First, the multi-walled carbon nanotubes (MWCNTs) closed ends were opened by acid reflux; then, using the capillary effect, the tubes were filled with copper by sonicating them in a copper salt solution. The effects of changing the reflux time, changing the molar concentration and replacing the copper nitrate salt with copper chloride have been studied. The success of this process has been tested using scanning electron microscopy (SEM), energy dispersive x-ray spectroscopy (EDS), x-ray photoelectron spectroscopy (XPS) and transmission electron microscopy (TEM). Using a 12 hour reflux time in 68% $HNO_3$ resulted in opening of the MWCNTs which in turn allowed filling them with copper. The filling took place by sonicating the opened MWCNTs in 0.87 mol/L $Cu(NO_3)_2$ solution. Subsequent characterization by EDS and XPS show the presence of copper in the MWCNTs. Variations in reflux time and copper molar concentration were observed to change the copper concentration. TEM images show that the Cu nanoparticles are located inside the nanotubes.
Multi-walled carbon nanotubes were reproducibly filled with copper using a $Cu(NO_3)_2$ solution. Altering the reflux time and the copper molar concentration were shown to affect the subsequent copper concentrations in the MWCNTs. These data form a proof of concept supporting the ability to use MWCNTs filled with copper for targeted radiotherapy.
**Keywords**: CNTs, MWCNTs, Carbon Nanotubes, Radiotherapy, Targeted Therapy.

## 1. INTRODUCTION

Carbon nanotubes (CNTs) are known for their unique physical and chemical properties. CNTs can be single-walled or multi-walled, and can possess a range of chiralities, diameters, and lengths, all of which affect the character of the CNT [1]. Nano-carriers, including carbon nanotubes, are being extensively studied for use in cancer diagnostics and therapies. In comparison to other Nano-carriers, CNTs have superior flow dynamics and better cell permeability due to their needle-like shape [2,3,4,5]. In addition, they can be shortened and functionalized to decrease toxicity [5,6,7]. Both the insides and outsides of the tubes can be utilized to carry treatment and targeting agents simultaneously. Consequently, carbon nanotubes have been the focus of many in-vitro and in-vivo studies where they serve to carry bio-functional agents [2, 3, 4, 5, 6].

The filling of carbon nanotubes with metallic nanoparticles is an established procedure in many fields and there are several methods to fill the CNTs whether using melted solids or salt solutions [7,8]. The solution method is chosen here to minimize the risk of radiation hazard, the alternative would require melting a radioactive material.

$Cu^{67}$ is a radioactive copper isotope that primarily decays via beta emission with a half-life of 2.6 days to $Zn^{67}$. The average range of the emitted beta particle is 5 mm in water, which makes this source suitable for small tumors with minimal shielding concerns[9]. This work describes a study to determine the feasibility of filling carbon nanotubes with copper as a first step to be used in targeted radiotherapy.

## 2. MATERIALS AND METHODS

The process for filling MWCNTs was done in two steps: first, opening the MWCNTs, followed by impregnating the MWCNTs with copper.

To open the MWCNTs, the tubes are stirred and refluxed in 68% nitric acid at 120°C for times between 12 and 24 hours. When refluxing, the MWCNTs and the acid are combined in a flask, with a magnetic rod for stirring. This process functionalizes the tubes and breaks the carbon-carbon double bonds at the CNT ends. After reflux, the tubes are washed with deionized (DI) water until pH-neutral. Then the wet tubes are left in an oven at 65°C for at least 24 hours to dry.

After the tubes are dried, they are sonicated in 0.87 mol/L $Cu(NO_3)_2$ solution for 30 minutes followed by DI water wash and sonication in DI water for another 30 minutes. The filled and washed MWCNTs are left to dry and samples are then prepared for analysis. Sample preparation is done by dropping filled MWCNTs sonicated for one minute in ethanol on 1x1 $cm^2$ pieces of Si, or onto a copper grid for TEM analysis. For SEM and EDS analyses, the Si samples were mounted on stubs using double sided carbon tape to secure them. Samples for XPS analyses were mounted directly on the removable stage using copper pins to secure the samples.

For copper filling analysis, SEM and TEM images were collected along with EDS and XPS spectra. A Zeiss LEO 1550 SEM (Zeiss, Oberkochen, Germany), with a field emission source was used. The sample is bombarded with 3-5 keV electrons. As those electrons strike the sample, secondary electrons leave and get collected by an in-lens detector located in the same column as the electron gun. For EDS, the SEM system is used but the stage is dropped down to around 15mm away from the pole piece and the accelerating voltage is increased to > 10 kV. The x-rays from the sample are detected by a Bruker x-ray detector mounted on the SEM tool.

For XPS analyses, a ThetaProbe (Thermo Fisher Scientific, Waltham, MA) x-ray photoelectric spectroscope was used. The x-rays in the XPS tool are produced from an aluminum source then filtered by a crystal resulting in a monochromatic Kα x-ray beam (1486.6 eV) striking the sample. The analysis area is 100 micrometers in diameter which is poor lateral resolution for nanomaterials. However, the data is collected from the first few nanometers from the surface giving a superior depth resolution when compared to EDS. In addition, XPS shows the chemical forms of the elements present in the sample. Combining the two spectroscopes provides sufficient data to support existence of Cu in the samples.

For transmission electron microscopy (TEM), a JEOL 2010 was used (JEOL, Tokyo, Japan). In TEM, the electrons are accelerated by an applied high voltage (200kV) and travel across a thin sample to provide a contrasted image based on the atomic number of the material.

# 3. RESULTS

## 3.1 Imaging of filled MWCNTs

Figure 1 represents SEM images of a sample with copper filled MWCNTs. The images of all the samples look similar, including the ones of unfilled MWCNTs. Therefore, more data from different modalities had to be acquired.

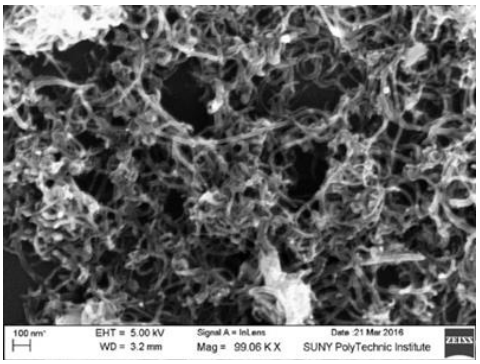



**Figure 1: Bright and dim MWCNTs are circled in the image on the right to highlight where the EDS data was collected from**

To verify that the copper is nucleated inside the tubes, TEM images were collected and they show partial filling of carbon nanotubes with copper. Unlike SEM, in TEM high atomic number materials such as Cu show as dark due to absorption of the electron beam, while the areas that transmit more electrons correspond to lighter atoms (such as carbon). TEM images in Figure 2 show success in partially filling the MWCNTs with Cu using $Cu(NO_3)_2$ solution.

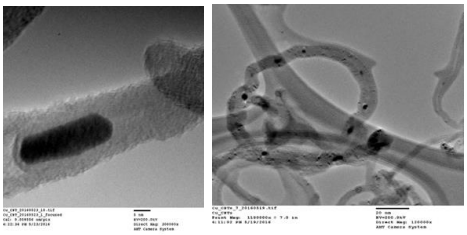


**Figure 2: TEM images show that the carbon nanotubes are partially filled with copper.**

## 3.2 Compositional analysis

To verify the copper filling of MWCNTs, EDS spectra were collected from the bright spots in the SEM images and compared to EDS data collected from dimmer areas in the MWCNT SEM images and to the Si background with no MWCNTs. The spectrum in figure 3, below, represent the composition of the sample imaged in figure 2.

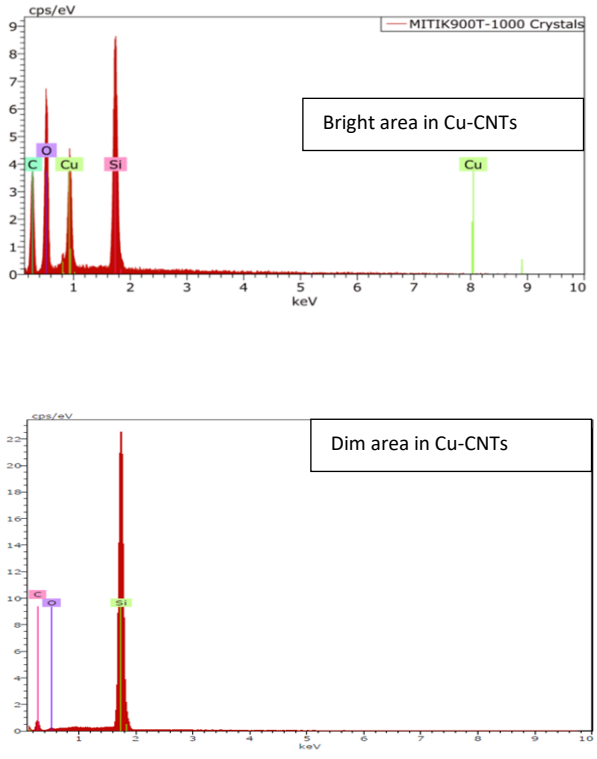



**Figure 3: EDS spectra of two different areas in a sample prepared using Cu(NO3)2 solution.**

The results show higher Cu content in the bright MWCNTs, from SEM imaging, compared to that from the less bright samples and from the background. However, due to the nature of this analysis technique, most of EDS signals are collected from more than 20 nm deep below the sample surface.

Therefore, the highest signal from each samples is always of Si. The carbon signal is a combination of signal of carbon nanotubes and contamination on the Si surface. The oxygen signal is from the surface contamination and functionalization of MWCNTs. The functionalization takes place in the opening process, during the acid reflux.

The same sample was analyzed by XPS, for surface characterization of the top few nanometers of the sample[10]. Because of that, the background silicon content is shown to be much lower in XPS than in EDS. In XPS, the initial scan is a survey to determine what elements exist in the sample. Following that, a high-resolution scan of each photoelectron peak is performed and this data is used for quantitative analysis of peak area and binding energy (Fig. 4).

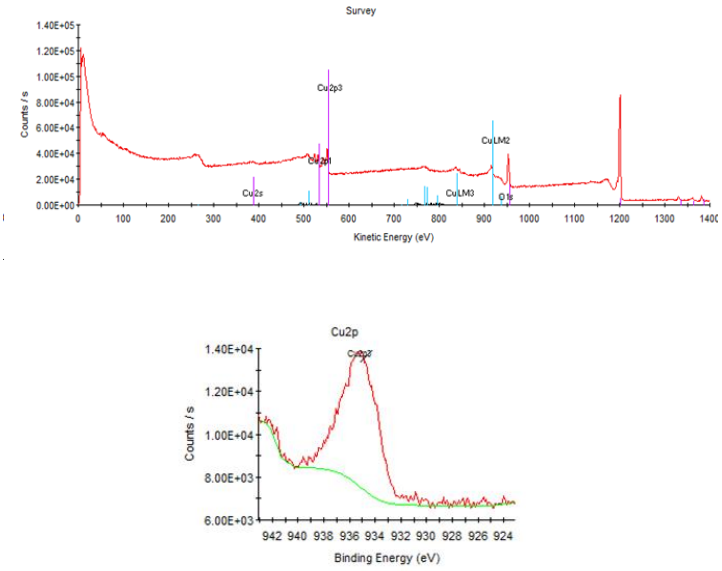



**Figure 4: XPS spectra of analyzed data. The top spectrum is a survey of the sample while the bottom spectrum is a high-resolution scan of a copper peak**

To study the effect of variation of the filling process, the reflux time and the molar concentration of the acid have been altered. Table 1 is a summary of the various reflux times and $Cu(NO3)_2$ salt concentrations used and the effects on measured copper concentration. Doubling the reflux time and the copper salt molar concentration increased the copper content by more than four and two-fold respectively.

**Table 1: effect of doubling the acid reflux time and/or the copper salt molar concentration in copper filling**

| Set # | *Set 1* | *Set 2* | *Set 3* |
|---|---|---|---|
| **$HNO_3$ reflux time** | 12 hours | 24 hours | 24 hours |
| **$Cu(NO_3)_2$ molarity** | 0.87 mol/L | 0.87 mol /L | 1.74 mol/L |
| **XPS Cu%** | 0.14 % | 0.91% | 1.71% |
| **EDS Cu%** | 1.46% | 4.43% | 8.58% |

## 4. DISCUSSION

In this study, we filled MWCNT's with copper using copper (II) nitrate under acid reflux. The collected data suggests that the filling procedure could be further optimized and is an element of further study. These data were consistent with both XPS and EDS, but both methods have drawbacks that need to be noted.

EDS is a very focused measurement, probing an area of a few nanometers in diameter and tens of nanometers depth. These measurements are focused on dim or bright regions and represent a small area, as such, they may not be representative of the whole sample. XPS complements this measurement in that these scans were over a region with diameter of 100 microns and depth to around 2-10 nm. The fact that these methods both lead to similar results, showing Cu existence in the studied sample and showing variation in the amount of copper with the alteration of the filling process, yields confidence that the data are consistent. However, quantitative conclusions based upon them are more difficult to draw as it can't be ruled out that some residue or surface copper was part of either measurement. This question should be part of further study in optimizing the filling procedure of MWCNT.

We used TEM to confirm that the copper in these MWCNT was, indeed, inside the nanotubes and not simply bound to the outside. Our TEM images show that we were successful in filling these nanotubes, but don't shed any light on whether there was surface copper or residue and to what degree. While we can say definitively that the MWCNT were partially filled with copper, measuring the amount and optimizing that process remains a subject of further study.

In the initial phase of this study, we used copper (II) nitrate to fill the nanotubes because this was a convenient and commercially available copper salt. The point, however, of this study is to demonstrate the feasibility of filling nanotubes

with 67Cu, which is typically available as a chloride salt. We repeated the experiment with copper (II) chloride and achieved similar results with similar concentrations and reflux times. (You should add a leading sentence explaining that the radioactive source would limit the metal ion concentration in the solution. The use of copper (II) chloride in concentrations equal to that which would be attainable with 67Cu, however, resulted in a very dilute solution which could not be measured with and of the methods we used here. However, the MWCNTs filled with non-radioactive Cu can be repurposed.

## 5. CONCLUSION

Partial filling of MWCNTs with Cu was observed under various processing conditions and using two types of copper solutions. These results show that it is feasible to fill carbon nanotubes with a radioactive Cu source for potential targeted radiotherapeutics applications. A variation of the Cu concentration was observed in the XPS and EDS data as a result of the variation of exposure time and concentration. However, TEM couldn't be used for quantification of the amount of copper in the MWCNTs, resulting in lack of confirmation of whether the increase in Cu is due to additional MWCNT filling rather than being due to residues around the MWCNTs. Replacing the $Cu(NO_3)_2$ with a $CuCl_2$ salt has also resulted in copper filled carbon nanotubes. This is a proof of concept of the feasibility of filling carbon nanotubes with $Cu^{67}$.

## 6. REFERENCES

[1] P. McEuen et.al., A. (2002). Single-Walled Carbon Nanotubes Electronics. IEEE Transactions on Nanotechnology, 1 (1), 78 – 85

[2] S. Ji et.al., A. (2010). Carbon Nanotubes in Cancer Diagnosis and Therapy. Biochimia et Biophysics Acta, 29 – 35.

[3] L. Williams et.al., A. (2008). Targeted Radionuclide Therapy. Medical Physics, 35 (7), 3062 – 3068.

[4] A. Ruggiero et.al., A. (2010). Imaging and Treating Tumor Vasculature with Targeted Radiolabeled Carbon Nanotubes. International Journal of Nanomedicine, 783 – 802.

[5] D. Peer et.al., A. (2007). Nanocarriers as an Emerging Platform for Cancer Therapy. Nature Nanotechnology, 2, 751 – 760.

[6] S. Hong et.al., A (2010). Filled and Glycosylated Carbon Nanotubes for in Vivo Radioemitter Localization and Imaging. Nature Materials, 9, 485 – 490.

[7] S. Murugesan et.al., A (2011). Amino-Functionalized and Acid Treated Multi-Walled Carbon Nanotubes as Supports for Electrochemical Oxidation of Formic Acid. Applied Catalysis B: Environmental, 103, 266 – 274.

[8] D. Ugarte et.al., A. (1998). Filling Carbon Nanotubes. Appl. Phys. A., 67, 101 – 105.

[9] N.I. Ayzatskiy, A. (2007). Comparison Of Cu-67 Production At Cyclotron andElectron Accelerator. Cyclotron and Their Applications, 243-245