MODIFICATIONS OF AN ENCRYPTED-BASED SQL MODELS FOR MULTILEVEL DATABASE

AHMED Y. MAHMOUD[1], MOHAMMED M. ABU-SAQER[2]

[1,2]Al-Azhar University-Gaza, Faculty of Engineering and Information Technology,

Department of Information Technology, Gaza, Palestine

E-mail: [1]ahmed@alazhar.edu.ps, [2]engmohammedsaqer22@gmail.com.com

ABSTRACT

Information security is becoming increasingly vital in a variety of applications. Database applications are no exception, and protecting information based on encryption plays a vital role in the protection of sensitive data. Securing data in several disciplines is a critical concern. Encryption was applied as a mechanism to secure data by database management systems and their applications. A promising approach has been seen in adopting multilevel security and encryption based on multilevel security. Recently, there has been an adaptation of the structure query language to be used in the encryption based on multilevel security; the used models are very time-consuming, especially for the large size of the database. In this paper, we proposed modifications of the models of select, update, and delete operations. The proposed modifications enhanced the performance of the models of select, update, and delete operations. The modification relies on the fact that we avoided repeating the decryption process and replaced it with a single encryption process. The obtained results show that the performances of the proposed modifications are better than the original model.

Keywords: *Multilevel Database, Encryption, Decryption, SQL Models, System Protection*

1. INTRODUCTION

Data are the essential element of any system and/or application. Protection of data is therefore a main necessity. As a result, companies and governments tend to devote considerable efforts to provide the necessary protection for sensitive data and information. Companies and governments seek to exploit all possible and available methods to protect such data and preserve their privacy form Hackers. Moreover, protecting their data from being accessed by those who are not authorized is a challenge.

Large institution or industrial enterprise that contains enormous quantities of equipment, products requires means of protection, especially if the property and the facility are massive. Then, enhancing the protection is necessary against intruder access and theft attempts.

The process of protecting data and preserving data in computerized systems is equally important, as it provides the basis for such systems. These systems are centered on providing services and building operations on such data. Therefore, failure to provide adequate protection for such data may adversely affect all enterprises, such as banks for example, any unauthorized access is a violation of the privacy of users and can cause harm to them, as well as the producing companies whose data is the main guide for the method of producing their goods, which are monopolized by them.

The major objective of security is to ensure that sensitive data is unreadable by unauthorized parties during storage, transmission and exchange [1].One of the methods/techniques used to achieve a secure transmission and exchange of information between the two parties is the encryption process.

The following three requirements must be met in order to improve security: confidentiality (C), integrity (I), and availability (A). CIA requirements [2], [3] are the name given to these three requirements. Researchers in the field of cryptography have so far focused their efforts on achieving the former requirements using a variety of encryption techniques such as hashing, asymmetric encryption, and symmetric encryption [4]–[11].

Multilevel security (MLS), on the other hand, was created to improve security. MLS has recently been used in a variety of domains, including military systems and databases; for example, the authors have used the select model-encryption based and its variant in the medical database systems [8]. The encryption based multi-level security mechanisms were used in [11]. The authors of [11] used the Bell-Lapadula model by MLS to classify the security level of each person (subject) and object (file, data source, and database components). The following methodology is used by MLS: (1) a subject (person, process, etc.) is not allowed to access/read an object (File, Database, data source, etc.) if the object's security level is higher than the subject's security level; (2) if the object's security level is lower than the subject's security level, the subject is not allowed to write to the object.

MLS methods will safeguard database systems against data loss and misuse, it's worth mentioning that we may use MLS to regulate the security policy in any given system [12].

If the MLS is used in conjunction with encryption, computerized systems may easily meet the CIA's application software security standards; the application software and information will be safe from unlawful and unauthorized users.

It is common knowledge that in the digital era, the usage of the internet and the massive dissemination of information on individuals; make the data essential for educational institutions, the government, and other service providers.. All businesses, organizations, and individuals who have databases are therefore required to protect their data.

The structure query language SQL has four fundamental operations (insert, select, update, and delete) that can be performed on a database. Although database security has been addressed by several researchers, there are very few that perform well in terms of security level and performance. To increase database security, certain computerized systems utilize encryption-based multilayer database models for all database activities. There are existing encryption-based multilevel database models for the former mentioned database operations, but these models are very time consuming due to the repetition of decryption operation, it becomes inefficient, especially with large data sets. In this paper, we proposed modifications of the models of select, update, and delete operations. The proposed modifications significantly enhanced the performance of the models of select, update, and delete operations. The rest of the paper is organized as follows: literature review is introduced in Section 2. The original models and the corresponding modified models are presented in Section 3. The performance of the modified models versus the original models and the experimental results are included in Section 4. Limitations of the research are presented in Section 5. Finally, we introduce the conclusion in Section 6.

2. LITERATURE REVIEW

In previous decades, symmetric and asymmetric encryption algorithms were considered in the literatures; recently, researchers have paid more attention to investigating, creating, and introducing new encryption algorithm categories; for example, the reader can see attributes-based encryption, homomorphic encryption algorithm categories, and Multilevel encryption algorithms [13]–[15].

NIST introduces and defines the idea of multilevel security encryption as the system that determines the privileges of users to receive information, either at or below its level. If the user has the same or lower level than the data, he/she can access (read) the data; if the user has the same level, then the user can write it. The MLS is then retained for the databases, which is helpful for putting a limit on unauthorized and unlawful database access. Researchers have devoted their effort to evaluate, develop encryption algorithms and authentication methods based on multi-level security in order to improve security and solve security issues (see for example [15]–[18]. The authors of [19] suggested an MLS schema based on the Pretty Good Privacy, Wireless Fidelity, and Hash Message Authentication Code systems. To ensure secrecy, the schema constructs and establishes communications using Pretty Good Privacy, and the messages are enciphered using the receiver's public key. Mahmoud et al. developed a system to examine the MLS theory in practice [11]. Furthermore, the developed system implemented several encryption methods in conjunction with MLS. The system was developed to investigate the encryption theory based on MLS for database management systems DBMS. The system was evaluated for encryption and decryption, and the implemented MLS proved to be a method for safeguarding databases.

Faragallah et al. presented a DBMS cipher that is based on the multilevel model[20]. They introduced the concept of multilevel security in relational databases and provide a comprehensive overview of an encryption-based multilevel security database model, which is a combination of multilevel security in relational databases and an encryption system that encrypts each record with an encryption key based on its security class level. Define the data manipulation procedures for the instance-based multilevel security paradigm as well. In addition, the authors of [17] introduced a novel paradigm for select operation based on multilayer security and suited to multilevel databases.

It is worth mentioning that despite of the enormous amount of effort that has been put forward by numerous researchers, these efforts have only devoted and addressed to one direction which is how to use and implement the concepts and mechanisms of multi-level security; they have not addressed how to enhance the performance of the used techniques. In this paper, we proposed modifications to the SQL operations models encryption based on multi level security to enhance the performance.

3. PROPOSED MODIFICATIONS OF THE SQL OPERATIONS MODELS

In this section, we shall present the original models of select, update and delete in the SQL and our proposed modifications for the select, update, and delete SQL operations. Note that The following notations will be used throughout the paper, L(user) represents the security level of the user, KCi denotes the key of encryption operation for the user, ti denotes to a single decrypted tuples, ti{TC} denotes the tuple classification, D denotes the decryption operation, E denotes the encryption operation and P denotes the data that user looking for.

3.1 Original Select Operation Model OSOM

Figure 1 shows the steps of a select operation based on multilevel security adapted to a multilevel database [20]. First, the system checks the user's security, then it sets the key of the encryption operation according to user-level security, and finally, the system checks if the user has the right to access the encrypted data stored in the database. The data is accessed as tuples or row by row in the choose operation paradigm, and each row is decrypted one at a time. As a query, the decrypted data is compared to the input data. If the comparison result is true, then the retrieved data is shown as a result of the query; otherwise, the same processes will be repeated until the end of file/table.

3.2 Modified Select Operation Model MSOM

Our proposed modification MSOM is reported in [8]. The inefficient performance of OSOM is due to the invoking decryption process for each tuple and compares the result to the query/ predicate. We avoid it in the proposed modification. We assume that our proposed modification MSOM uses the same steps but it implements the encryption once. Our proposed modification model works as follows: (1) checks the security level of the user with the tuple classification; (2) assign the key of encryption to be used for decryption, this is due to the use of different key for each security class; (3) if t_i[TC] (clearance) of the tuple = the security level of user then an encryption will be invoked and applied for the query (It encrypts the data in the query); (4) applies traditional select; if the query matches with any encrypted tuple in the database, then the target tuple will be decrypted and the result will be displayed. Hence the decryption is called only once (in the case of comparison is true) otherwise the decryption will not be invoked. The MSOM is depicted in Figure 2.

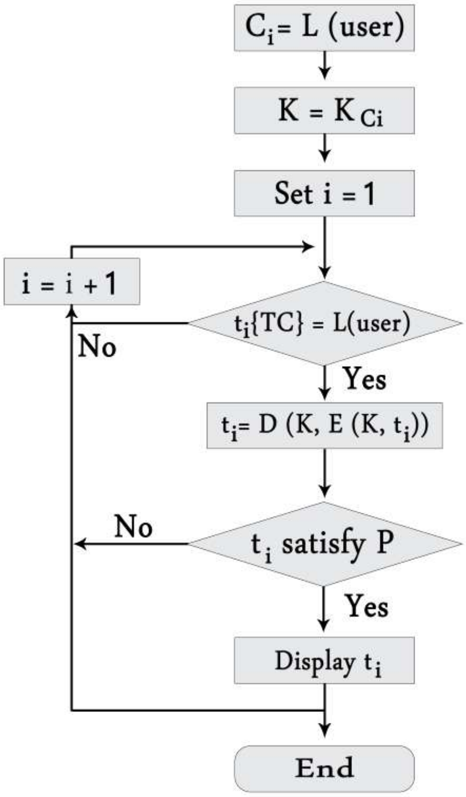

Figure 1: Original Select Operation Model OSOM

3.3 Original Delete Operation Model ODOM

The steps of the original delete operation model ODOM [20] adapted multi level security is illustrated in Figure 3. The deletion and selection processes share the first steps as shown in the figure. The user's security level is checked and the encryption key is determined according to the security level. The user's security level is compared to the security level of the data to be deleted. If the user has the right to delete, this implies that it has the level of security required to access these data, then the system decrypts the stored row by row and compares these data after decryption with the data entered by the user. If the security level of the user is found to be higher than the level required accessing the data, the user identifies the data that the data has to be deleted by another user with the same level of security to delete it as in the former case.

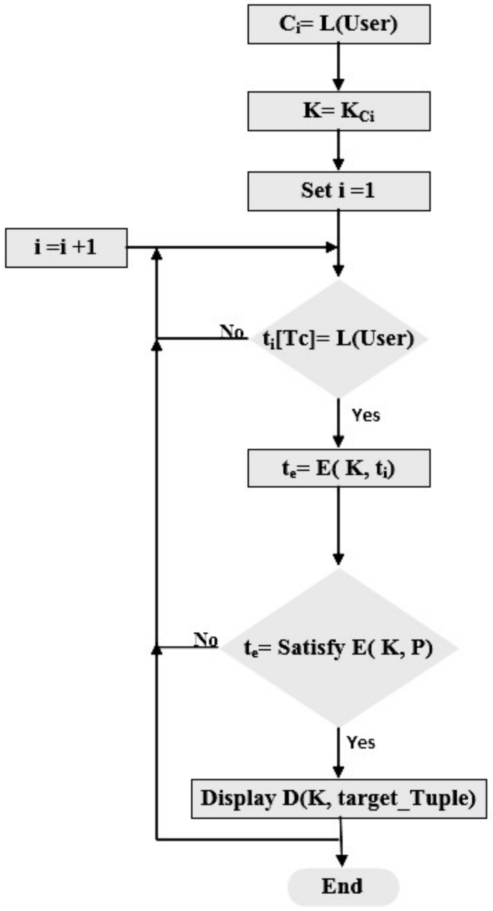

Figure 2: Modified Select Operation Model MSOM

3.4 Modified Delete Operation Model MDOM

The steps of the proposed modification MDOM are illustrated in Figure 4; the inefficiency of ODOM is due to the executing decryption process for each tuple. The decryption is repeated for every tuple and this becomes very time-consuming when it is handling a large size of data. In the modified version of the model MDOM, the repeated decryption was avoided and replaced with single encryption. Thus, this modification improves performance in terms of reducing the time taken to execute the deletion process. The MDOM follows the same steps and the settings as in ODOM except, it replaces the decryption process with the encryption; the encryption process is executed only once.

3.5 Original Update Operation Model OUOM

Figure 5 shows the steps of an update operation based on multilevel security adapted to a multilevel database [20]. As in the models OSOM and ODOM, the system checks the user level to determine the appropriate encryption key and then checks the user's security level to ensure that the user has the right to access the data.

If the user has access to the data, then the stored data is retrieved from the database and decrypted row by row; the decrypted rows are compared to the data entered by the user if the comparison predicate is true, then the model checks the data to be modified, either the target data includes the primary key of the table or not, if it does not include the data being updated and then encrypted to be stored. Otherwise, the model checks the security level of the user, if the security level of the user less than the classification of tuples then the tuple unchanged otherwise the update is performed. It is appropriate to mention that the update is performed within the encryption process.

3.6 Modified Update Operation Model MUOM

Figure 6 described the modified update operation model MUOM, the MUOM follows the same steps as in OUOM, but it differs in the following, it modified the comparison mechanism, instead of executing decryption and then performing the comparison process, the MUOM avoid the decryption for each row and it replaces it with encryption of the predicate P, if the predicate result is true, then the target tuple/ row is decrypted and the update process is performed. The elapsed time of this process is significantly reduced by this change and also when the encryption in the storage process is eliminated if the data are modified. The rest of the steps are the same as in the OUOM.

4. PERFORMANCE OF THE MODIFIED MODELS VERSUS THE ORIGINAL MODELS

We developed an application for simulating the modified models and to evaluate their performance versus the original models. The developed application is in Java and MySQL on HP G5 Intel(R) core i7 8th Gen Personal Computer with 16-GB RAM and Windows 10. We used the AES advanced encryption standard for encryption, the details of AES can be found in [2]. AES has three modes; we used AES128 for confidential security level (C), AES192 for secret security level (TS), and AES256 for top secret security level (S).

The classification of the security level/clearance has been selected based on Bell-Lapadula. Tables 1 and table 2 display the data before and after encryption, respectively. It's worth noting that the encryption is done using the built-in AES for base64encoder.

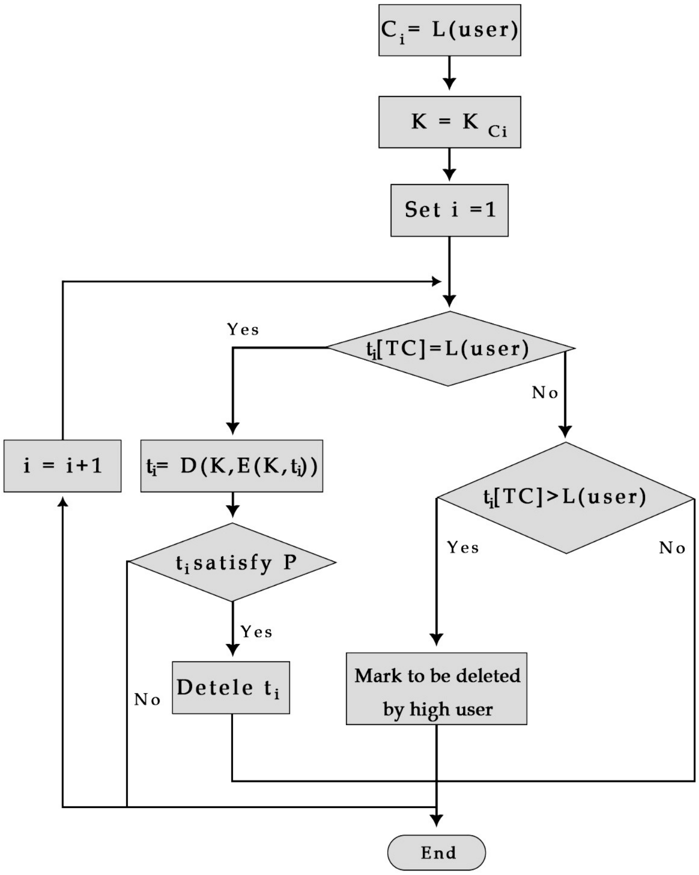

Figure 3: Original Delete Operation Model ODOM

Table 1: Personal Data before Encryption

Personal ID	Name	DOB	Address	TC
998994147	Mohammed Jabber	05/08/1970	DerElbalh	C
985745692	Ahmed Ali	02/03/1989	Khanunes	S
124548733	Ali Mahmoud	04/05/1985	Mghazi	TS
999662231	Amal Kamal	15/01/1998	Gaza city	C
858323141	Sara Abd	22/12/2000	Rafah	S

Table 2: Personal Data after Encryption

Personal ID	Name	DOB	Address	TC
CH7FZEz5bckW	fCiVPBigOZkBFPvPZ7P+	AXLSbU3ibcQWbg==	dSKPGBmvPZFJ	C
CH/IakH4asQT	cC+QOBHtfLxNNw==	AXXSbUbibcQZZw	ei+cMwCjOY4=	S
AHXJaEH1a84S	cCuUfTisNJBOK/4=	AXPSbUDibcQZaw==	fCCVPA+k	TS
CH7Ea0P/bs4Q	cCqcMVWGPZBAMg==	AHLSbUTibcQYZg==	diaHPFWuNYlY	C
CXLFbkf+bckQ	YiaPPFWMPpk=	A3XSbEfibs0Rbg==	YyabPB0=	S

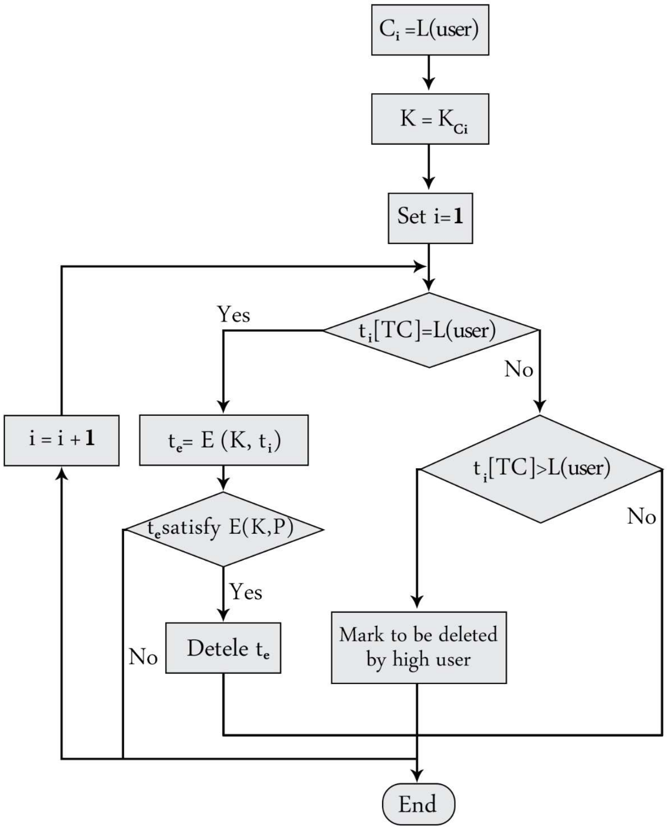

Figure 4: Modified Delete Operation Model MDOM

The proposed models modifications are evaluated according to the performance (elapsed time), we consider different size of data and different number of tuples to conduct the evaluation as shown in the following tables. We build a function to generate fictitious data (sufficient number of tuples for the purpose of our research) to conduct our experiments and to evaluate our proposed modifications.

Table 3 shows that the obtained results of the proposed modification MSOM give better performance and it is more effective than the OSOM in retrieving the target tuple. The obtained results show that the MSOM is significantly better than the original select operation model when the number of tuples and the size of data become large. The obtained results are compatible with the theoretical analysis since OSOM applies decryption for each tuple while MSOM applies encryption and decryption only once. It is worth mentioning that if our target tuple is located at index n, the elapsed time is significantly increased as the number of tuples *n* increased

Table 4 shows that the obtained results of the proposed modification MDOM gives better performance and it is significantly more effective than the original model ODOM. The obtained results of the proposed MDOM significantly better than ODOM when the number of tuples becomes is large, similar to MSOM, if target tuple is located at index n, the elapsed time is significantly increased as the number of tuples *n* increased.

Table 5 shows that, the obtained results of the proposed modification MUOM gives better performance and it is significantly more effective than the original model OUOM. The obtained results of the proposed MUOM significantly better than OUOM when the number of tuples becomes large, this is similar to MSOM and MDOM models, if the target tuple is located at index n, the elapsed time is significantly increased as the number of tuples n increased.

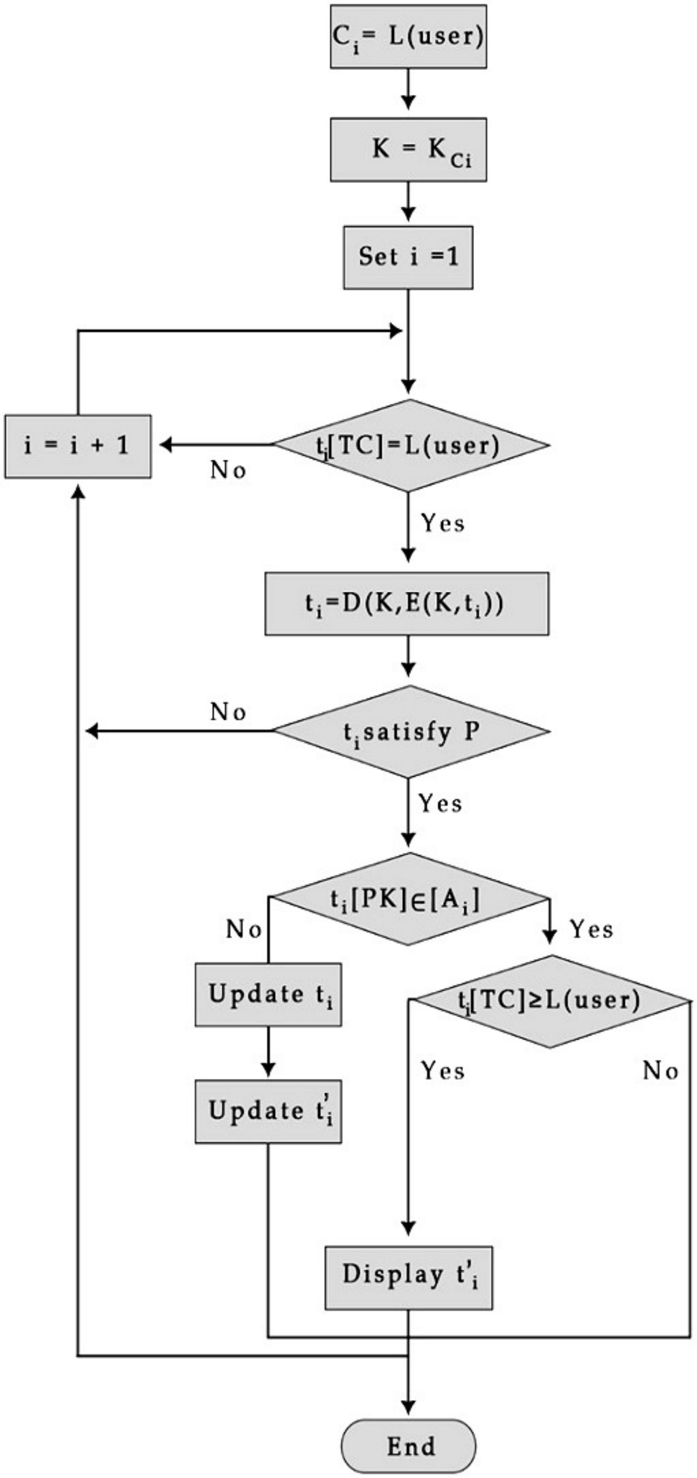

Figure 5: Original Update Operation Model OUOM

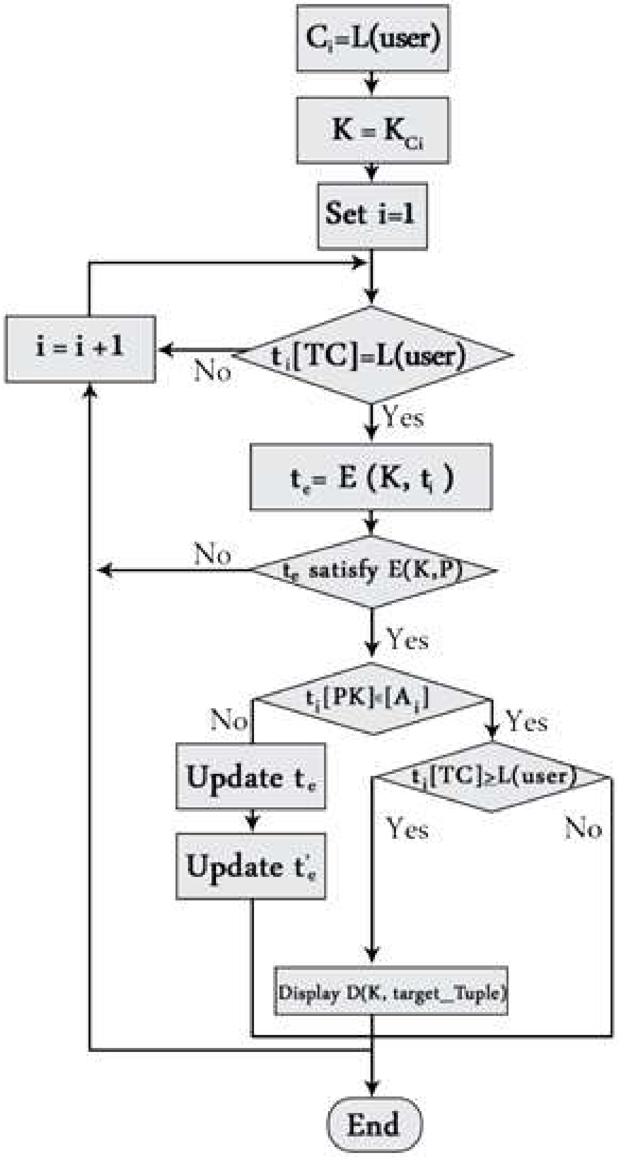

Figure 6: Modified Update Operation Model MUOM

Table 3. Elapsed Time for OSOM and MSOM

# of Rows	Data Size (MB)	OSOM (sec)	MSOM (sec)
10000	3	0.933189	0.019458
50000	7	1.966384	0.035943
100000	13	4.111600	0.066796
200000	26	8.238519	0.215501
400000	50	18.66730	0.283111
800000	98	37.96110	0.670170
1000000	121	42.21637	0.699946

Table 4: Elapsed Time for ODOM and MDOM

# of Rows	Data Size (MB)	ODOM (sec)	MDOM (sec)
10000	3	0.619440	0.012748
50000	7	2.806944	0.041424
100000	13	5.839819	0.103823
200000	26	11.37836	0.193851
400000	50	25.42086	0.283111
800000	98	38.19223	0.670170
1000000	121	50.53036	0.768155

Table 5: Elapsed Time for OUOM and MUOM

# of rows	Data Size (MB)	OUOM (sec)	MUOM (sec)
10000	3	0.536646	0.017206
50000	7	2.655029	0.038547
100000	13	5.534666	0.079681
200000	26	11.19678	0.195612
400000	50	21.56605	0.365219
800000	98	42.79916	0.624820
1000000	121	50.50558	0.803017

5. LIMITATIONS

Due to the lack and the difficulties for obtaining large sized databases. We generated random data to obtain large enough database size to examine the proposed modifications models versus the original models. The obtained results showed that the proposed modifications are more effectively significant than the original models.

6. CONCLUSION

Database systems are the essential part of any organization; increasing the response time and performance of database systems should not affect the security level of databases; the performance of database systems should be enhanced together with the protection of the DBS against any risk and threats. In this paper, proposed modifications of the select, delete, and update operations models for multilevel database security. The proposed modifications gave better and faster performance due to the avoidance of multiple decryptions. In our proposed modifications MSOM, MDOM, and MUOM, the encryption and decryption are called only once. Our proposed modified models show better performance versus to the original models (OSOM, ODOM, and OUOM) and this is very obvious when handling and processing large number of tuple (large sizes of data). The OSOM, ODOM, and OUOM models become significantly inefficient when the number of tuple (size of data) is increased.

REFERENCES:

[1] J. Alves-Foss, P. W. Oman, C. Taylor, and W. S. Harrison, “The MILS architecture for high-assurance embedded systems,” Int. J. Embed. Syst., vol. 2, no. 3–4, pp. 239–247, 2006, doi: 10.1504/ijes.2006.014859.

[2] W. Stallings, Cryptography and Network Security Principles and Practices. 2012.

[3] W. Stallings, Computer Security Princuplew and Practices. 2014.

[4] A. Elçi, A. G. Chefranov, H. Wang, L. Johnston, K. Wolfe, and J. Mull, “Theory and Practice of Cryptography Solutions for Secure Information Systems,” vol. i.

[5] A. G. Mahmoud, A. Y., & Chefranov, “Secure Hill cipher modifications and key exchange protocol,” 2010 IEEE Int. Conf. Autom. Qual. Testing, Robot., vol. 2, pp. 1–6, 2010.

[6] A. Mahmoud and A. Chefranov, “Hill cipher modification based on pseudo-random eigenvalues,” Appl. Math. Inf. Sci., vol. 8, no. 2, pp. 505–516, 2014, doi: 10.12785/amis/080208.

[7] A. Y. Mahmoud and A. G. Chefranov, “Secure Hill Cipher Modification Based on Generalized Permutation Matrix SHC-GPM,” vol. 102, no. 2, pp. 91–102, 2012.

[8] A. Y. Mahmoud and M. M. Abu-Saqer, “Modification of select operation model for multilevel security: Medical database systems as an application,” Proc. - 2020 Int. Conf. Assist. Rehabil. Technol. iCareTech 2020, pp. 47–50, 2020, doi: 10.1109/iCareTech49914.2020.00016.

[9] A. Y. Mahmoud and A. G. Chefranov, “A Hill Cipher Modification Based on Eigenvalues Extension with Dynamic Key Size HCM-EXDKS,” Int. J. Comput. Netw. Inf. Secur., vol. 6, no. 5, pp. 57–65, 2014, doi: 10.5815/ijcnis.2014.05.08.

[10] A. G. Mahmoud, A. Y., & Chefranov, “Hill cipher modification based on eigenvalues hcm-EE,” Proc. 2nd Int. Conf. Secur. Inf. networks, pp. 164–167, 2009.

[11] A. Y. Mahmoud and M. N. A. Alqumboz, “Encryption based on multilevel security for relational database EBMSR,” Proc. - 2019 Int. Conf. Promis. Electron. Technol. ICPET 2019, pp. 130–135, 2019, doi: 10.1109/ICPET.2019.00031.

[12] R. A. Abdelwahed, Ann S.; Mahmoud, Ahmed Y.; Bdair, “Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip.,” Int. J. Inf. Sci. Manag., vol. 15, no. 1, pp. 1–26, 2017.

[13] and V. V. Brakerski, Zvika, “Efficient Fully Homomorphic Encryption from (Standard)

LWE.No Title," SIAM J. Comput., vol. 43, no. 2, pp. 831–871.

[14] T. and N. Lepoint, "A comparison of the homomorphic encryption schemes FV and YASHE," in International Conference on Cryptology in Africa, Springer, Cham, 2014, pp. 318–335.

[15] K. Satyanarayana, "Multilevel Security for Cloud Storage using Encryption Algorithms," nternational J. Eng. Comput. Sci., vol. 5, no. 7, 2016.

[16] N. Kaur, R. Singh, and H. S. Saini, "Design And Analysis Of Secure Scheduler For MLS Distributed Database Systems," 2009 IEEE Int. Adv. Comput. Conf. IACC 2009, no. March, pp. 1400–1404, 2009, doi: 10.1109/IADCC.2009.4809221.

[17] X. D. Zuo, F. M. Liu, and C. Bin Ma, "A new approach to multilevel security based on trusted computing platform," Proc. Sixth Int. Conf. Mach. Learn. Cybern. ICMLC 2007, vol. 4, no. August, pp. 2158–2163, 2007, doi: 10.1109/ICMLC.2007.4370502.

[18] Y. Elovici, R. Waisenberg, E. Shmueli, and E. Gudes, "A structure preserving database encryption scheme," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3178, pp. 28–40, 2004, doi: 10.1007/978-3-540-30073-1_3.

[19] S. R. Masadeh, A. Azzazi, B. A. Y. Alqaralleh, A. Ali, and M. Al Sbou, "A Novel Paradigm in Authentication System Using Swifi Encryption /Decryption Approach," Int. J. Netw. Secur. Its Appl., vol. 6, no. 1, pp. 17–24, 2014, doi: 10.5121/ijnsa.2014.6102.

[20] O. S. Faragallah, E. S. M. El-Rabaie, F. E. Abd El-Samie, A. I. Sallam, and H. S. El-Sayed, Multilevel security for relational databases. 2014. doi: 10.1201/b17719.