Multilevel Security Management for Global Transactions

Hyun-Cheol Jeong
Dept. of Medical Engineering, Kwangju Health College
683-3 Sinchang-dong Kwangsan-gu Kwangju 506-701 Korea
Tel: +82-62-958-7774, Fax: +82-62-953-4946
E-mail: hcjeong@www.kjhc-c.ac.kr

Abstract: The most important issue in database security is correct concurrency control under the restrictive security policy. The goal of secure transaction management is to keep security and provide many concurrent users with the high availability of database. In this paper, we consider the security environment of multidatabase system with replicated data. The read-from relationship in the existed serializability is improper in security environment. So, we define new read-from relationship and propose new secure 1-copy quasi-seriailzability by utilizing this relationship and display some examples. This security environment requires both the existed local autonomy and the security autonomy as newly defined restriction. To solve covert channel problem is the most difficult issue in developing secure scheduling scheme. The proposed secure 1-copy quasi-serializability is very proper for global transactions in that this serializability not violates security autonomy and prevents covert channel between global transactions.
Keywords: *Multidatabase, Global, Secure One-Copy Quasi-Serializability, Local Security Autonomy*

1. Introduction

The consistency and security of data become very important factor in database system. Authorized users only are legally permitted to access very sensitive information. Security policy is essentially supported in database system to maintain data security. Security manager assigns security level to user and data. BLP model[1][2] which is mandatory access control is adopted as the access mechanism of database. This policy assures secure property to prevent data with higher security level from being directly disclosed to users with lower security level. Data is replicated to increase the availability in every site. One-copy serializability(1SR) is utilized as the correctness criteria of replicated data. Before multidatabase systems (MDBS) is constructed, each irrelevant local database may have the same information like an address, occupation, etc. for a person. Namely, It means that a personal data can be replicated in each site. Data replication is desirable in MDBS because search cost is decreased in remote site and data availability is increased in insipte of system fault. W. Du[3] suggested the one-copy quasi-serializability(1QSR) of global transactions(GT) that has weaker constraint than 1SR in multidatabase system with replicated data. Quasi-serializability(QSR)[4] is proper in multidatabase system because the interaction between GTs is handled through scheduling GT and the interaction between GT and local transaction (LT) is separated through controlling information flow among sites. QSR provides high concurrency control without violating local autonomy and not aborts GT because of discords between local execution. In this paper, we newly define the secure one-copy quasi-serializability (S1QSR) and display some examples for S1QSR to effectively manage GT in multilevel MDBS (MLS/MDBS) to be achieved a few research. MLS/MDBS consists of multilevel local database management systems (MLS/ LDBMS) that are heterogeneous and autonomous. In this paper, section 2 describes related works. Section 3 presents MLS/MDBS, a model to process transaction. Section 4 describes new serializability called S1QSR and we present some examples for S1QSR in this section. In section 5, we discuss the S1QSR serializability by comparing with the existing serializabilities. Section 6 describes our conclusions and future work to be achieved.

2. Related Works

Many researches were proposed to manage replicated data without violating local autonomy. W. Du[3] expanded QSR[4] into 1QSR for the purpose of controlling transaction to access replicated data. Local servers are adjusted among them to postpone or ignore subtransactions of which arrivals are early or late. Also, replicated update-transaction executes write operation to secondary copies in every site in order to maintain the consistent value of them. 1QSR easily preserves the serializability of GTs because it does not consider local indirect conflicts. J. Jing[5] utilized propagation lock in the site where is in primary copy to prevent transaction from violating 1SR. But, propagation lock delayed LTs to be submitted to primary copy site. S. Jajodia[6] solved covert channel problem for information to be indirectly disclosed. He replicated every data with lower security level in database with higher security level. So, information flows only from lower security level to higher security level. But, He didn't suggest the secure propagation mechanism for replicated data to have consistent value. M.H. Kang[7] proposed new transaction model for multilevel secure database and some techinques such as pessimistic, semioptimistic, optimistic mechanism. O. Costich[8] defined nested transaction that has partially different security level for some operations and data in multilevel secure database with homogeneous environment. He suggested multilevel one-copy serializability as new correctness concept. I.E. Kang[9] proposed concurrency control algorithm to assure global serializability. He considered local autonomy and security constraints in multilevel secure federated database system. When the partial security order in each site is globally ordered, secure certification algorithm serializes GT in timestamp order and requires every ticket that subtransaction dominates to be read. And, the algorithm preserves global one-copy

serializable history. But, this paper has some strong restrictions. Security level in each site must be globally ordered. Because each transaction manager is in every security level, there is considerable overhead in system construction. BLP[1][2], security policy ,utilizes two properties to prevent direct information flow. First, in simple property, the read operation is possible when transaction security level is equal to or higher than data security level. Second, in *-property, the write operation is possible when the data security level to be updated is higher than the data security level to execute read operation. This property has the dependency between read and write operation for data security level. R. Sandhu[10] restricted *-property to execute write operation when transaction security level is the same as data security level. This restriction prevents the intentional destroy of integrity. In this paper, we define S1QSR and present the some examples for S1QSR in MLS/MDBS that has each security manager in global and local module. Also, we utilize the restricted *-property and simple-property to prevent direct illegal information flow and remove the integrity violation.

3. Transaction Processing Model

A model to process transaction, as shown on figure 1, consists of three major components (i.e. global module, local execution and security management module, and a set of local sites). If GT is submitted, GTM decomposes GT into some subtransactions and decides their global order to execute the physical operation in each site. Next, GTM submits them to LEM and plays a role of coordinator according to atomic commit protocol. But, GTM not recognizes information for LT and can not control LT. GSM manages the security level of GT according to security level evaluation criteria standardized in MLS/MDBS. When primary copy(Pc) is updated, GSM submits ST to LESM to write secondary copy(Sc) in every site.

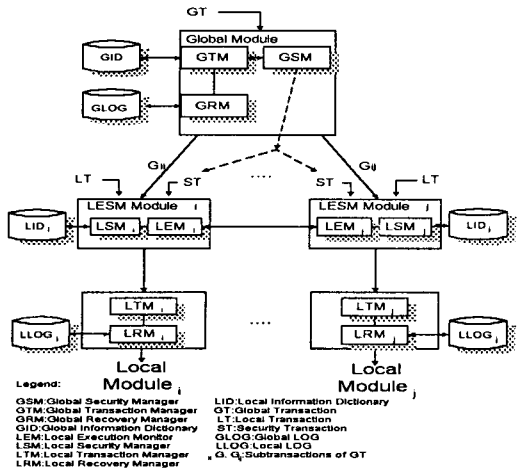

Figure 1. MLS/MDBS Model

The rule for primary copy decision is as follows.

《Rule 1》 Primary Copy Decision

Primary copy is decided as follows according to two steps. Step 1. GSM assigns security level to GT and GTM submits subtransactions of GT to each site. GTM recognizes the composed operations of transaction. Then, finds out the read set and write set of the submitted GT. Step 2. Every data must be carefully updated in order to maintain the consistency and security of replicated data. For each element in write set, primary copy is data with the highest security level among replicated data consisted in every sites. Namely, {each replicated $D \in {}^{\forall}(site)|$highest $SL(D)_{D \in writeset}$}. The transaction with the same as the security level of primary copy executes write operation. ▪

After GSM consults the information window(IW) in GID, GSM decides the site that Pc virtually is in by the Pc decision rule. IW preserves some information that are data item, security level, Pc and Sc for data in every sites, update bit, Before Value(BeV) and After Value(AeV) for a data. ST that GSM submits is particular transaction. This transaction is different from LT because it executes only update for Sc in all sites. We assume that updating Sc is executed after Pc is updated. Each Sc has BeV and AeV when it is updated. ST submitted to each site consists of write operation, Sc site to be updated and security level, and Pc value to write. That is, $W^S(AeV:S_i)$. GSM refers to IW and decides the security level of ST by Security Function (SF).

《Definition 1》 Security Function

SF: {Sc(D) $\in {}^{\forall}$(site)| SL for D satisfying with the restricted *-property}→ ST ▪

SF assigns security level that satisfies the restricted *-property for every Sc to ST. So, ST is able to access each Sc. LEM plays a role of a participant for GT and takes subtransactions for GTM to submit. Next, LEM submits them to LMDBS and returns the result of LMDBS to GTM. A LEM provides information to preserve the serializability of GT whit another LEM via communication. LSM independently assigns security level to LT and local data and maintains local information in LID. LTM handles the concurrent control of transaction submitted to each site.

4. Secure One-Copy Quasi-Serializability

4.1 Introduction

QSR suggested the correctness criteria to handle concurrent control for global transaction in multidatabase system. QSR is apt to assure transaction execution in global order. It is weaker constraint than serializability[11]. GTM controls subtransactions executed in each site. Many LTs executed in another site have no direct precedence relation among them. If local execution E_1: $GT_1 \rightarrow LT_1 \rightarrow GT_2$ and E_2: $GT_2 \rightarrow LT_2 \rightarrow GT_1$, there is no precedence relation between LT_1 and LT_2. GTM controls the serialization of GT_1 and GT_2 in global order. If global order is $GT_1 \rightarrow GT_2$, GT_2 is deferred until next GT_1 like local execution E_2: $LT_2 \rightarrow GT_1 \rightarrow GT_2$. 1QSR suggested the correctness criteria to handle global concurrent control in multidatabase system with replicated data. Each local execution is serializable. If global order is $T_i \rightarrow T_j$, every site executes operation in ${}^{\forall}op_i \rightarrow {}^{\forall}op_j$. Their read-from relationship and final write operation are identical. We present 1QSR for GT in example 1.

《Example 1》 1QSR

$GT_1=\{G_{1i}, G_{1j}\}$; $G_{1i}:w_{g1}(x_i)$, $G_{1j}:w_{g1}(x_j)$, $GT_2=\{G_{2i}, G_{2j}\}$, $G_{2i}:r_{g2}(x_i)w_{g2}(y_i)$, $G_{2j}:w_{g2}(y_j)$
$RT_1=\{RT_{1i}, RT_{1j}\}$; $RT_{1i}:w_{r1}(x_i)$, $RT_{1j}:r_{r1}(y_j)r_{r1}(z_j)$,
$RT_2=\{RT_{2i}, RT_{2j}\}$; $RT_{2i}:w_{r2}(x_i)$, $RT_{2j}:w_{r2}(y_j)$
$LT_1:r_{l1}(x_i)r_{l1}(y_i)$, $LT_2:w_{l2}(z_j)r_{l2}(y_j)$
Then, the executions in every site are as follows.
E_i: $r_{l1}(x_i)w_{g1}(x_j)w_{r1}(x_i)r_{g2}(x_i)w_{g2}(y_i)w_{r2}(y_i)r_{l1}(y_i)$
E_j: $w_{g1}(x_j)w_{r1}(x_j)r_{r1}(z_j)w_{l2}(z_j)r_{l2}(y_j)r_{g2}(x_j)w_{r2}(x_j)$
E_i :$w_{g2}(y_i)w_{r2}(y_i)r_{l1}(x_i)r_{l1}(y_i)w_{g1}(x_j)w_{r1}(x_i)r_{g2}(x_i)$
E_j :$w_{g1}(x_j)w_{r1}(x_j)r_{r1}(z_j)w_{l2}(z_j)r_{l2}(y_j)r_{g2}(x_j)w_{r2}(x_j)$
Then, E_i and E_j are $GT_1 \rightarrow RT_1 \rightarrow GT_2 \rightarrow RT_2$, $GT_1 \rightarrow RT_1 \rightarrow GT_2$, $GT_2 \rightarrow RT_2$ in E'_i,$GT_1 \rightarrow RT_1 \rightarrow GT_2 \rightarrow RT_2$ in E'_j So, E' is 1QSR because it is equivalent to E. Namely, $E=\{E_i, E_j\} \equiv E=\{E'_i, E'_j\}$. ▪

4.2 S1QSR

S1QSR is defined as correctness criteria to handle global concurrent control by introducing two constraints such as security autonomy and covert channel prevention into 1QSR in the security environment of multidatabase systems. Security manager assigns security level to the submitted transaction and data. Each security level classifies according to security evaluation criteria standardized in MLS/MDBS.

《Definition 2》 Security Level

For the transaction set, $T=\{T_1, T_2, ..., T_n\}$, and data set, $D=\{x,y,..., \}$, the security level of transaction is $SL(T) \in \{T, S, C, U\}$, and the security level of data is $SL(D) \in \{T, S, C, U\}$. This symbol, $<_H$ means higher security level between security levels. Namely, $U <_H C <_H S <_H T$. ▪

LSM in each site assigns security level to local data and transaction and maintains correct value by protecting local data from being insecure. Therefore, We consider security autonomous[12] together with the existed local autonomy (i.e. communication, design, and execution autonomy) in MLS/MDBS.

《Definition 3》 Security Autonomy

Each LSM independently assigns security level to transaction and data belonging to self-site. Therefore, He has privileges to protect his database. ▪

Because the read-from relationship of the existed serializability is improper for MLS/MDBS, new secure read-from relationship is requested. This relationship considers both security and read-from relationship.

《Definition 4》 Secure Read-from Relationship

When security level is $B <_H A$, $SL(T_i) \leq_H SL(T_j) = SL(x)$, if there is the relation of $R^A_j[W^B_i(X^B)]$ or $R^B_j[W^B_i(X^B)]$ between two transactions, T_i and T_j, there is secure read-from relationship between them. ▪

To define S1QSR, we consider some relevant matters. First, the transaction to be executed according to global order must satisfy secure read-from relationship in behalf of preventing direct information efflux. Second, when transactions act in collusion to establish covert channel, this indirect information efflux is prevented. Also, we maintained the BeV and AeV for each data and preserved the most recent value. When global order is $T_i \rightarrow T_j$, $SL(T_j) <_H SL(T_i)$, T_i, $T_j \in$ {only GTs}, $w_i(y)r_i(x)w_j(x)$, indirect information efflux is occurred. GSM assigns security level to ST. ST that is transaction with reliable security level is submitted to update secondary copy. Covert channel is not established because there is no conflict between ST and GT. Read operation and write operation have the same security level for $R^B_j[W^B_i(X^B)]$. For global order $T_i \rightarrow T_j$, $SL(T_j) >_H SL(T_i)$, if $T^T_j:w^T_j(y^T)r^T_j(x^S)$, $T^S_i:w^S_i(x^S)$ and E_i: $\underline{w^S_i(x^S)}w^T_j(y^T)$ $\underline{r^T_j(x^S)}$, there is no covert channel because T_i with lower security level is preceded according to global order. Namely, It is a reason that the high and the low security level for two transactions not violate global execution. But, if $SL(T_j) <_H SL(T_i)$, $T^T_i:w^T_i(y^T)r^T_i(x^S)$, T^S_j: $w^S_j(x^S)$, E_2: $w^T_i(y^T)$ $\underline{r^T_i(x^S)}$ $\underline{w^S_j(x^S)}$, there is covert channel because they are executed according to global order and violate security level. According to global order $T_i \rightarrow T_j$, covert channel is established for x. The conditions for secure one-copy quasi-serial execution are as follows.

《Definition 5》 Secure One-Copy Quasi Serial Execution

If a set of transactions $\{E_1,E_2,...,E_n\}$ satisfies the following conditions, it is S1QSE.

1. Each site execution, E_i, is serializable without direct or indirect information efflux.
2. If T_i precedes T_j, all operations of T_i is executed prior to the operations of T_j through the global order of transaction for T_i,T_j $\{(GT) \cup (ST)\}$, if T_i is last transaction to update data and secure read-from relationship, T_j read AeV. If there is the secure read-from relationship with covert channel, T_i precedes T_j in the order and T_j reads BeV. ▪

The first two conditions of secure one-copy quasi-serial executions are the same as those of 1QSR. ST executes write operation to update copies in every local site. The global order between ST and GT must be assured to maintain data consistency. The last condition means that the last write operation and secure read-from relationship is equivalent to last execution without indirect information efflux, called covert channel.

《Example 2》 S1QSE

The security level of transacion is assigned as follows. $SL(GT_1)=T$, $SL(GT_2)=S$, $SL(LT_1)=T$, $SL(LT_2)=S$; $SL(x_i)=S$, $SL(x_j)=S$, $SL(y_i)=C$, $SL(y_j)=T$, $SL(z_i)=T$, $SL(z_j)=S$, $SL(k_i)=S$, $SL(k_j)=U$. Primary copies are z, k in $site_i$, x, y in $site_j$. Then, global transactions and local transactions are submitted as follows.

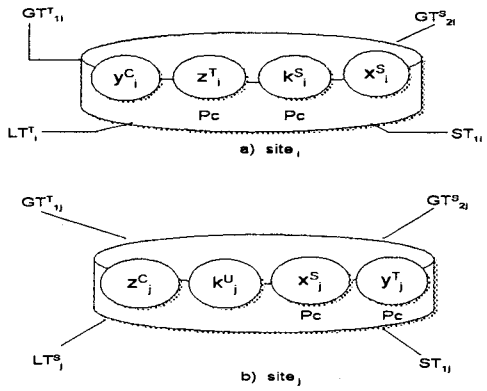

Figure 2. S1QSE

$GT_1=\{G_{1i}:w_{g1}(z_i)r_{g1}(y_i)r_{g1}(k_i), G_{1j}:r_{g1}(z_j)w_{g1}(y_j)r_{g1}(x_j)\}$,
$GT_2=\{G_{2i}:r_{g2}(x_i)w_{g2}(k_i), G_{2j}:w_{g2}(x_j)r_{g2}(k_j)\}$,

$ST_1=\{S_{1i}:w_{s1}(x_i)w_{s1}(y_i), S_{1j}:w_{s1}(z_j)w_{s1}(k_j)\}$,
$LT_i:w_{l1}(z_i)r_{l1}(y_i)$, $LT_j: r_{l1}(x_j)r_{l1}(k_j)$
The executions in each site are as follows.
$E_i:w^T_{gl}(z^T_i)w^T_{li}(z^T_i)w_{sl}(x_i)r^T_{gl}(y^C_i)r^T_{gl}(k^S_i)r^T_{li}(y^C_i)w_{sl}(y_i)r^S_{g2}(x^S_i)w^S_{g2}(k^S_i)$
$E_j:r^T_{gl}(z^C_j)w^T_{gl}(y^T_j)r^T_{gl}(x^S_{j/BeV})r^T_{lj}(x^S_j)w_{sl}(z_j)w_{sl}(k_j)r^T_{lj}(k^U_j)w^S_{g2}(x^S_j)r^S_{g2}(k^U_j)$
For primary copy, updating data by ST_{1l} and ST_{1j} creates new value in each site.

Therefore, secondary copies have BeV and AeV. If the underlined part of E_j is $w^T_{gl}(y^T_j)r^T_{gl}(x^S_j)$ .... $w^S_{g2}(x^S_j)$, covert channel between $GT_1$and GT_2 is established. To avoid covert channel GT_1 reads $x^S_{j/BeV}$.E is S1QSE since $GT_1 \rightarrow ST_1 \rightarrow GT_2$, $GT_1 \rightarrow GT_2$ in E_i and E_j. ▪

《Definition 6》 Secure One-Copy Quasi-Serializability
A global execution of a set of transactions is secure one-copy quasi-serializability if it is equivalent to a secure one-copy quasi-serial execution of the same set of transaction. ▪

《Example 3》 S1QSR
For the same situation in example 1, let $E'=\{E'_i,E'_j\}$.
Where,
$E'_i:r^T_{gl}(k^S_i)w^T_{li}(z^T_i)w^S_{g2}(k^S_i)w^T_{gl}(z^T_i)r^T_{li}(y^C_i)w_{sl}(x_i)$
$r^T_{gl}(y^C_i)w_{sl}(y_i)r^S_{g2}(x^S_i)$
$E'_j:r^T_{gl}(z^C_j)w_{sl}(z_j)w^T_{gl}(y^T_j)r^T_{gl}(x^S_{j/BeV})w^S_{g2}(x^S_j)w_{sl}(k_j)r^T_{lj}(x^S_j)$
$r^T_{lj}(k^U_j)r^S_{g2}(k^U_j)$
$GT_1 \rightarrow GT_2$, $GT_1 \rightarrow ST_1$, $ST_1 \rightarrow GT_2$ in E'_i, $GT_1 \rightarrow ST_1$, $GT_1 \rightarrow GT_2$, $ST_1 \rightarrow GT_2$ in E'_j. Therefore, E'is S1QSR because it is equivalent to E of example 2. ▪

5. Discussions

The ML-1SR introduced security policies into the existed one-copy serializability in homogeneous database system with replicated data. ML-1SR prevents covert channel without security manager by preserving that databases with higher security level have all database with lower security level in system model. So, The higher security level database is, the more memory is required. Also, the operations of transaction are strongly dependent among them since one transaction has many nested transactions.

The newly proposed S1QSR is the serializability for global transactions in multidatabase systems with replicated data. S1QSR introduces security policy into one-copy quasi-serializability.

This system model consists of three levels. Security manager is in global, local module and preserves security autonomy and prevents covert channel. So, S1QSR is different from ML-1SR. Memory problem in S1QSR is trivial. But, there are overheads for security manager. Also, transaction commit is faster than ML-1SR since transaction is not nested. The 1SR in multidatabase system without replicated data solved indirect conflict problem between local transactions by using ticket method and assured serializability. S1QSR has no problem for indirect conflict because this considers global order. 1SR has transaction manager in each security level. This is considerable overhead. Also, 1SR has strong constraint that security level is globally ordered to simplify the problem of conflict and local autonomy with security requirement. But, S1QSR mitigates the strong constraints of 1SR. Also, S1QSR not violates security autonomy and is able to prevent covert channel.

6. Conclusions

Recently, information security becomes very hot issues. But a lot of situations become exposed. In every field, database system is essential and widely applicated. So, we must strongly recognize the importance of security. This paper defines secure one-copy quasi-serializ-ability and presents the examples for this serializability in the security environment of multidatabase systems with replicated data. Each site keeps security autonomy by security manager and prevents both direct information efflux and covert channel establishment and assures serializability. Therefore, replicated data in every site has secure, consistent and correct value. In the future work, we will be developing and proving the algorithms for assuring S1QSR. Also, the secure recovery mechanism will be researching.

References

[1] C. P. Pfleeger, *Security in Computing*, Prentice Hall, pp. 249-250, 1989.

[2] S. Castano, *DatabaseSecurity*, Addison-Wesley, pp.82 -96, 1994.

[3] W. Du, et al, "Supporting Consistent Updates in Replicated Multidatabase Systems", VLDB,Journal#2, pp.215 -241, 1993.

[4] W. Du, A. Elmagarmid, "Maintaining Quasi Serializability in Multidatabase Systems", Proceedings, 7th International Conference on Data Engineering, pp. 360-367, 1991.

[5] J. Jing, W. Du, A.Elmagarmid, O. Bukhres, Maintaining Consistency of Replicated Data in Multidatabase Systems", IEEE, pp.552-559, 1994.

[6] S. Jajodia, B. Kogan, "Transaction Processing in Multilevel Secure Databases Using Replicated Architecture" , Proceedings, Symposium on Security and Privacy, pp. 360-368, 1990.

[7] M. H.Kang, O. Costich, and J. N. Froscher, "A Practical Transaction Model and Untrusted Transaction Manager for a Multilevel-Secure Database System" Database Security VI: Status and Prospects (A-21), B. M. Thuraising ham and C. E. Landwehr (Editors), Elsevier Science Publishers B.V.(North-Holland) IFIP, pp.285-300,1993.

[8] O. Costich,"Transaction Processing Using an Untrusted Scheduler in a Multilevel Database with Replicated Architecture ", Database Security V: Status and Prospects, C.E.Landwehr and S.Jajodia(Editors), Elsevier Science Publishers B.V.(North-Holland) IFIP, pp. 173-189,1992.

[9] I. E. Kang,T. F. Keefe,"Concurrency Control for Federated Multilevel Secure Database Systems", 8th IEEE Computer Security Foundations Workshop, pp.118-135, 1995.

[10] R. Sandhu,"Lattice-Based Access Control Models", IE EE Computer, pp.9-19, 1993.

[11] Bernstein, *Concurrency Control & Recovery in Database Systems*, Addison-Wesley, 1987.

[12] H. C. Jeong and B. H. Hwang, "Managing of Replicated Data in MLS/DMDBS",Proceedings, KIPS Spring Conference, Korea Information Processing Society, pp. 203-206, 1995.