Improving Fraud Control in Small Banks using Dynamic Object-based Separation of Duties

Ephrem Kwaku Kwaa-Aidoo
University of Education, Winneba
P. O. Box 25
Winneba

ABSTRACT

Conflicts arise when the execution of two or more tasks by a person creates a vulnerability which when exploited could threaten a business and its goals. These threats could lead to a severe loss of corporate resources and in some cases result in the collapse of businesses. This paper discusses the issue of implementing separation of duty within an information system to deal with conflicting tasks. It examined the issue of separation of duty within small banks and their efforts to prevent fraud. The paper argues that separation of duty in these organisations is not effective and can be compounded by the use of mechanisms like job rotation. It focuses on object-based separation of duty and its possible use in small firms. It proposes the introduction of elements of the Chinese wall security policy and its derivatives to introduce granularity into the implementation of object-based separation of duty.

General Terms

Inforamtion Security, banking fraud,

Keywords

Separation of Duty, Chinese Wall Security Policy, Small Banks

1. INTRODUCTION

The principle of separation of duty involves the practice of dividing and allocating different tasks in a business process to different individuals to prevent a single individual from misusing the process [1, 2]. Perhaps the most basic separation of duty rule is that any person permitted to create or certify a transaction may not be permitted to execute it. This rule ensures that a minimum of two people is required to perform a transaction. The rationale for separating duties is to discourage fraud by distributing the responsibility and authority for a task over several people. It raises the risk of being caught by introducing the mandatory involvement of more than one individual in a fraud [3, 4].

The basis for dividing a business process into tasks to implement a separation of duty policy is the existence of a conflict [5]. Conflicts are said to arise when the execution of two tasks by a person creates a vulnerability which when exploited, could threaten the business and its goals or lead to the loss of some resources. In defining separation of duties the focus has always been on the user, the role or the permission with one factor being the focus at any one time. Subsequently one traditionally has a situation with conflicting users, conflicting roles or conflicting permission.

The objective of the study was to obtain a better understanding of the nature of fraud controls in small banks particularly as it is manifested in rural banking, assess the effectiveness and recommend ways in which it can be improved. This was done by analysing the current controls used in these banks, identifying the weaknesses in these controls with the framework of known information security models. These objectives led to the following research questions.

i. What fraud prevention mechanisms are used by Rural and Community Banks in Ghana?
ii. Are the fraud prevention mechanisms adequate?
iii. In what way can the Chinese Wall Security Policy be used to improve fraud prevention?

The Clark – Wilson model identifies two important mechanisms that are at the heart of control of fraud in commercial organisations. These are a well-formed transaction and separation of duty [6]. It has conventionally been classified into two; strong exclusion or static separation of duty and weak exclusion or dynamic separation of duty [3]. The distinction between the two is dependent on the time of its implementation. Implementation during the design/administration time known as static separation of duty whilst implementation during runtime which is known as dynamic separation of duty [7, 8]. Static separation of duty permanently prevents users from performing any tasks that are conflicting to tasks within his permission and does not change given under any circumstances. Dynamic separation of duty, on the other hand, prevents the exercise of permission when certain conditions exist. Therefore based on the context in which a transaction is being processed a user can be prevented from executing a task. Dynamic separation of duties has been further classified into simple dynamic, object-based, operational, history-based, order dependent and order-independent dynamic separation of duty [3].

Perhaps the most important benefit of implementing dynamic separation of duty is to prevent the execution of validly assigned roles and permissions within the same transaction if there is a conflict in any of these roles or permission. In other words, though permissions have been validly assigned, a subject cannot exercise these rights together in one transaction if they are seen to be conflicting.

2. CONCEPTUAL FRAMEWORK

2.1 Dynamic Separation of Duty and Fraud Control

As mentioned earlier, a key characteristic of dynamic separation of duty is that it focuses on the various tasks within an instance of a business process. The problem with this characteristic is that it is unable to deal effectively with the risk of subjects exercising validly assigned roles or permissions in different transactions at different times to perpetrate fraud. These risks could be exploited in situations where job rotation, for example, is practised.

Object-based separation of duties is a dynamic separation of duty policy that deals with conflicts relating to a specific data item. Under this policy, users are allowed to perform the task in question on a data item if they have not executed any other transaction upon that data item [9-11]. In the context of a bank, it could apply to a transaction voucher or cheque where the voucher is seen as the object. For example, when a clerk issues a bank cheque to a customer, the same clerk cannot process that cheque when it is presented to the bank for withdrawal. There are however objects that cannot be dealt with using this type of policy. For example, it cannot deal with situations where customer accounts are the object. The problem is that unlike cheques which are processed once, customer accounts are reusable therefore if this rule is enforced, users can only perform one transaction on an account. The implication would be that there would come a point when some accounts cannot be operated on by all the banking staff for the reason of having performed a transaction on the account.

2.2 Brewer-Nash Model (Chinese wall Security policy)

The Brewer-Nash policy is a multilateral security policy that deals with the disclosure of information hence focus on confidentiality. The Chinese wall security policy (CWSP) is a mandatory access control policy. It, has a voluntary element where users can choose which information they would like to see implicitly denying themselves the right to information from conflicting classes. It was a specific design with the financial industry in mind.

Implementation of object separation of duties could, however, be modified to take into consideration the level of conflict created due to the transaction history of a user on that account. The introduction of elements of the modified Chinese Wall Security Policy is a very practical means to determining the level of conflict between a current transaction that a user wants to perform and the transaction history of the user concerning that customer account [12].

The modification of the CWSP is to prevent users from exercising different legitimately assigned permissions in different processes on the same object to commit fraud. Such permissions could be in mutually exclusive roles in separate transactions at different times. Hence it would not normally be picked up in static or dynamic separation of duties. Elements of variations of the CWSP could be introduced to modify object-based separation of duties to deal with the above problem.

In exercising the voluntary elements of the CWSP, users can choose which information they would like to see implicitly denying themselves the right to information from conflicting classes. This was specifically designed with the finance industry in mind. Financial institutions providing corporate business services to other organisations can have insider knowledge of its rivals making and the disclosure of such information highly unethical and potentially leading to legal action. When an analyst in the firm has information on a client they must be denied information of rival firms to prevent unauthorised disclosure. In other words, such an analyst must uphold the confidentiality of information provided to him by his firm's clients and not advise organisations where he has insider knowledge of the plans, status or standing of a competitor. The policy operates at three levels.

1. At the lowest level, individual objects containing specific data items with each concerning a specific company are considered.
2. At the intermediate level, all objects concerning the same company are grouped. These are referred to as 'company data sets'.
3. At the highest level all company data sets whose corporations compete or in conflict, are grouped. They are referred to as conflict of interest classes [13].

The main rule in the CWSP is that once a subject has accessed an object the only other objects accessible by that subject can come from the same company dataset or a different conflict of interest class [14, 15]. In other words, an analyst can get information about any company but once that is done, the analyst is not allowed to get information about any other company in the same conflict of interest class. This means that a subject can at most have access to one company dataset in each conflict of interest class and any information that an analyst can get from a system depends on what they have accessed in the past.

The problem with this model is that it assumes that conflict of interest is static. This is not so especially when the interest of companies constantly change and may have different types and levels of interest in other companies. Conflict of interest(CIF) classes can therefore overlap, and the assertion of having a completely disjoint conflict of interest classes is challenged in the variant known as the Aggressive Chinese Wall Security Model (ACWSP) [16]. In the CWSP conflict of interest are mutually disjoint sets however the ACWSP conflict of interest classes can overlap. The scenario used was that if an airline company A has an interest in company B and a petroleum company C also has an interest in company B. In such a case company A and C could be considered as being in the same CIF. In the CWSP such a conflict cannot exist were CIF classes are disjoint and this is one problem the ACWSP resolved.

The access control model for data mining environments, a model based on the Chinese wall policy, draws from the aggressive Chinese wall security policy and makes use of overlaps in conflicts of interest data classes to ensure data integrity. It,, identifies two other problems that were thought to be outstanding [12]. The first is that the severity of the conflict between two companies should be definable. This is because the level of conflict may be such that it is negligible and may not affect access to information. The other issue was that the security policy model should be dynamic. That is to say, situations change and if a company acquires an interest in another company it might come into conflict with other companies that it previously was not in conflict with. If a company ceases having an interest in a company that it previously had an interest in, it also ceases to conflict with companies that it conflicted with.

Loock and Eloff [12] propose two mechanisms for dealing with these problems. The first is to define a conflict of interest sphere around a company and this is defined by a radius (**r**). The second is to define the severity of conflict between two companies which is defined as the distance. On one hand, when the radius is higher, the more interests a company has and potentially more companies it could conflict with. On the other hand the higher the distance between two companies the lower the conflict between them.

3. METHODOLOGY

The study was exploratory and adopted a qualitative approach to enable a deeper understanding of the issues. This was the area of rural banking security has not been researched thoroughly in the past.

The methodology used is described in chart below.

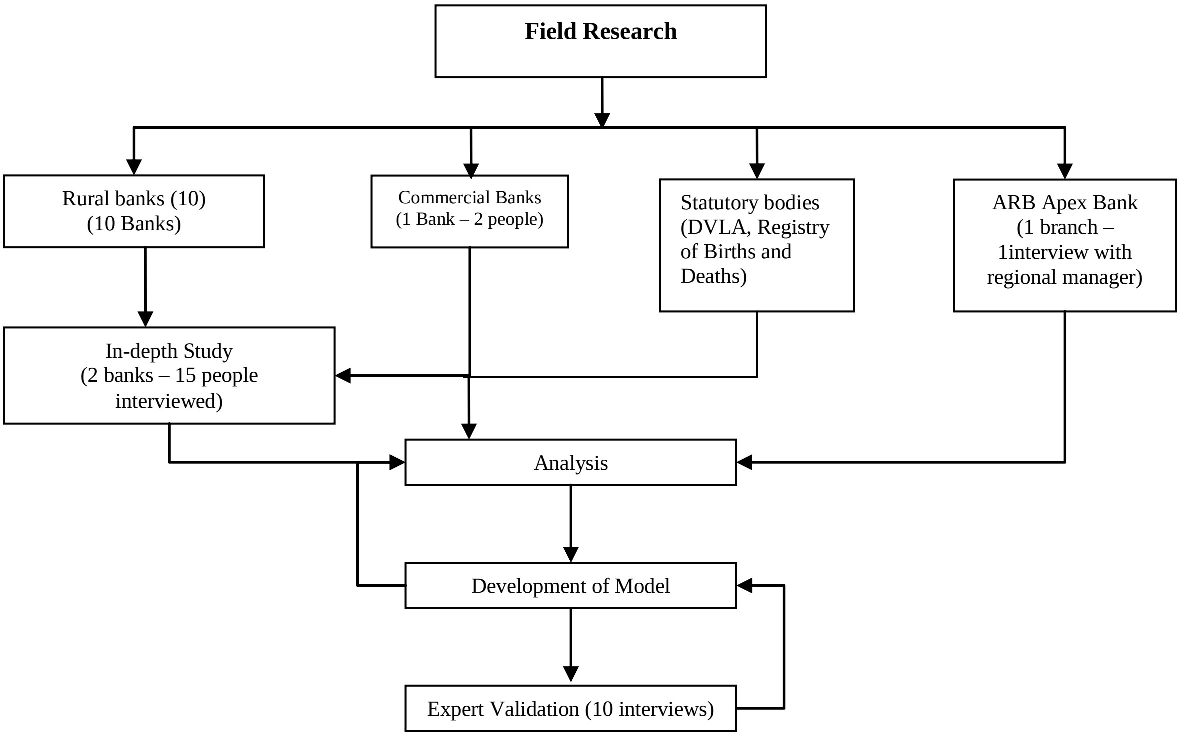
Field Research
Rural banks (10)
(10 Banks)
Commercial Banks
(1 Bank – 2 people)
Statutory bodies
(DVLA, Registry of Births and Deaths)
ARB Apex Bank
(1 branch – 1interview with regional manager)
In-depth Study
(2 banks – 15 people interviewed)
Analysis
Development of Model
Expert Validation (10 interviews)

Fig 1: Methodology

3.1 Sampling

The rural banks studied were drawn from the coastal and middle belt due to their expected homogeneity as a result of their historical and cultural similarities. This homogeneity was further confirmed from the consistency of the data collected. Table 5.2 shows the distribution of rural banks in the various regions studied compared to other regions.

Table 1: Distribution of Rural Banks

Region	Total No of Rural Banks	Percentage (%)
Southern and middle belt	104	80.6
Northern Ghana	14	10.9
Volta	11	8.5
Total	**129**	**100**

This region has a total of 104 rural banks making a total of 401 agencies. In total ten rural banks were randomly selected and surveyed. Two out of the ten rural banks were studied in more detail by observation and further interviews. One branch of the ARB Apex Bank and one commercial bank were studied.

A sample of 10 rural banks was selected representing 10% of the banks in those regions. The selected sample had a total of 50 agencies. Table 1 shows the sample banks that were included in the study and their respective regions.

Table 2: Sample Sizes from Regions

Region	Sample Size
Western	2
Central	2
Eastern	1
Greater Accra	2
Brong Ahafo	1

Ashanti	2
Total	**10**

3.2 Data Collection and Analysis

Bankers are highly reluctant to inform the public about fraud and information security incidents within their organizations hence the assurance of anonymity was crucial to ensure the success of the data collection process.

The data collection process involved administration of a structured questionnaire to 10 Rural Banks and an in-depth study of 2 out the 10 Banks. The in-depth study involved a two (2) week observation of each bank and further interviews of staff of the banks.

To validate the data collected, an interview with a regional manager of the ARB Apex Bank was conducted. Also, two (2) members of staff of commercial banks were interviewed.

4. RESULTS

4.1 Fraud Control Mechanisms in Rural/Community Banks

Among the Banks surveyed for this study, separation of duty was not widely used. It was impossible to implement such mechanisms due to small staff numbers. The most used mechanisms included job rotation, authorisations, post-transaction auditing vaults. This is indicated in the chart below;

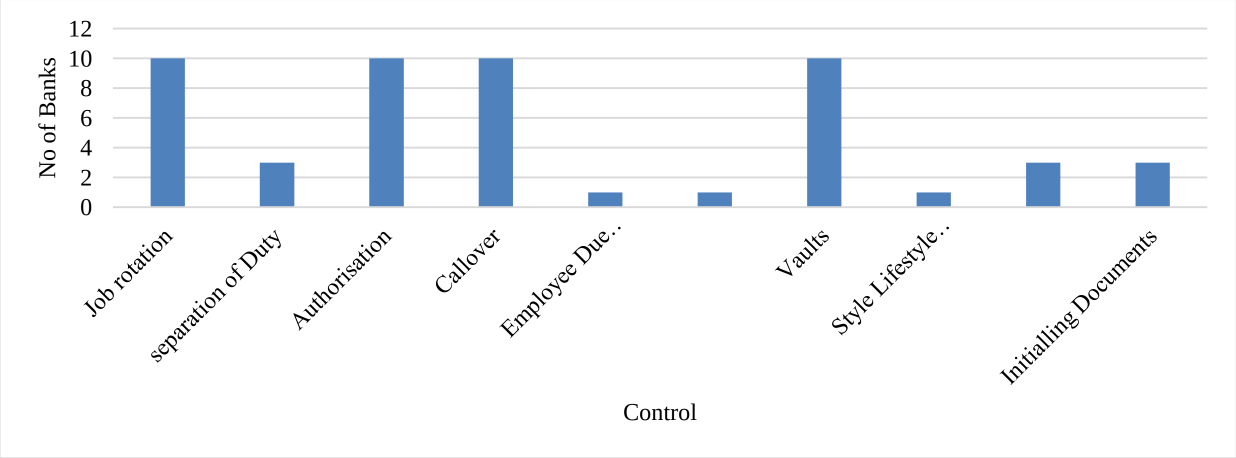

Fig 2: Internal Control Measures Used by Rural Banks

4.2 Services offered by the banks

The banks surveyed offered a total of 14 different services as shown in Fig 3 some of the services were offered by all the banks whilst others were offered by very few of them.

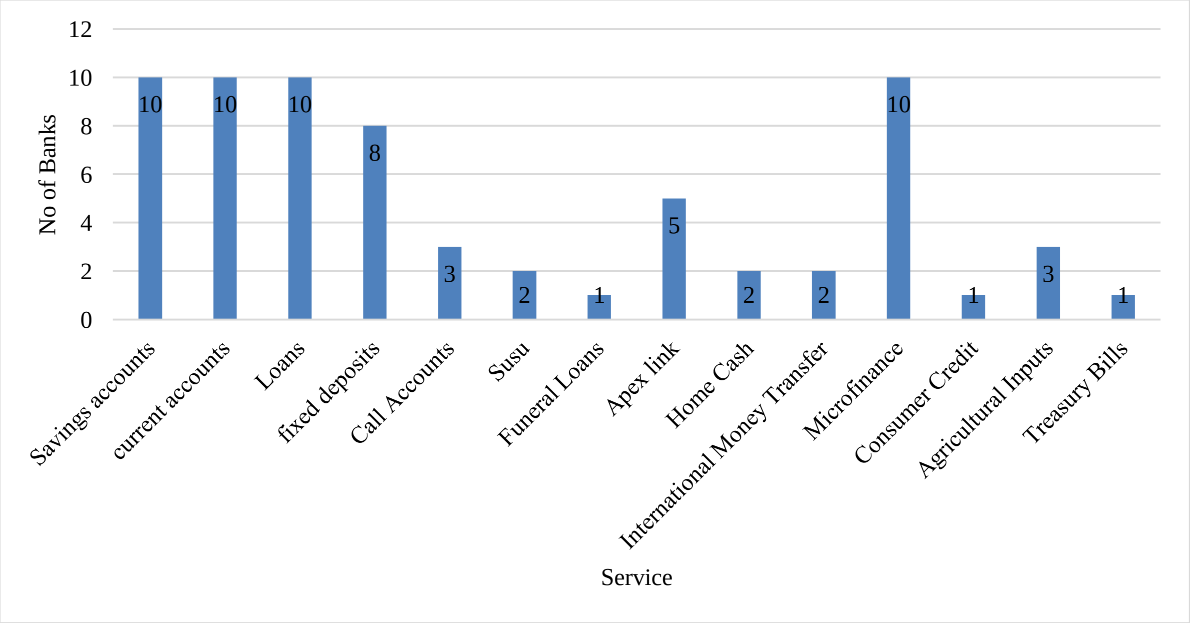

Fig 3: Services Offered by Banks

4.3 Rural Bank Agencies and Staff Strength

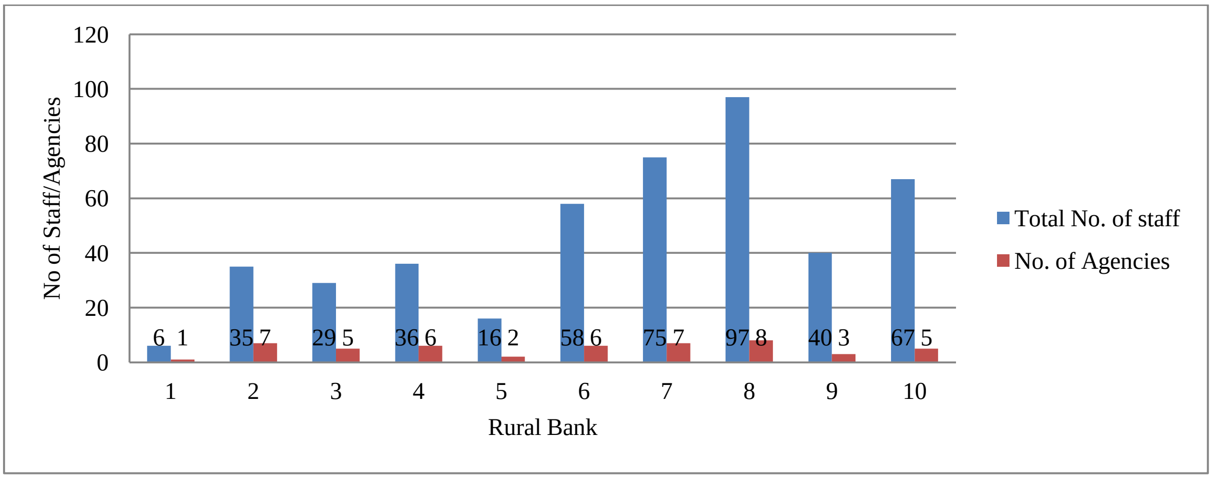

Fig 4: Total No of Staff and the No of Agencies of Rural Banks

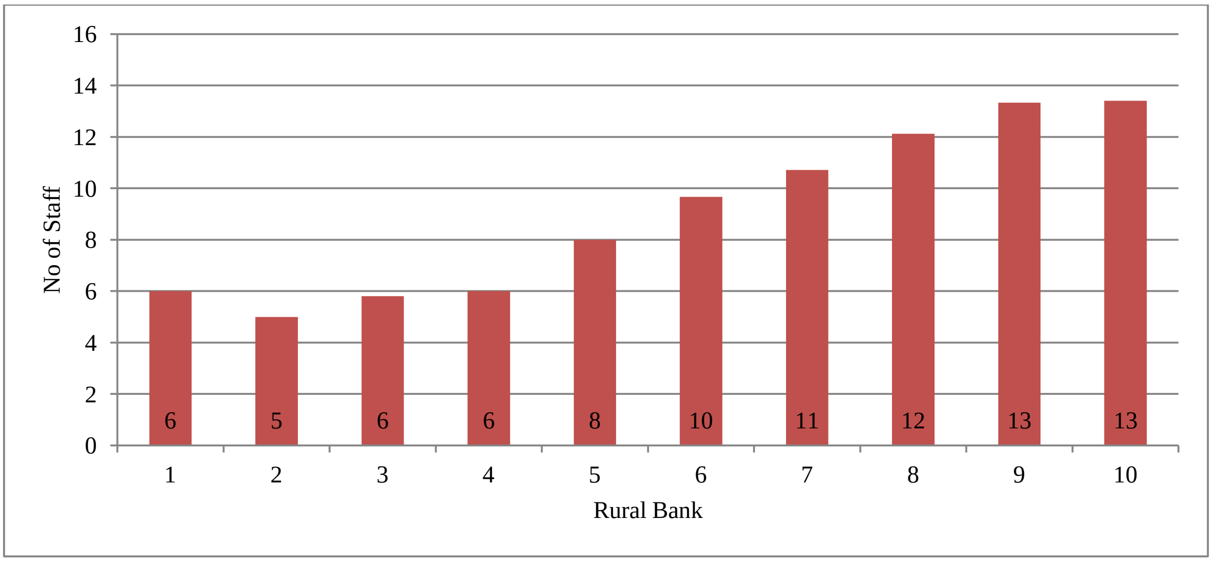

Fig 5: Average staff per agency

5. DISCUSSION

From Figure 1 one of the most used internal control mechanism is Job rotation. This mechanism involves employees being assigned different roles on a rotational basis for a specified period. Job rotation is known to help organisations improve on security. Aside from providing knowledge redundancy, it reduces the risk of fraud, data modification, sabotage, theft and misuse of information [17]. Job rotation also provides the opportunity for peer auditing and enables employees to detect fraudulent activities of their peers.

These advantages notwithstanding, it could also present clear risks. The view is that when a person stays longer in a position the more likely they are to be assigned more responsibility and gain more privileges and access. They are also more likely to become more familiar with tasks and gain the ability to abuse privileges and commit fraudulent or malicious activities.

These banks, as shown in figures 3 and 4, have small staff sizes and our study indicated an average staff strength of 9 including security and other non-banking personnel. With these small numbers and the numerous services as shown in Figure 2, it is unlikely that separation of duty can be effective. There is a risk that employees could get the opportunity to perform two unrelated but conflicting tasks that could create an opportunity for fraud. For example, employees that knew what job they would be doing next could perform certain preparatory activities in their current job and perform other activities in their next job to complete a fraud. This risk is further compounded because the banks explained that they had a system of deputising where employees can anticipate that they would be filling in for absent colleagues.

There are known cases in the literature where employees have used their legitimately assigned permissions in one role and also exercised other permissions legitimately in other roles with these transactions working together to enable fraud[18-20].

6. USING THE CHINESE-WALL SECURITY POLICY TO IMPROVE SOD

The CWSP and its derivative models, therefore, looks at the historic activity of a user and assigns the users rights to other data objects. Applied to transactions, a user's historic activity on a system could be used as a means of preventing fraudsters from executing two unrelated transactions to enable fraud. The introduction of concepts like the sphere of conflict and the extent of the conflict could be used to determine the extent to which transactions performed by employees in the past conflict with current transactions.

In object-based separation of duties employees (subjects) is unauthorised to perform transactions on accounts (objects) that are in a state which might conflict with the current transaction. To achieve this, there is the need to use the access control triple namely the data object in question, the type of transaction and subject performing the transaction.

In this scenario, the conflict would be between the history of access control triple with regards to that particular object (customer account) and the access control triples of the current transaction with regards to the same object. The principle of putting together the history of transactions to determine level risk makes use of the principle of aggregation where adversaries put bits of information together to get the bigger picture. Here the attacker puts transactions together to commit fraud rather than putting data objects together.

A state of an access control triple for an object which puts it at higher conflict with a current transaction would imply that it is easier for the employee to commit fraud if the current transaction were to go on. Thus the level of conflict indicates the level of risk the current transaction poses. If the risk of a current transaction is higher, the level of security requirements for the transaction to proceed should be increased or set to a higher level and would require a higher level of authorisation or scrutiny.

In other words, a series of transactions by a subject on an object should determine whether the subject can have further access of a particular type in the future. The issue would not depend solely on who you are but also on what you have done to determine whether one has the opportunity to commit fraud.

For a subject S_1 who has performed transactions $T_{(1......n)}$ on an object O_1, if S_1 wants to perform a transaction T_c, the conflict C will be between the

$C= f\,[S_1O_1T_{(1.....n)}] – f\,[S_1O_1T_c]$

$C= f\,[S_1O_1(T_{(1.....n)} –T_c)]$

The level of conflict with respect to a specific object and subject will depend on the historical transactions of the subject on the object and the current transaction.

The tranquillity principle is used in dealing with object-based separation of duties. It is however not to be applied in terms of upgrading or downgrading the security level of the object that has been accessed by a subject. Rather it is to be used to upgrade or downgrade the level of conflict between a history of a user and a current transaction. When an employee performs a transaction that conflicts with another transaction, the security requirement to perform the second transaction is increased. Object-based separation of duty is to help deal with any opportunity that could arise to commit fraud.

7. DISTANCE AND CONFLICTING TRANSACTIONS

Distance as used in the new access control model for data mining environments to measure the severity of the conflict. This principle is used to deal with overestimation of conflict. The problem with object-based separation of duties is that employees could easily be prevented from performing any transactions with time because they would have performed every transaction on an account. In the rural banking setting where staff sizes are small, the implementation of traditional object-based separation of duties policies could be a serious problem where the transaction history of bank staff can progressively put each member of staff in a position where every transaction conflicts with the current transaction.

In the proposed model, conflict is determined by the historical transactions of a subject on an object and the current transaction the subject requires performing. So given the historical transaction $T_{1...n}$ and current transaction T_c, the conflict rating which determines the level of risk will be the function of the two will be;

$C = f(T_{1...n,}\ T_c)$

Where

C = Level of Conflict

$T_{1...n}$ = Transaction history of Subject on Object

And *T_c=Current transaction c*

Also, aside a subject's transactions there would have been other intervening transactions by other subjects which may reduce the risk. An example is if an employee opened an account and subsequent transactions of the customer have been handled by other staff, then the risk of it being a fictitious account, for example, will be reduced. This is because it is expected that other employees would have verified the existence of the customer. On the other hand, if there have not been any intervening transactions which could have possibly answered some questions then it must be flagged as a high-risk transaction requiring additional authorisation.

The fraud risk therefore becomes;

$R = f(T_{1...n,}|O_{H,}\ T_c)$

Where

R = Fraud Risk

$T_{1...n}$ = Transaction history

T_c = Current transaction c

$O_{H\,=}$ Objects history

And *$T_{1....n,}|O_H$ = Transaction history of given an object history (O_H)*

As mentioned earlier the level of conflict determines the level of risk and this would be the basis for determining the level of authorisation or scrutiny required to get the transaction in question processed.

Different levels of risk would have a different authorisation requirement. When the current fraud risk is determined a corresponding level of authorisation would be required to ensure the transaction proceeds.

Rules relating to which transactions are conflicting would be determined by risk manager to reflect the risk management policies which are based on a risk assessment, risk rating of the staff and other prevailing factors like the number of staff etc. This also introduces a human element control. This is particularly important because having some level of human configuration for the system maintains flexibility and also ensures that such controls are responsive and adaptive.

8. CONCLUSIONS

Effective separations of duties need conditions that can completely isolate tasks that conflict with each other. These conditions are however not always available as has been discussed. The introduction of mechanisms that improves the ability to prevent users from any undesirable access becomes necessary. This paper has discussed achieving this by measuring the level of conflict at run time and assigning controls based on that.

The development of a specific predictive models using specific mathematical and statistical techniques to determine the extent conflict to enable system managers decide the level of oversight and the necessary mechanics for managing such conflict will be considered in the future studies.

9. REFERENCES

[1] Hu, V.C., D.F. Ferraiolo, and D.R. Kuhn, *Assessment of Access Control Systems* 2006, Computer Security Division, National Institute of Standards and Technology: Gaithersburg.

[2] Behr, A. and K. Coleman, *Separation of duties and IT security*, in *CSO Magazine*. 2017, IDG Communications: California.

[3] Simon, R.T. and M.E. Zurko, *Separation of Duty in Role-Based Environments*, in *10th Computer Security Foundations Workshop* 1997.

[4] Ferroni, S., *Implementing Segregation of Duties.* ISACA Journal, 2016. **3**.

[5] Perelson, S., *SoDA: A Model for the Administration of Separation of Duty Requirements in Workflow Systems*. 2001, **Port Elizabeth Technikon**.

[6] Clark, D.D. and D.R. Wilson. *A Comparison of Military and Commercial Computer Security Policies*. in *IEEE Symposium on Computer Security and Privacy*. 1987. Oakland California: IEEE.

[7] Perelson, S. and R.A. Botha, *Conflict Analysis as a Means of Enforcing Statis Separation of Duty Requirements in Worflow Environments.* South African Computer Journal, 2000. **26**.

[8] Tsegayeand, T. and S. Flowerday, *A Clark-Wilson and ANSIrole-based access control model.* Information & Computer Security, 2020. **28**(3): p. 2056-4961.

[9] Nash, M.J. and K.R. Poland, *Some Conundrums Concerning Separation of Duty*, in *IEEE Symposium on Research in Security and Privacy*. 1990, IEEE: Oakland California. p. 201-209.

[10] Habib, M.A. and C. Praher, *Object Based Dynamic Separation of Duty in RBAC*, in *Internet Technology and Secured Transactions*. 2009: London.

[11] Ellen Zurko, M. and R.T. Simon, *Separation of Duties*, in *Encyclopedia of Cryptography and Security*, H.C.A. van Tilborg and S. Jajodia, Editors. 2011, Springer US: Boston, MA. p. 1182-1185.

[12] Loock, M. and J.H.P. Eloff, *Investigating the Usage of the Chinese Wall Security Policy Model for Data Mining*, in *International Symposium on Information and Communications Technologies*. 2005: Cape Town.

[13] Brewer, D.F.C. and M.J. Nash, *The Chinese Wall Security Policy*, in *IEEE Symposium on Research Security and Privacy*. 1989, IEEE: Oakland Califonia.

[14] Minsky, N.H. and V. Ungureanu, *Unified Support for Heterogeneous Security Policies in Distributed Systems*, in *USENIX Security Symposium*. 1998: San Antonio.

[15] Fehis, S., O. Nouali, and M.-T. Kechadi, *A New Distributed Chinese Wall Security Policy Model.* Journal of Digital Forensics, Security and Law, 2016. **11**(4).

[16] Lin, T.Y., *Chinese Wall Security Policy - An Aggressive Model.*, in *Fifth Annual Computer Security Applications Conference*. 1989: Tuscon, Arizona.

[17] Stewart, J.M., E. Tittel, and M. Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*. 3rd ed. 2018, San Francisco: John Wiley and Sons Inc.

[18] Association of Certified Fraud Examiners, *2018 Global Study on Occupational Fraud and Abuse*, in *Report to the Nations*. 2018, Association of Certified Fraud Examiners: Austin, Texas, USA.

[19] Dadzie-Dennis, E.N., et al., *Employee Fraud in the Banking Sector of Ghana.* SBS Journal of Applied Business Research, 2018. **6**.

[20] Sanusia, Z.M., M.N.F. Ramelib, and Y.M. Isa, *Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss.* Procedia Economics and Finance, 2015. **28**: p. 107-113.