Design of a Secure Public Accounts System for Enhanced War Against Corruption Using Intelligent Software Agent

Olugbemiga Solomon Popoọla[1(✉)], Kayọde Boniface Alese[2], Ayọdele Solomon Kupoluyi[2], Caleb Ayọdeji Ehinju[2], and Adebayọ Olusọla Adetunmibi[2]

[1] Computer Science Department, Ọsun State College of Education Ila-Ọrangun, Ila-Ọrangun, Nigeria
popsol7@yahoo.com, popsol777@gmail.com
[2] Computer Science Department, Federal University of Technology, Akurẹ, Akurẹ, Nigeria

Abstract. Transparency of methods is a measure of accountability in governance. Availability of public data is a measure of transparency. However, confidentiality and integrity are mandatory requirements for the security of public data, which consequently enhances accountability. Maintaining public data availability, while optimal degree of their integrity and confidentiality are ensured, is a paramount preoccupation of any good government. Among such data are the public bank accounts. Treasury Single Account (TSA) is a measure towards the security of public funds; but it constitutes liquidity challenge to the banking sector of the economy. This paper presents a leakage-blocking public finance management (PFM) mechanism; a secured multiplatform for receipts and payments system, which is liquidity-friendly to the commercial banking industry. A web (Internet) platform is required for all transactions. Software intelligent agents are employed in monitoring receipt and payment processes made by the clients of the revenue-generating Ministries, Departments and Agencies (MDAs) of the government. The mechanism ensures that the centralized bank account's transactions are logged; and appropriate heads and subheads are updated accordingly after every successful transaction. Thus the inflow of revenue would be tracked, and illegal bank accounts reported promptly. Therefore, public accounts would be under intensive surveillances, guaranteeing the accountability of every kobo generated.

Keywords: Accountability · Availability · Integrity · Confidentiality
Public accounts · Treasury Single Account

1 Introduction

A financial reform process of the present Nigeria democratic dispensation conceived and nurtured the Treasury Single Account (TSA) as an alternative approach towards fighting financial leakages and corruption being perpetrated through the government fragmented Revenue Bank Accounts (RBAs), which has hitherto been in operation [1].

V. Odumuyiwa et al. (Eds.): AFRICOMM 2017, LNICST 250, pp. 246–252, 2018.
https://doi.org/10.1007/978-3-319-98827-6_23

Coincidentally, TSA has provisions in sections 80 and 162 of Nigeria constitution of 1999 (as amended). It maintains a single account, where all receipts are paid, and from where all payments are made.

Liquidity in the banking sector of the economy is a major challenge of TSA [2]. In a developing democracy with developing economy, running the commercial banks out of cash is dangerous to small and medium scale industries. The present implementation of TSA has given highest premium to where/who keeps government money; with the presumption that it is only a centralized reservoir of funds that could be managed centrally. But, the true spirit of Public Financial Management (PFM) is how government funds could be managed efficiently and cost-effectively.

This paper presents a revised implementation of TSA, which is liquidity-friendly to the commercial banking industry. The design is a distributed reservoir of government funds whose management is centralized. The design also captures all categories of government funds holistically.

2 Current Implementation of TSA

Under the present arrangement, MDAs are categorized into eight, based on budgetary and/or funding status. Based on the categories, some MDAs would use an electronic collection platform – Government Integrated Financial Management Information System (GIFMIS) – through the Deposit Money Banks (DMBs) to remit receipts into the TSA; while some others would open a sort of Sub-accounts with CBN where their receipts would be remitted through Remita, the CBN payment gateway [3].

MDAs are to voluntarily close all existing RBAs, and forward evidence of such closure to OAGF. Those categories that require Sub-accounts with CBN are to channel the request to open such account through the OAGF. After request is granted, such MDA has to register in order to use Remita. Even, they could register to spend part of the collection made to the Sub-accounts through the same CBN payment gateway (Remita). Receipts and payments reports have to be forwarded to OAGF manually. Criteria for exemption from TSA are not explicit, because opportunities are opened to MDAs to apply for exemption [4].

Summarily, the payer visits MDA to obtain some sort of codes; go to a DMB, which must use Remita to process the remittance; the DMB generates payment evidence for the payer, which he takes to the appropriate MDA to effect the delivery of the goods and/or services paid for. At the close of each working day, the DMBs clear the revenue account into the CBN designated TSA, maintaining a zero-balance account for the RBAs [4].

2.1 Current Challenges of TSA

Zero-balance accounts would pose a serious liquidity challenge in the banking industry: Reducing the DMBs lending power. Cash-crunch might lead to work force downsizing; a negative trend that is looming in the banking industry [2].

Remita's monopoly of government funds remittance negates the spirit of competitiveness in a supposedly deregulated market. Monopoly would definitely hamper

appropriate computing standards upon which adequate benchmarking of solution of such magnitude of importance should be anchored. This has led to charges, which is currently based on a certain percentage of funds collected; instead of a uniform charge, which should be based on volume of transactions [5].

The nature of the fragmented public accounts requires an automated system for the confirmation of their closure, which does not feature in the current implementation. Threats of sanctions through government circulars do not guarantee a faithful closure of all these bank accounts. Even new fraudulent bank accounts could still be opened in the future if not prevented.

3 Best Security Practices for Information Systems

All risks, threats and vulnerabilities are measured for their potential capability to compromise confidentiality, integrity and availability of information. Hence, all security controls, mechanisms and safeguards are designed and implemented to provide confidentiality, integrity and/or availability. Certainly, the strength of any system is not greater than its weakest link. Defense-in-depth security strategy is integrated, by building up, layering on and overlapping modular security measures. This provides security compensations: If one defensive measure fails, there are other defensive measures in place that continue to provide protection. The weakness of one security measure is compensated for by the strength of others. Hence, vulnerability of a single weak link would not aid successful exploitation of the system [6].

Separation of duties (SoD) is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties, or division of labour, or separation of powers. Literatures from the Information Systems Audit and Control Association (ISACA) report that SoD specifies that no single individuals should have controls over two or more phases of an operation, so that a deliberate fraud is more difficult to occur; because it would definitely require collusion of two or more individuals or parties. Therefore, potential damage from the actions of a single person is reduced [7].

Need-to-know principle gives access rights to a person to perform their job functions. This principle is used in the government, when dealing with different clearances. Even though two employees in different departments have a top-secret clearance, they must have a need-to-know in order for information to be exchanged. Within the need-to-know principle, network administrators grant the employee least amount privileges to prevent employees' access, so that they cannot do more than what they are supposed to [6]. Moreover, least (minimal) privilege principle requires that in a particular abstraction layer of a computing environment, every module (i.e. a process, a user or a program) based on the layer being considered, must be able to access only such information and resources that are necessary to its legitimate purpose and duty [7].

To be effective, security controls must be enforceable and maintainable. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail [6]. Reports of all suspicions to the technical/surveillance stakeholders must be automated, online, and real-time.

4 The All-Sectors Accommodating TSA

Reengineering the current TSA implementation would eliminate most of, if not all, the challenges being experienced in some sectors of the economy. In preparation for a smooth deployment of a robust solution, some actions and processes need be carried out on the core stakeholders.

The MDAs should be tagged on per branch bases. Interested electronic payment platforms (ePays) should be registered. DMBs should be registered on per branch bases. Comprehensive coding of goods and services would address all forms of government businesses and activities. Every transaction is assigned a unique code, which is automatically translated to the goods/service descriptions on the goods/service request form and payment invoice.

At the takeoff, the basic databases would include MDAs, DMBs, E-Transaction Systems, Economy Sectors, Receipts, Payments, Treasury Subheads, Goods, Services, Donations, Foreign Currency Receipts, Foreign Currency Payments, Raised Funds, Grant and Counterpart Funds. Databases are expected to grow over some time until the working conditions of the system satisfy set objectives. The need for necessary visibility of unusual and/or unauthorized actions to some kind of law enforcement agents such as Economic and Financial Crimes Commission (EFCC) (as may be modified to fit into contemporary forensic technologies) might account for such growth. Also, availability of authentic public data to the general public through the media houses might justify expansions of databases. Local and remote backups of databases are automated in accordance with some timely schedules (Fig. 1).

The CBN hosts a GIFMIS; the receipts and payments management and coordinating platform. It generates invoices, verifies payments, issues payment evidences, manages databases, maintains electronic ledgers, and coordinates multiple backups for preventive purposes. The CBN gives feed-backs to appropriate MDAs, Payers and DMBs on every transaction. The GIFMIS hosts intelligent agents and tamperproof subsystems for keeping constant surveillance on the system so that automated real-time reports of tamper-attempts are ensured. The intelligent agent specifically scans the intranet of appropriate DMB for possible fraudulent duplication and/or opening of bank accounts for MDAs.

The package in Fig. 2 is wirelessly connected and integrated into the DMBs' intranets, through which they are connected to each other (i.e. extranet) and the Internet. There is a single common program for processing all payment transactions of the government, eliminating the duplications that are usually occasioned by policy-specific programs such as for the aviation industry and foreign currency donor/counterpart funds. Goods and services setup and corresponding subheads are defined as parameters. Goods and services could be added/modify very easily.

Only authorized users have access to the system, and such could perform only authorized tasks. It is a multi-user system with user-defined security levels; and there is no restriction on the number of users. Every change in the database requires authentication of the administrator, the CBN governing body and electronic audit moderating body; and the system keeps audit trail of all changes. Transactions reports link is only accessible at the appropriate time.

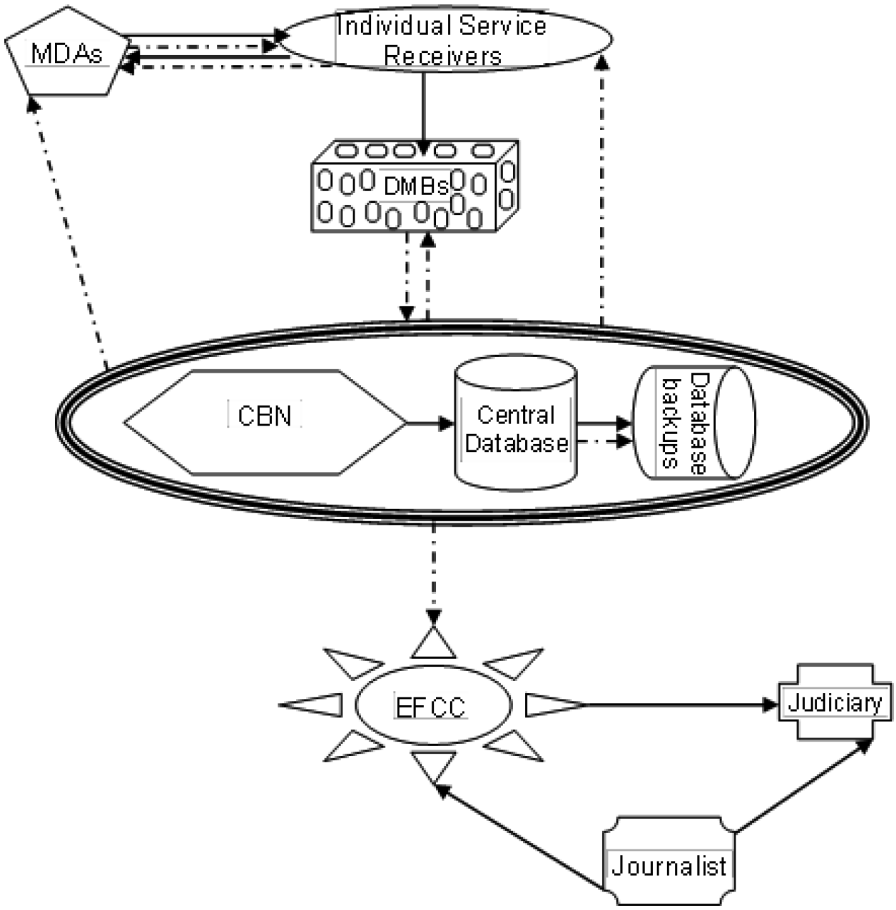

Fig. 1. Architecture of a corruption-fighting TSA

The intelligent agent searches for existing MDAs' bank accounts, which were fraudulently kept from being closed. Suspected existence or duplications of bank accounts are automatically detected and reported to the system administrator and/or the EFCC for appropriate actions (Fig. 2).

4.1 Security Features

User access to database is through the package only. All updates are carried out using stored procedures after proper validations, data integrity checks, and transaction auditing. Users have only execute permission to the stored procedures, and only when called via the package (Fig. 2). Every transaction is monitored by the system; and also keeps an audit trail for the same. Before processing reports, the system ensures that all expected data is received and all databases are updated.

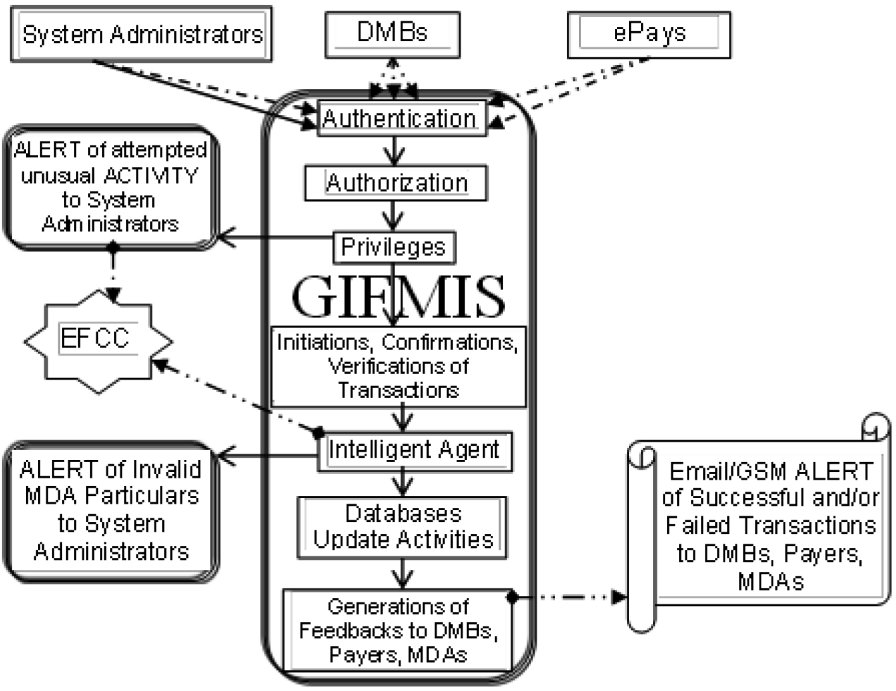

Fig. 2. Network of security modules

Apart from the physical network access security, the package has its own User Access system. The system administrator has the highest authority level and access to all options of the package. He can create Supervisory Users and grant them access to restricted work options. The security of the information systems are audited on timely basis with automated mechanism. Every change in the database bears the signature of the transaction point and the supervisor in charge.

5 Conclusion

Information security is the process of exercising due care and due diligence to protect information and information systems, from unauthorized access, use, modification, destruction, disclosure, distortion, disruption or distribution. This makes information security an indispensable part of all business operations across different domains.

This design focused on financial security issues as they feature right from issuing of invoice to clients by the MDAs till payments/receipts transactions are updated on the databases at the CBN. New data concerning any MDA is entered only once. Goods/services per MDA per DMB per Treasury subhead are mapped with very high level of consistency. There is a single program and common databases for all users. Integrity and availability of data are guaranteed.

Hence, the design presents a TSA that is intelligent, automated, online, and real-time. Therefore, MDAs, ePays and DMBs with invalid identities are not allowed for any transaction; illegal bank accounts are blocked; defaulting MDAs, ePays and DMBs are promptly detected and located. Automated local and remote backups are ensured; enhancing the Confidentiality, Integrity and Availability requirements of public accounts processes and records; and maintaining the quality assurance of public financial management, which guarantees a lifelong sustainability of the actual objectives of Treasury Single Account.

6 Recommendations

Appropriate security policy legislations should be put in place for adequate regulatory procedures for the enhancement of the effectiveness and efficiency of the electronic processing activities. Adequate security of the remote backups of databases should be ensured; and scheduled system evaluation is necessary for possible performance upgrade.

Proper use of information technology systems should be ensured through relevant, regular and up-to-date workshops and seminars for the different categories of public financial management stakeholders. To ensure optimum throughput, regular maintenance of any information technology installations is important.

References

1. Ifeanyi, M.: Treasury single account (in Nigeria) issues and implications. Covenant University, Canaanland, Ọta, Nigeria (2015)
2. Eme, O.I., Chukwurah, D.C., Emmanuel, N.I.: An analysis of pros and cons of treasury single account policy in Nigeria. Arab. J. Bus. Manag. Rev. (OMAN Chapter) **5**(4), 20 (2015)
3. Ọtunla, J.O.: Introduction of e-Collection of Government Receipts. Federal Treasury Circular, Ref: Nọ TRY A1 & B1/2015/OAGF/CAD/026/V.1/253 (2015)
4. Accountant-General of the Federation (AGF): Guidelines on the Implementation of TSA/e-Collection. Office of the Accountant-General of the Federation (2015)
5. Taiwo, O.: TSA and Taxation (2015). www.pwc.com/nigeriataxblog
6. Popoọla, O.S., Ajayi, O.D., Salawu, A.K.: Electronic processing of examinations for educational systems (EPEES): a security framework. KWASU (Kwara State Univ.) Int. J. Educ. (KIJE) **2**(1), 193–206 (2014)
7. David, H., et al.: Enterprise resource planning (ERP) security and segregation of duties audit: a framework for building an automated solution. Inf. Syst. Audit Control Assoc. (ISACA) J. **2**, 11–25 (2007)