CRITICAL ASSESSMENT OF AUDITING CONTRIBUTIONS TO EFFECTIVE AND EFFICIENT SECURITY IN DATABASE SYSTEMS

Olumuyiwa O. Matthew[1] and Carl Dudley[2]

[1]MSc in Information Technology Management, MCPN, AMBCS,
The University of Wolverhampton, United Kingdom.
o.o.matthew@wlv.ac.uk
[2]Oracle Professor in Database Technology University of Wolverhampton, UK.
UK Oracle User Group Official, oracle ACE Director
carl.dudley@wlv.ac.uk

ABSTRACT

Database auditing has become a very crucial aspect of security as organisations increase their adoption of database management systems (DBMS) as major asset that keeps, maintain and monitor sensitive information. Database auditing is the group of activities involved in observing a set of stored data in order to be aware of the actions of users. The work presented here outlines the main auditing techniques and methods. Some architectural based auditing systems were also considered to assess the contribution of auditing to database security. Here a framework of several stages to be used in the instigation of auditing is proposed. Some issues relating to handling of audit trails are also discussed in this paper. This paper also itemizes some of the key important impacts of the concept to security and how compliance with government policies and regulations is enforced through auditing. Once the framework is adopted, it will provide support to database auditors and DBAs.

KEYWORDS

Auditing, Techniques, Security, Framework, Procedure

1. INTRODUCTION

Database Auditing allows security personnel to ascertain who did what to which data, when and how [1]. It is a mechanism used to monitor the actions of every user in a database [2]. Database auditing helps strengthen the security of the database by keeping logs of the activities performed on a database. It can be used to confirm that data or information is not accessed by those without permission and that they do not go beyond the privileges granted to them by the database administrator.

The security mechanism must not only prevent attacks but also detect potential attacks. After all, the best security policy is still not going to stop every attacker. This is where auditing helps in monitoring the environment and identifying potential attacks [3]. Lu et al [4] describe auditing operations as critical processes for identifying malicious behaviour, maintaining data quality and improving system performance. Mullins [5] said database auditing is the process of monitoring

Dhinaharan Nagamalai et al. (Eds) : CSITA, ARIN, ISPR - 2015
pp. 01–11, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.50801

access to and modification of selected database objects and resources within operational databases and retaining a detailed record of the access where said record can be used to proactively trigger actions and can be retrieved and analysed as needed. This means with auditing records, a database administrator can carry out analysis on the trend of events in a database system.

Database auditing is an increasingly important aspect of database security. The implementation of user identification, authentication and access control are part of the security measures, but with all of these in place, database is still not fully secured. None of these measures are capable of monitoring and logging database activities, to allow subsequent detection of security breaches [2]. To manage access to sensitive data, a user can be subjected to a variety of authentication and access control mechanisms which implement rules and controls for known and acceptable data access behaviours. But to protect against and discover unknown or unacceptable behaviours always requires a need to monitor data access. To assist in this task, a database system that provides an audit facility must be used.

The level of security that a database system offers is, at least in part measured by the level of auditing that can be implemented with the system. Yang [6] explains that there is no security without auditing; therefore security and auditing should be implemented in an integrated fashion. Auditing database activity and access can help identify security issues and resolve them quickly. Auditing as a function needs to play a central role in ensuring compliance with regulations because an audit produces documentation of actions, practices and conduct of a business or individual. It can be used to measure compliance to policies, procedure, process and law. So, it helps measure the compliance of both the developers and users to the business ethics.

This paper has been divided into different sections. Section 1 is a brief introduction to the subject of database auditing. Section 2 gives an overview of existing techniques, models and architectures. Section 3 has the finding from the research and proposed algorithm for the auditing procedure. Section 4 is about the risk assessment. Section 5 concludes the paper focusing on recommendation.

2. RELATED WORKS

Database auditing is now seen as a major factor in determining the security level of a database system. It is proven that no system or database can be one hundred per cent secured but the ability of it to recover from attack as quickly as possible with the help of auditing facilities provided by the DBMS is of paramount importance. Liu and Huang [7] said that all architects must bolster policies by using database auditing in addition to other security features built into all major database platforms. This is an indication that security measures alone cannot ensure security without auditing. Different actions are performed on a database ranging from logging, deletion, update, and privilege control. All these actions contributes to the security of a database depending on the basis to which they are carried out.so auditing is used to check for the genuineness of every actions performed on a database. Huang and Liu [7] put it that database auditing involves observing a database so as to be aware of the actions of the database users, to help ensure that information is not accessed by those without the correct permissions.

Looking at the concept from the field of telecommunications industry, the term data audit was explained by Bagchi et al [9] as a broad range of custom and ad hoc, application- level techniques for detecting and recovering from errors in a switching environment. Elshiekh and Dominic [10] looked at auditing in terms of a statistical database used as a mechanism for keeping up-to-date logs of all queries made by each user and constantly checking for possible compromise whenever a new query is issued. Kogan and Jajodia [11] put it that auditing capability is one of the

requirements for secure databases and that a secure database management system, among other things, has to provide not only facilities for recording the history of all updates but high-level support for querying this history as well. This is an indication that this concept at any time can query i.e. audit any update done to the system to ascertain the quality of information in the database.

2.1 Database efficiency improvement

Wentian and Miklaus [12] point out that auditing the changes to a database is critical for the identification of malicious behaviour, maintenance of data quality and improving system performance. Waraporn [13] gives two major reasons for database auditing which are to have data log files which helps in the recovery of transactions and also in the investigation of transactions. This is true because information security in term of authentication and authorisation can help protect information but does not provide help in investigating transaction activity. Therefore, the efficiency of the system can also be improved with the use of auditing techniques. Every system should have self-check facilities to improve its quality and efficiency.

2.2 Database auditing for compliance

Database auditing has also helped to improve the compliance of organisations to the different acts and regulations concerning data privacy from both the customer's and the organisation's points of view. When databases are audited, data integrity is maintained. Due to the high rate of information and financial fraud, several laws and regulations were propounded by different governments to militate against this trend. Hasan and Winslett [14] historically informed that the drumbeat of financial accounting scandals, from ENRON in 2000 to Satyam InfoTech in 2008, has prompted the introduction of regulations intended to guarantee the integrity of business records. This gives room for companies to have control over their sensitive data. Organisations that handle sensitive data are now held to a much higher standard of data access accountability [15]. This arises from the different regulatory compliance laws enforced by different countries and regions. Yang [6] explain that auditing as a function needs to a play a central role in ensuring compliance because an audit documents actions, practices and conduct of a business or individual. It then measures their compliance to policies, procedure, process and law. Regulations such as the following have common auditing-related requirements: Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), International Convergence of Capital Measurement and Capital Standards- a Revised Framework (Basel II), Japan Privacy Law and European Union Directive on Privacy and Electronic Communications.

2.3 Database auditing methods

There are different auditing techniques and methods depending on what type of auditing to be carried out or what data is to be audited. According to Mullins [5] database auditing can be categorized into three major types. Namely:

- Authorization Auditing - Who can do what?
- Access Auditing - Who did what, Modifications?
- Replication Auditing - Who copied which data where.

While Noreen et al [8] itemized the following as different methods

- **Triggers** - Set of procedures that automatically executes in response to a certain event.
- **Transactional Log** - A log maintained by SQL Server to store information of almost any activity taking place on the database Server.

- **C2 Auditing** - It records the database information that goes beyond server level events.
- **Default Trace** - It runs as a background service of MS SQL Server 2005 and assists the database administrator (DBA) to check the database users' activities.

While according to Srivastava [16] said auditing techniques are divided into the following types:

- **Statement Auditing-** The auditing of selective SQL statements irrespective of the schema object on which they are fired is Statement auditing. For example, auditing on the DDL statement fired by a user.
- **Privilege Auditing-** Privilege auditing is nothing but the audit of the usage of selective privileges like the Create Table privilege by a user. Privilege auditing can be done on any user or on all users.
- **Schema Object Auditing -** Auditing on specific schema objects is met by schema object auditing. All DML activities, Grant and Revoke performed on a specific table or all tables within a schema can be captured.
- **Fine Grained Auditing-**Fine grained auditing provides auditing on data access based on the data content.

Dudley [17] itemized the different types of auditing techniques that can be used on the Oracle database including the default System-based auditing, fine-grained auditing, trigger-based auditing, flashback techniques and flashback data archive.

Each of the authors prove and explain all the techniques with examples to show the impact on security.

2.4 Database auditing models, framework etc

There are few open source projects or publication in this area. However, the following related publications in database auditing derive frameworks, algorithms, architectures, techniques, or models for carrying out database auditing.

Bagchi et al [9] came up with an audit subsystem architecture that shows the design of the database audit process and its interaction with other system components. The proposed audit framework provides audit functionality and consists of the top-layer shell (the ***audit interface)*** and the individual elements that implement specific audit triggering, error detection and recovery techniques.

Bottcher and Steinmetz [18] proposed another system architecture for a privacy audit system of any XML database, extended by a middleware that consists of a query log and a backlog. These two above architecture were proposed as a solution to carry out basic audit in a system.

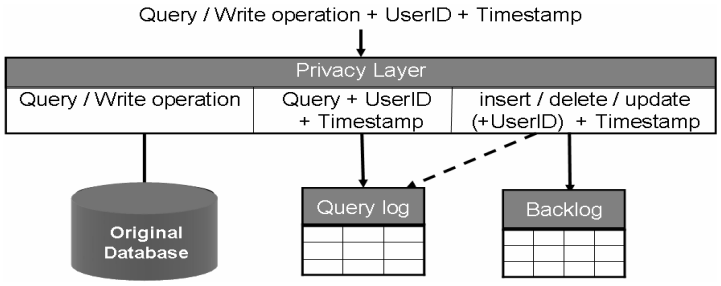

Figure 1- system architecture [18]

Another architecture was shown in Woo et al [19] which has three main components for auditing a database system. The logger, analyzer and notifier.

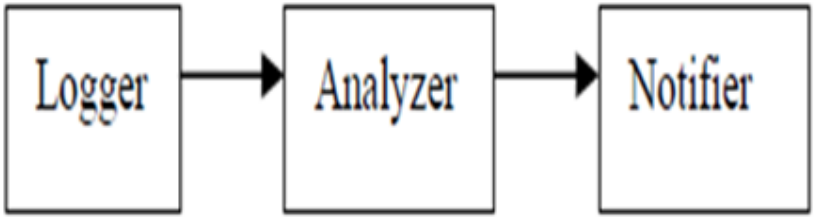

Figure 2-Anatomy of Auditing System (Bishop 2003) in Woo et al [19]

Woo et al produce this architecture in order to verify every access made into the system. The analyser does this by analysing every query and update activity on the system and comes up with authorizations which the notifier will further send to the appropriate session as the case may be.

Agrawal et al [20] have developed an architecture for their Sarbanes-Oxley solution which consists of four main components: (i) workflow modelling, (ii) active enforcement, (iii) workflow auditing, and (iv) anomaly detection. Agrawal solution was designed for compliance purposes and incorporates the work process into the system.

Johnson and Grandison [21] also proposed an architecture based system called Hippocratic Database(HDB) which enables compliance with security and privacy regulations without impeding the legitimate flow of information.

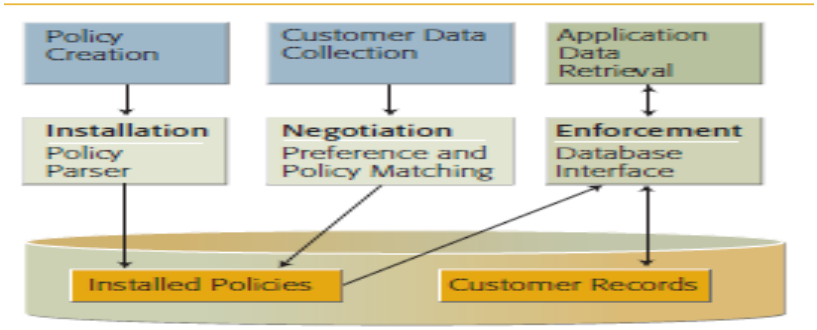

Figure 3- HDB active enforcement architecture [21]

Yangquig et al [22] produced an audit model that set up traces through database stored procedures to collect audit data The audit module stored and transported audit data in standard XML format to the audit server.

Noreen et al [8] proposed a system architecture for a target database on which auditing is to be performed. It is mounted on an instance of Microsoft SQL Server (MS SQL 2005).

Zonnone et al [23] also proposed an approach that will verify the compliance of user behaviour with data protection policies. The introduction of all these architectures only serves to emphasise the importance of auditing to any database environment. Security is not complete until there is an effective and efficient auditing system in place.

2.5 Database Audit and Protection (DAP) versus Database Activity Monitoring (DAM)

DAP — a term Gartner has developed to replace the earlier DAM concept — refers to suites of tools that are used to support the identification of and reporting on inappropriate, illegal or otherwise undesirable behaviour in RDBMSs, with minimal impact on user operations and productivity. These suites have evolved from DAM tools (which offered analysis of user activity in and around RDBMSs) to encompass a more comprehensive set of capabilities, including:

- Discovery and classification
- Vulnerability management
- Application-level analysis
- Intrusion prevention
- Support for unstructured data security
- Identity and access management integration

DAP provides better auditing and monitoring support than native logging, which can add significant overhead and does not provide the same level of granularity as DAP tools. DAP, moreover, provides comprehensive cross-platform support in heterogeneous database environments, and can serve as an effective addition to identity and access analytics [24].

3. DISCUSSION OF FINDINGS

Database auditing is a recognised technology used to determine if security and other policies are being violated. It is used in obtaining details about system usage, data modification and to help in the detection and recovery of database systems from system failure or human errors. Therefore the implementation and management of this technology is critical to the efficiency and performance of the system.

3.1 Auditing procedures and techniques

The auditing procedures in most environments start with logging activities (i.e when and how logging was done). This includes the logon and logoff records with failed and successful ones. Every environment provides this. The second stage is to check for privileges, user's definitions and other security attributes like role definition, password changes, deletion and addition of users. The third stage is to check for changes made to the database schema such as data being copied from one table to an additional table thereby changing the schema. The fourth stage is the auditing of the use of sensitive data. The fifth stage is concerned with auditing the changes made to stored procedures or codes. Other auditing stages that can be carried out involve the audit of database errors because attackers tend to make several erroneous attempts before making head way. Also, auditing any changes made to the definition of what is to be audited. These identified procedures were proposed in the framework for auditing shown below.

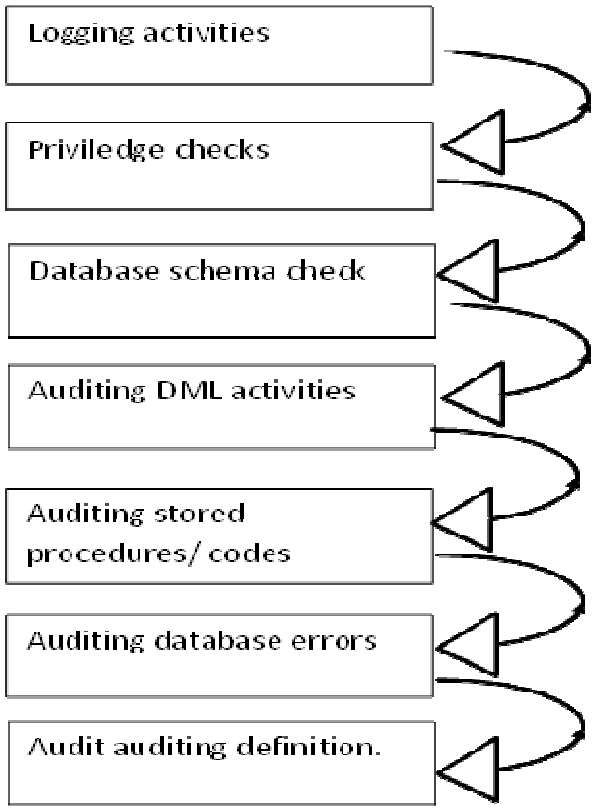

Figure 4 -A framework for auditing procedure

3.2 Impact of auditing on security

Auditing activities within a database can help identify security issues and also resolve those issues. In fact it can be said that there is no security without auditing. The following are areas identified in which auditing impacts greatly on the security of a database.

- Auditing activities enable future accountability for current actions.
- Auditing activities can help deter users and even intruders from inappropriate actions based on that accountability.
- These activities also help in investigating suspicious activity.
- It helps Notify an auditor of actions by an unauthorized user.
- Also helps detect problems with an authorization or access control implementation.
- Auditing activities also address auditing requirements for compliance.

3.3 Impact of government policies and regulations on auditing

There exist today numerous policies and regulations which have been put in place because increasing numbers of organisations are faced with sensitive information protection difficulties. These policies have stringent requirements on the collection, processing and disclosure of personal data. Now because of the difficulties associated with companies coping and enforcing these laws, there is a new trend to adopt a database compliance auditing system. It is obvious that without a compliance auditing system in place it is very difficult for organisations to monitor and enforce compliance with the policies and regulations.

Johnson and Grandison [21] give an example of a company called BankCo which uses HDB active enforcement to operate as a middleware layer above the database enforcing fine-grained policies. These policies are advised to be built into the database which gives the organisation a control measure over who has access, when the access occurs and where the access took place.

3.4 How to handle audit trail size

The database auditors are responsible for monitoring access to the database and tracking malicious actions after they have occurred [4]. When auditing is enabled in any DBMS, the audit output is recorded in an audit trail. The size of this trail can grow out of control when database activity increases. This will lead to issues such as how to keep it to a manageable size. Nando [25] explains the solution could be to relocate the audit trail to a different tablespace (Oracle) and set up an automatic purge process to keep its size under control. Nando [25] pointed out that this is one of the new features in Oracle Database 11g release2. This enables the database administrator to move audit trails from the SYSTEM tablespace to a different area of choice, allowing better management of the audit trail and to minimise the performance impact and disk space management.

Well-kept audit trail involving sensitive data should be part of any database deployment [26]. This helps in keeping track of malicious activity on the database. The failure to get this detailed audit records of database activity represents a serious organizational risk on many level. Many enterprises will turn to native audit tools provided by their database vendors or rely on ad-hoc and manual solutions. These approaches do not record details necessary to support auditing, attack detection, and forensics. Furthermore, native database audit mechanisms are notorious for consuming CPU and disk resources forcing many organizations to scale back or eliminate auditing altogether. Finally, most native audit mechanisms are unique to a database server platform. For example, Oracle logs are different from MS-SQL, and MS-SQL logs are different form DB2.

4. RISK ASSESSMENT

Based on nCircle [27] survey data breaches increased by 95% in 2010. The survey also shows that audit cost in 2008 to 2009 increased by 45%, while from 2009 to 2010 it increased to 47% (nCircle 2010 p4). Also from the nCircle [27] survey, meeting security compliance requirements was the biggest security concern in 2010 with 30% among other areas of concern. The PWC [28] survey, shows that there are two major factors acting as the driver for information security expenditure which are protecting customer information (34%) and complying with laws/regulations (17%).

Therefore, organisations should have a database compliance auditing system which has in place all the policies and laws applicable to their operations. This incorporates enforcement compliance with internal security policies and the ability to demonstrate continuous compliance.

5. CONCLUSION

In this paper, a critical assessment of auditing has been performed and an auditing procedural framework was developed. The rationale of the work presented here is to review some existing auditing techniques and architectures to bring out major benefits, in order to produce a framework which will effectively facilitate the database auditor to perform the intricate task of auditing. This procedure must be customized to the processes and operations already in place, and the relevant policies and regulations. This will allow organisations to enforce automated security and privacy controls that will align with existing laws and regulations to facilitate cross-border information

transfers. The adoption of a particular architecture or model for auditing activities has strategically placed organisations in a high level of effective security.

The work done on the auditing procedural framework can be enhanced in future by the inclusion of other stages of auditing not identified here and other functionalities. Firstly, each stage can be expanded by splitting it into sub-stages which will make it a more comprehensive system. Secondly, the entire proposed framework could be incorporated into a DBMS for adoption by organisations as part of their process.

Recommendation is also made to organisations to adopt a compliance auditing system which has policies and regulations inbuilt. This provides a control measure over those that have access, when and where access is made and also allows the demonstration of continuous compliance.

REFERENCES

[1] Dudley, C. (2012) Database Auditing. Lecture 14: 7C1006L14 [online]. [Accessed 17 May 2012]. Available at http://wolf.wlv.ac.uk/stech/68343/Slides/7CI006.

[2] Qiang, H. and Lianzhong, L. (2009) A Logging Scheme for Database Audit, Computer Science and Engineering, 2009. WCSE '09. Second International Workshop on 2009, pp. 390-393.

[3] Baccam, T (2010) Oracle database security: what to look for and where to secure. SANS analyst Program, April 2010. [Online]. London. [Accessed 23 may, 2012]. Available at: http://download.oracle.com/doc

[4] Lu, W., Miklau, G. and Immerman, N. (2013) Auditing a database under retention policies. The VLDB Journal—The International Journal on Very Large Data Bases [online], 22(2), pp. 203-228 .

[5] Mullins, C. (2008) Database Auditing. NEON enterprise software. Texas. [Accessed 24 July, 2012]. Available at:<http://www.neonsoft.com.

[6] Yang, L. (2009) Teaching database security and auditing. In Proceedings of the 40th ACM technical symposium on Computer science education (SIGCSE '09). ACM, New York, NY, USA,241-245.DOI=10.1145/1508865.1508954 http://doi.acm.org/10.1145/1508865.1508954

[7] Liu, L. and Huang, Q. (2009) A Framework for Database Auditing, Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on 2009, pp. 982-986.

[8] Noreen, Z. Hameed, I. and Usman, A. (2009) Development of database auditing infrastructure. In Proceedings of the 7th International Conference on Frontiers of Information Technology (FIT '09). ACM, New York, NY, USA, Article 78, 6 pages

[9] Bagchi, S., Liu, Y., Whisnant, K., Kalbarczyk, Z., Iyer, R., Levendel, Y. and Votta, L.(2001) A framework for database audit and control flow checking for a wireless telephone network controller, Dependable Systems and Networks, 2001. DSN 2001. International Conference on 2001, pp. 225-234.

[10] Elshiekh, A. and Dominic, P. (2008) A new auditing scheme for securing statistical databases Information Technology, 2008. ITSim 2008. International Symposium on. [Online]. pp.1-5.

[11] Kogan, B. and Jajodia, S. (1991) An audit model for object-oriented databases Computer Security Applications Conference, 1991. Proceedings., Seventh Annual. [Online]. pp.90-99.

[12] Wentian, L. and Miklau, G. (2009) Auditing a Database under Retention Restrictions, Data Engineering, 2009. ICDE '09. IEEE 25th International Conference on 2009, pp. 42-53.

[13] Waraporn, N. (2010) Database Auditing Design on Historical Data. In Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10). Jinggangshan, China, April. 2010, pp. 275-281

[14] Hasan, R and Winslett, M. (2011) Efficient audit-based compliance for relational data retention. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11). ACM, New York, NY, USA, 238-248.

[15] Mazer, M. (2006) Auditing Databases for Compliance and Risk Management, DM Review, vol. 16(3), pp. 18-19

[16] Srivastava, M. (2009) Fine Grained Auditing in Oracle 10g [online]. [Accessed 28th July, 2012]. Available at: < http://hosteddocs.ittoolbox.com/ms080609.pdf>

[17] Dudley, C. (2012) Auditing techniques for oracle database 11g. Lecture delivered during oracle conference 2012, Texas, USA.

[18] Bottcher, S. and Steinmetz, R. (2006) Finding the Leak: A Privacy Audit System for Sensitive XML Databases, Data Engineering Workshops, 2006. Proceedings. 22nd International Conference on 2006, pp. 100-100.

[19] Woo, J., Lee, Sael. And Zoltowski, C (2007) Database Auditing [online]. [Accessed 24th July, 2012]. Available at :http://www.citeseerx,ist,psu.ed

[20] Agrawal, R., Johnson, C., Kiernan, J. and Leymann, F. (2006) Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology Data Engineering, 2006. ICDE '06. Proceedings of the 22nd International Conference on. [Online]. pp.92-92.

[21] Johnson, C. and Grandison, T. (2007) Compliance with data protection laws using Hippocratic Database active enforcement and auditing [online].

[22] Yangqing, Z., Hui, Y., Hua, L. and Lianming, Z. (2009) Design of a New Web Database Security Model, Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on 2009, pp. 292-295.

[23] Zannone, N., Petkovic, M. and Etalle, S. (2010) Towards data protection compliance [online]. IEEE, pp.1-4Available at: http://wlv.summon.serialssolutions.com/

[24] Wheatman, J. (2012) Database Auditing Monitoring is evolving into Database Audit and protection. Gartner Incorporation [online] February, 2012, [Accessed 22 September,2012]. Availableat:http://www.gartner.com/technology/

[25] Nando, A. (2010) managing Audit trails. Oracle Magazine [online] November 2010, [Accessed 19 September 2012].Available at:http://www.oracle.com/technetwork....

[26] Akanji, A. and Elusoji, A. (2014) A Comparative Study of Attacks on Databases and Database Security Techniques. [online].

[27] Ncircle (2010) information security and compliance trend study: Technical report [online]. California. [Accessed 03 August 2012]. Available at <:http://www.inteco.es/file/us>

[28] PWC (2012) Information security breaches survey: Technical report [online]. London. [Accessed 03 August 2012]. Available at :< http://www.pwc.co.uk/.../uk-information-security-breaches-survey-technica>

AUTHORS

Olumuyiwa Matthew received B.Tech and MSc degrees in Computer Science and Information Technology Management respectively. He is currently working towards the PhD degree with the department of Mathematic & Computer Science University of Wolverhampton, Uk. His current research interest is issues relating to the adoption of Multi-tenant database.

Carl Dudley holds the post of Emeritus Professor in Database Technology at the University of Wolverhampton, UK. He has been active within the Oracle database environment for the last 27 years, being a director of the UK Oracle User Group and speaking regularly at international conferences since 1991. He has also participated in the SQL Standards ISO group. In November 2002, Carl was selected as 'DBA of the Year' by Oracle Corporation. This worldwide award was given to him in recognition of his contribution to the Oracle user community and his work on innovative Oracle Server projects. Carl achieved Oracle ACE Director status in 2009 and is now a Fellow of the British Computer Society. His research interests lie in database performance tuning and database security.