American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-7, pp-210-218
www.ajer.org
Research Paper Open Access

Holistic Security Model for Mobile Database in Nigeria

Fidelis C. Obodoeze[1], Lois Onyejere Nwobodo[2], Samuel Obiji Nwokoro[3]
[1]*(Department of Computer Engineering Technology, Akanu Ibiam Federal Polytechnic Unwana, Nigeria*
[2]*(Department of Computer Engineering, Enugu State University of Science and Technology (ESUT), Nigeria*
[3]*(Department of Computer Science, Akanu Ibiam Federal Polytechnic Unwana, Nigeria)*

ABSTRACT : *Due to proliferation on the usage of mobile computing devices such as mobile phones, smart phones, Tablet PCs and Portable Digital Assistant (PDA) in Nigeria and world over, it is expected that these light-weight, powerful, low-cost computing devices will pave way for data-driven applications in mobile environments. These portal mobile devices can be connected to corporate database and application servers so that application processing can take place at any time and from anywhere. This can throw up a lot of security challenges. Hackers, malicious programs and rival firms can penetrate the corporate servers through various security holes or vulnerabilities. This paper examines these security holes that can emanate from three major windows- the mobile device, the mobile network and the corporate database server and critically x-rays various solutions that can ward them off in order to protect critical data from attack, eavesdropping, disruption, destruction and modification. This paper finally proposes a holistic security model to protect corporate mobile database in Nigeria.*

Keywords: *demilitarized zone (DMZ), encryption, firewall, malicious program, mobile database, redaction, security hole/ vulnerability*

I. INTRODUCTION

A mobile database is a database that can be connected to by a mobile computing device (the client) over a wireless mobile network to the server. A database server is used for the central storage of all application data, while small-footprint relational databases are used on the mobile clients.

A mobile database is either a stationary database, or a database which is actually stored by the mobile device. This could be a list of contacts, price information, distance travelled, credit or debit card or any other information. The client and server have wireless connections. A cache is maintained to hold frequent data and transactions so that they are not lost due connection failure.

The mobile database became prevalent in today's businesses in Nigeria because of the following reasons:

1. There is proliferation on the usage of mobile devices and smartphones since 2002 when the then Obasanjo Regime ushered in the GSM Telecommunication in Nigeria.
2. The number of smartphones in use today in Nigeria and around the world exceeds 2 billion in 2015.
3. Next billions of portable devices could be reached in the next few years.
4. More businesses now move towards employer's mobility, so connecting mobile devices to company's private corporate network makes business sense.
5. Powerful lightweight computing devices and low-cost mobile connectivity paved the way for data-driven applications in corporate networks.
6. Mobile data-driven applications pave way to connect and access data from anywhere and at any time.

1.1 Research Questions

In order to properly define the objectives and focus of this research paper, the following research questions will be answered by this paper:

1. What is a mobile database?
2. What are the securities in mobile database?
3. What is the security architecture of mobile database?
4. What are the security holes or vulnerabilities to a mobile database?

5. What are the issues, solutions to mobile database securities and what are the possible solutions/recommendations?
6. What are the security strategies or model to mobile database management in Nigeria?

1.2 Scope and contributions of this paper

This paper will examine the security challenges affecting the safe and smooth usage of mobile devices and smart phones on mobile databases which are constantly connected to corporate network of firms. This paper will equally examine the current mobile security attack models to assist in designing effective countermeasure framework that is suitable for protection of mobile database in Nigeria. Finally, this paper will propose far-reaching measures for a three-tier solution for – the mobile device, mobile network link and mobile database server's protection against hackers and malicious codes attacks.

II. MOBILE DATABASE SECURITY CHALLENGE

Despite the claims of anti-virus vendors, malware problems are near impossible to control. Attackers own user workstation subnets and mobile devices, and very often malware either directly finds a route to databases (critical infrastructure) or it opens a tunnel for manual hacker gangs to exploit.

2.1 Security of Mobile Database

Mobile database that resides inside the mobile device needs to be synchronized with the server at a particular point of time usually at the end of the day after transactions is completed for the day. Secured network is needed to transmit or transfer the mobile data from the mobile device (client) to the server. Fig. 1 shows the architecture of Mobile database security.

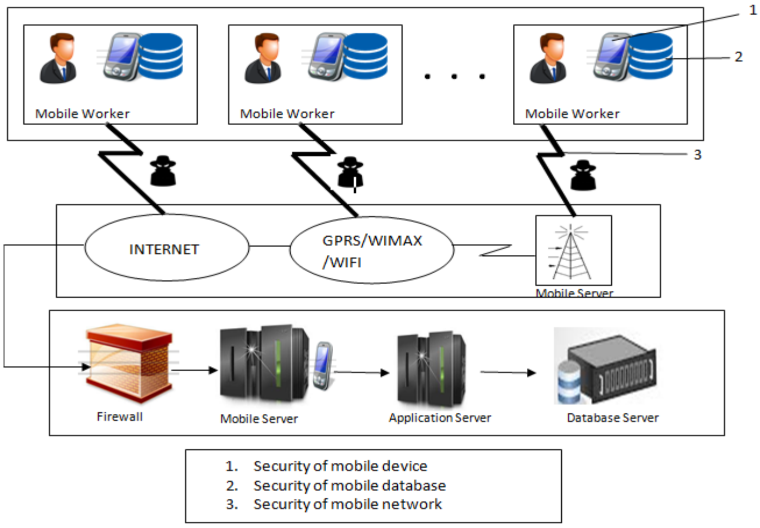

Fig.1. Architecture of Mobile database security [1]

From Fig. 1, it can be seen that security is needed at the mobile device, the mobile network link (internet, GPRS, WiMAX, Wi-Fi, GSM Base station) as well as the Servers (Application and Database) because security can be compromised from any of these three points.

The overall security of the mobile database application can be achieved by ensuring:

(a.) Security for the mobile device,
(b.) Security for the central computer or server,
(c.) Security for the communication link or network,
(d.) Security for application specific issues.

2.2 Areas of attack or vulnerability

Three (3) major areas are susceptible to attack in mobile database. They include the following areas:

1. The network link
2. The mobile device
3. The mobile database server

Once the three areas of attack or vulnerability are secured, the entire mobile database is secure. But if any of these three areas is vulnerable, then the entire mobile database can be hacked and penetrated.

2.3 Several possible attacks or vulnerabilities to a mobile database

There are several possible attacks that can affect the mobile network that even the legitimate users are not able to utilize its services. Such attacks are not limited to attacks from malicious codes – viruses, worms, Trojans, SMS and MMS spams, attack on the communication link by eavesdropping of network traffic of the application or a fake client or server node, attack against the server computer, attack against the mobile database application. Also Denial-of-Service (DoS) attacks are possible and can deny legitimate users from having access to the network and its services. Critical data assets of an organization can be stolen by hackers and criminals using the following cycle depicted in Fig.2. Here, an average attacker will first of all select the target (organization, computer, network) to attack, thereafter gather enough background information about the target. After gathering the background information of the target, the attacker then plans the attack, replays the attack (testing) and finally executes the attack and steals the data.

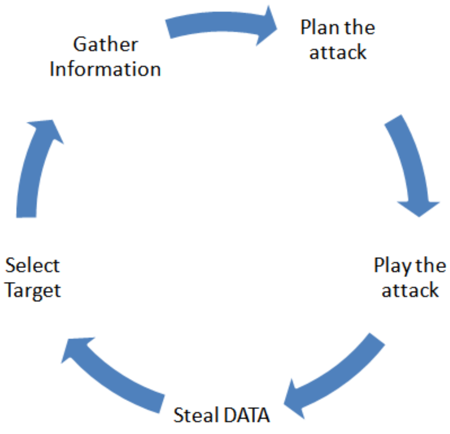

Fig.2. Plan-Attack Cycle [2]

Fig. 2 shows the threat levels that can exist in mobile database application. It can be seen from Fig. 3 that there exist malicious apps and malicious site. Malicious Apps are rogues mobile applications uploaded by hackers on malicious sites with the intention of deceiving the victims to download and install in their mobile devices with the sole intent to steal victim's private data. These malicious apps are usually sandboxed in the JavaScript module of the browser software. Once this JavaScript codes are executed it will trigger the malicious codes or malware to begin to steal victim's information or data.

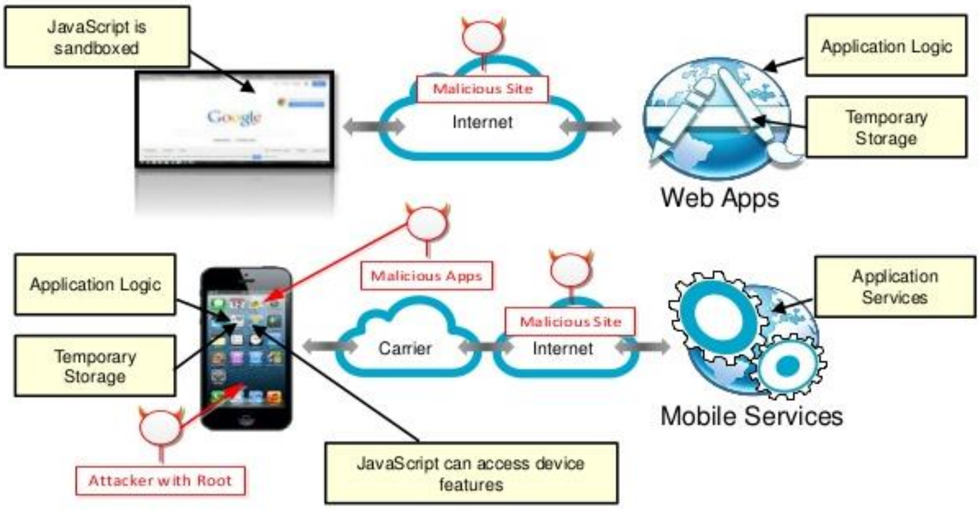

Fig.3. Malicious JavaScript apps uploaded on the browser by hackers to deceive victims

III. RELATED WORKS

This section deals on related works covering different mobile database security schemes to protect mobile database against attacks from malicious codes and hackers.

3.1 Oracle 12c mobile database security

Fig. 4 shows a multi-layered security spanning preventive, detective, and administrative controls. This includes transparent data encryption, data redaction, data masking, privileged user controls, privilege usage analysis, conditional auditing and real application security. Combined with Oracle Audit Vault and Database Firewall, as shown in Fig. 5, Oracle Database 12c provides unprecedented controls to help organizations address existing and emerging security and compliance requirements [3].

Oracle Audit Vault and Database Firewall provide a first line of defense for databases and consolidate audit data from databases, operating systems, and directories. A highly accurate SQL grammar-based technology monitors and blocks unauthorized SQL traffic before it reaches the database. Information from the network is combined with detailed audit information for easy compliance reporting and alerting. With Oracle Audit Vault and Database Firewall, monitoring controls can be easily tailored to meet enterprise security requirements [4]. This is shown in Fig. 5.

Oracle Advanced Security, a commonly used option with Oracle Database Enterprise Edition, provides two important preventive controls to protect sensitive data at the source including database encryption (Transparent Data Encryption (TDE)) and on-the-fly redaction of display data. TDE stops would-be attackers from bypassing the database and reading sensitive information directly from storage by enforcing data-at-rest encryption in the database layer. Data Redaction complements TDE by reducing the risk of unauthorized data exposure in applications, redacting sensitive data before it leaves the database. Together these two controls form the foundation of Oracle's defense-in-depth, multi-layered database security solution. See Fig. 6.

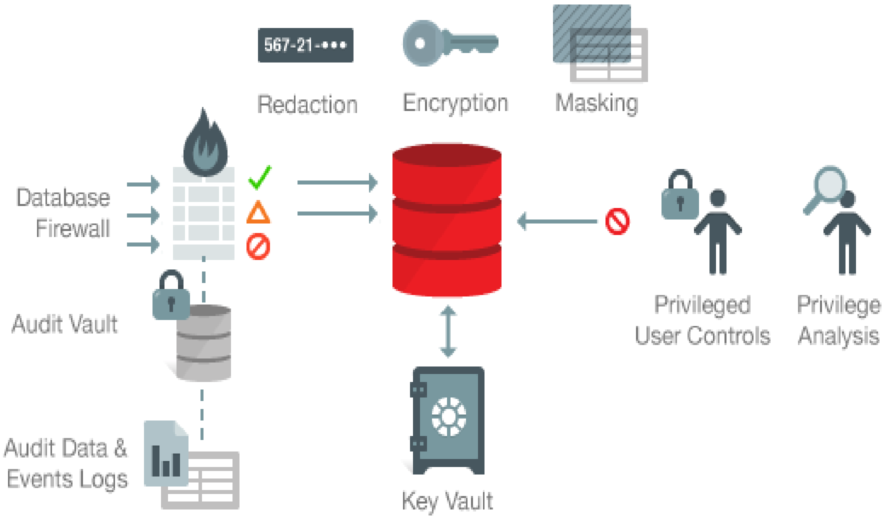

Fig. 4: Oracle 12c mobile database security architecture [3]

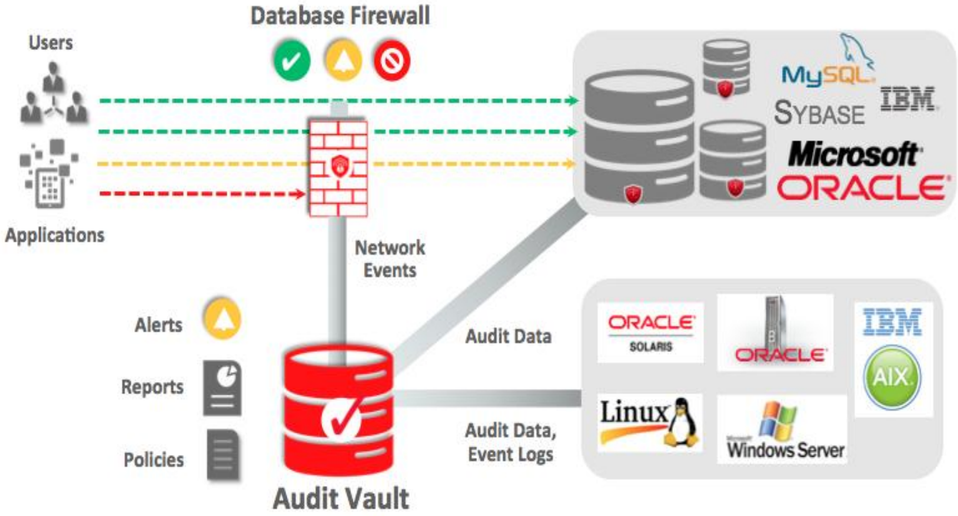

Fig.5: Oracle Audit Vault and Database Firewall [4]

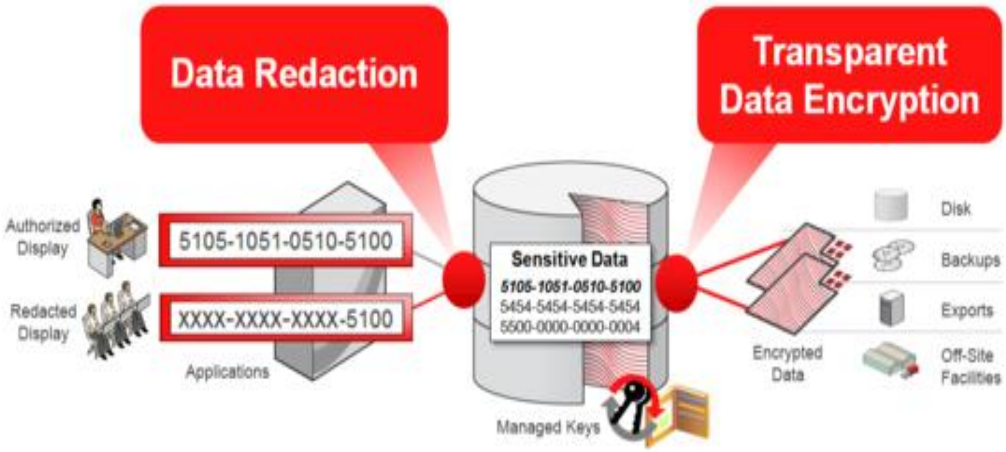

Fig.6: Oracle 12c database security architecture [4]

IV. VARIOUS SCHEMES TO PROTECT CORPORATE NETWORK FROM HACKERS AND MALWARES IN NIGERIA

This section discusses the various possible schemes that can be applied by organizations operating mobile database in Nigeria to protect their corporate data from hackers and malwares' attacks. Such schemes include the following:

1. Protect corporate networks using network protective devices such as firewalls from external hackers.
2. Demilitarized zones (DMZ) server to protect corporate networks from external hackers in public networks. Fig.7, Fig. 8 and Fig.9 show how DMZ and firewall are used to block malicious programs and hackers from gaining access to corporate database server and applications.
3. Encryption of local database, encryption of application server, encryption of network links etc.
4. Authentication and Authorization mechanisms in both database server and web server to control access to the database and application servers as well as the communication links.
5. Enforcement of user access control mechanisms can be used to deter fraudulent employees (hackers within).
6. Use of Ant-virus and Anti-spyware programs can help in stopping the activities of hackers using malicious programs as backdoors.
7. Use of log files or audit trails can be developed and maintained to monitor the activities of internal staff of an organization to prevent or stop insider attack.
8. Company's data should be stored and secured in physically protected servers and data centers and must not be contracted or sourced out to an external service provider.
9. Tunneling and Virtualization can also be used to protect private networks from attacks from hackers. Details can be found here [5].
10. Application provided security by using database triggers to safeguard data manipulation.
11. Applying separate user accounts for authoring and the read-only application to limit access to critical application and database.

4.1.1 DMZ and Firewall

Every business organization is connected via internal private network (intranets) and this private network is in turn connected to a public network (internet) or partner's network (extranet). The database server that stores critical data of the organization is connected to the private network (intranet) of the organization. Employees of the organization are connected to the database server via the client computers or mobile devices. There is an internal security hole or vulnerability here because an employee can be a source of malware which can be used to steal organization's critical data from the database server. Equally, an external security hole can come from hackers or malicious codes over the internet to the organization's corporate private network. As shown in Fig. 7, a demilitarized zone (DMZ) can be created using firewall to block any external attack from hackers or malicious codes from the internet. Also firewall cannot allow the employees access to download and install malwares into the computers or mobile devices (clients). It can also be seen that in Figs. 7, 8 and 9 that firewall can be used to block malicious program from the internet (uploaded by hackers) from entering into the company intranet. The firewall can be a piece of hardware equipment or software.

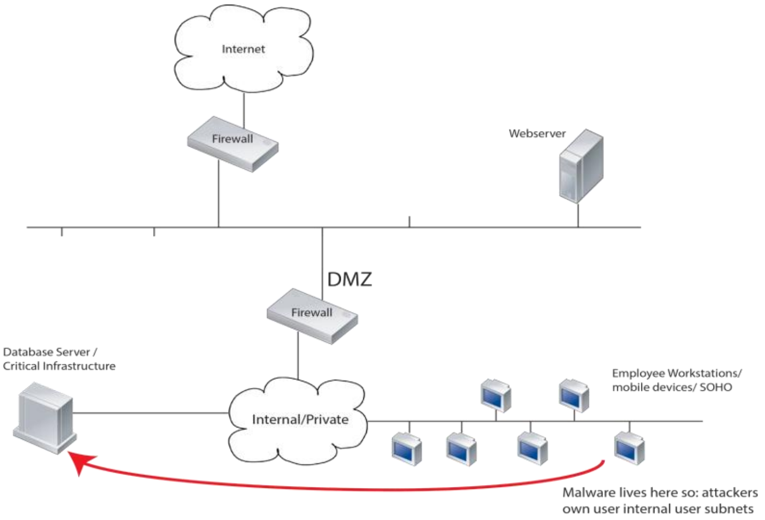

Fig.7. An organization's private network protected by a Demilitarized Zone (DMZ) using firewall

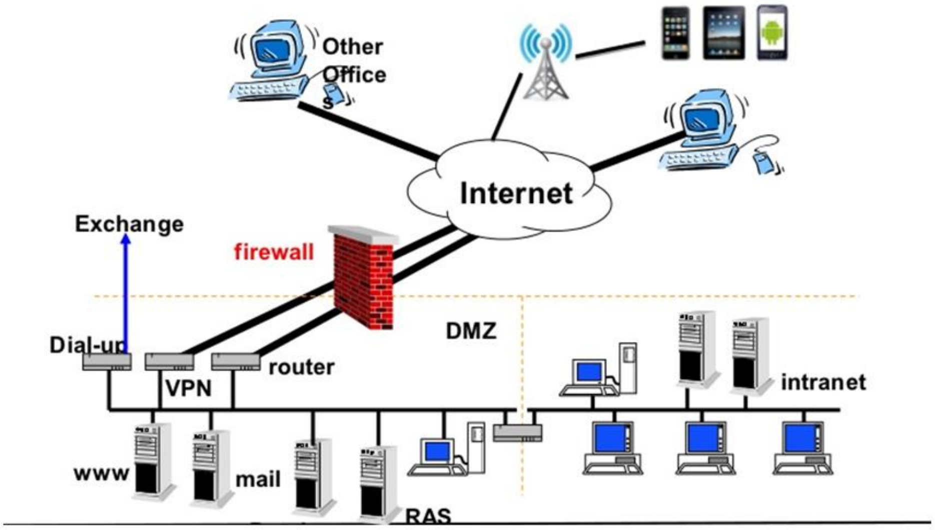

Fig.8. An organization's the Application and database servers protected by a Demilitarized Zone (DMZ) to protect attack from internet and intranet

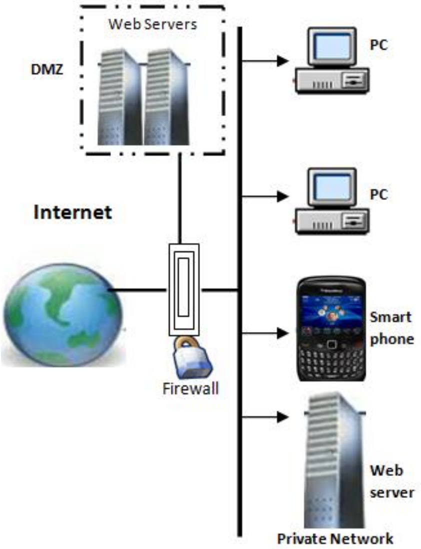

Fig.9. A typical DMZ and firewall securing private network against hackers

4.1.2 *Encryption of the mobile data and mobile database server*

Encryption solves the problem of attack on data privacy, confidentiality and integrity of data. Mobile data such as voice, SMS, MMS, can be attacked during a communication session via the network link by eavesdropping and modification by the man-in-the-middle attack as depicted in Fig. 10. According to [6], the use of encryption and decryption cryptographic process can be used to protect or secure GSM or mobile data – voice, SMS and MMS. To ensure that the mobile SMS data remains confidential, a password-based cipher was used to encrypt the SMS message's content. For SMS mobile data to be a secure or protected during an end-to-end communication session there is need for confidentiality and integrity of the message. Authentication can be achieved by simply looking at the message itself, which includes the sender's phone number. Encrypting the message with a password-cipher, as stated earlier, provides confidentiality while a message digest was used to ensure integrity of the GSM SMS data. Fig. 11 shows clearly the encryption and decryption methodology that can be used to protect mobile users' data engaged in an end-to-end communication session to protect the data from being attacked from insecure network link.

As depicted in Fig. 11, using a key K_1, sender S encrypts message M_1 and sends M. The recipient R receives message and using the key, K, decrypts it into M_2. Provided they share the same password (private key), so that K_1=K_2=K, and no errors happen during transmission, R will recover the message so that M_1=M_2. Public key can also be used for secure mobile communication sessions involving more than two persons and only the genuine recipients can get the secret key and used it to communicate securely. Highly confidential or mission-critical mobile data needs to be protected using encryption and decryption cryptographic transformations protect the data from hackers or malicious codes.

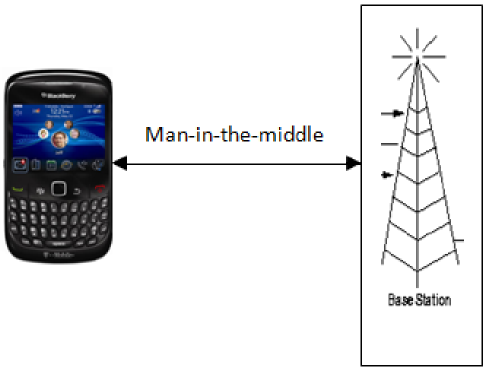

Fig.10. Subscriber with Smart phone to telecommunication network (with man-in-the-middle) attack model

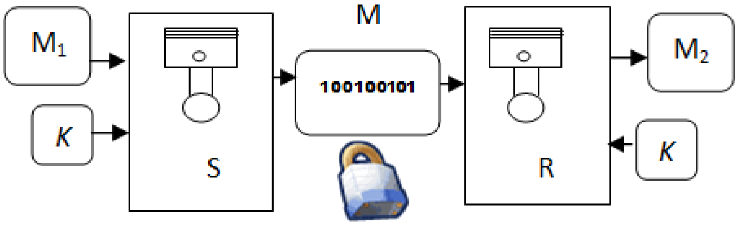

Fig.11. End-to-end encryption and decryption of SMS mobile data [7]

To protect the corporate mobile database server, encryption can also be applied to solve the challenge. This can be done in two ways – inside the Mobile DBMS (MDBMS) and outside the database.

If encryption is done inside the DBMS product, data can be encrypted and decrypted within the database and the process will be transparent to the applications. The data is encrypted as soon as it is stored in the database. Any data that enters or leaves the database, though, will be transmitted as clear text. Encryption generally is implemented within the database through a database procedure call and capabilities measured through database add-ons.

Generally encryption outside of the database depends on the transit between client and server. A more secure solution is moving the encryption to the applications that generate the data. When client-server applications are used, security protocols such as Secure Socket Layer (SSL), sensitive data is in clear text form for the shortest possible time. Encryption is performed within the application that introduces the data into the system; it travels encrypted and can be stored encrypted at its final destination. This provides a good end-to-end data protection, but may require changes to applications to add or modify encryption and decryption capabilities. An Encryption Server provides a centralized encryption services for entire database environment

4.1.3 Authentication and Authorization

Authentication and authorization are good protective security measures to protect internal hackers, i.e. company's employees who may want to compromise the security of the database server via their mobile database device. These measures ensure that only authorized personnel are allowed to have access to the database server and accompanying applications. Security schemes such as username and password, pin codes, biometric solutions can be applied here to enable legitimate authorized users have administrative access to the database servers and accompanying applications.

4.1.4 Audit trail and log files

The implementation of audit trail and log files will help monitor the activities of internal employee of personnel of an organization against any form of attack or compromises against the database server and the data.

4.1.5 Anti-virus and Anti-spyware

The installation and regular updating of anti-virus software and anti-spyware program can help stop the activities of malicious programs such as virus, worms and logic bombs. Anti-spyware can be used to check the activities of spyware which are used by hackers and spammers to hijack and monitor a database server/application remotely in order to steal corporate data.

V. RECOMMENDATIONS

Table 1 summarizes the various recommended holistic solutions to various security challenges to mobile database in Nigeria.

Table 1: Some recommended solutions for various mobile database security challenges

S/N	Security issue	Solutions
1	Unauthorized disclosure of sensitive data as result of device loss or theft or attack to corporate network server	• Use of PIN, PASSWORD, PASS CODE, PASS PATTERN, TOKEN, Biometric factor like fingerprint, Iris recognition, voice recognition etc. • Remote wiping of data • Use LOCK OUT facility of mobile device to lock out unauthorized user when he or she tries more than 5 times to enter the PIN/PASSWORD • The data can be wiped out via remote wiping once device is stolen
2	Interception of data by hackers through Wi-Fi, Bluetooth, etc	• Make sure the Bluetooth and Wi-Fi facilities are turned off when not in use
3.	Attack of critical corporate private network and database over the internet by hackers and malicious codes	• Create Demilitarized Zone (DMZ) using firewalls to block the access to the private network. • Encrypt all transactions relating to the database and applications. • Use authentication to validate authorized database users and network
4.	Attack due to internal employee using mobile device over the private network of the organization	• Create Demilitarized Zone (DMZ) using firewalls to block the access to the private network using malwares and other malicious codes. • Create user accounts and assign privileges to only the authorized employees to access any application and database server. • Create log files to monitor each authorized employee's activities and operations • Use audit trail to monitor every activity or action of company's employee.
5.	Unauthorized access and modification of the data	• Use Encryption • Use Server Authentication and Client Authentication

	during transmission	• Grant/Revoke commands
6.	Destruction of sensitivity of data due to the device corruption	• Use backup and recovery procedures.

VI. SUMMARY AND CONCLUSIONS

In this paper, we pointed out the fact that the majority of corporate organizations in Nigeria and elsewhere now connect their critical data (in their corporate networks) to mobile networks in in order to ease distribution of data. In the event of this data distribution, the corporate data is exposed to a quantum of security vulnerabilities and challenges. Security challenges such as eavesdropping, denial-of-service (DoS) attack, data modification, data corruption or destruction, spoofing and outright stealing of data will become commonplace. The critical corporate data needs to be protected against any of these forms of attack because failure will lead to catastrophic event.

Many research works have been done in tackling these myriads of security challenges using a monolithic solution framework but for the mobile database to be protected full-proof there is need for a holistic security solution. Distributed database security is integral to the design and proper functioning of a distributed database. There are three important pieces to distributed database security- physical, User, and Network. These pieces work in conjunction with policies standards, and procedures. Policies are directions that support a goal. Solutions described above must be applied to a distributed database on a goal. Also, human factor and traits should not be ignored in this system. Because, a user as who one uses this system, would be considered as an effective factor for security.

Therefore, this paper proposed a holistic approach (in three fronts) to solving the mobile database security challenges - firstly protecting the mobile network device itself, secondly the mobile network and finally protecting the corporate network and database server using a variety of solutions such as encryption, cryptographic key management, corporate firewall or Demilitarized Zone (DMZ), user monitoring via log files and audit trail, user control, authorization and authentications and other measures.

REFERENCES

[1]. D. Roselin Selvarani1 and Dr. T. N. Ravi2, A Review on the role of Encryption in Mobile Database Security, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 12, December 2014.

[2]. Trendo Micro, “The rise of smart phones and the usage on the Internet: The security issues and solutions”, Retrieved on December 18, 2012 from http://www.trendmicro.com/us/enterprise/product-security/mobile-security/index.html

[3]. Oracle, Security and Compliance, Comprehensive Defense in Depth, Retrieved online on 20th June 2016 at http://www.oracle.com/technetwork/database/security/index.html

[4]. Oracle, Oracle Audit Vault and Database Firewall, Retrieved online on 20th June 2016 at, http://www.oracle.com/technetwork/database/database-technologies/audit-vault-and-database-firewall/overview/overview-1877404.html

[5]. E. Dulaney, “CompTIA Security+ Study Guide Fourth Edition”, Sybex USA., pp. 29-33.

[6]. F.C. Obodoeze, Cyber Security for GSM Data Protection, Master’s thesis submitted to Department of Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Nigeria., pp.84, November 2010.

[7]. T. Strang, Lecture, Topic: Programming Mobile Devices, Security Aspects, WS2007/2008, University of Innsbruck. pp. 15,18,19,20.

Authors’ Profiles

Fidelis Chukwujekwu Obodoeze is a doctoral research candidate at Department of Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Nigeria. He is about to round off his Ph.D research on oil and gas pipeline physical security using Multi Agent Systems and Wireless Sensor Network. He is currently lecturing at the Department of Computer Engineering Technology Akanu Ibiam Federal Polytechnic Unwana, Nigeria. He specializes in IT & Network Security, IT and Industrial Automation, Wireless Sensor Network and real-time control systems. He can be contacted on the following email fidelisobodoeze@gmail.com.

Lois Onyejere Nwobodo is a lecturer at the Department of Computer Engineering Enugu State University of Science and Technology (ESUT). She is currently doing her doctoral research work at the Department of Electronic & Computer Engineering, Nnamdi Azikiwe University Awka, Nigeria. Her research interests focus on Artificial Intelligence (AI) and control systems. She can be contacted on ifeonyi@yahoo.com.

Samuel Obiji Nwokoro works at the Department of Computer Science, Akanu Ibiam Federal Polytechnic Unwana, Nigeria. His research interests are in Could Computing, Virtual Reality Application and Network Security. He is presently an ICT Technologist II (Network Unit) in the same Institution. He is a member of IEEE and IAENG. He can be contacted on sonwokoro@akanuibiampoly.edu.ng.