INTERNET OF THING (IoT) AND DATABASE SECURITY IN BANKING SECTOR IN UYO METROPOLIS OFAKWA IBOM STATE, NIGERIA

Nseabasi Peter Essien (Ph.D)
&
Stella Stephen Godwin
Department of Industrial Technology Education, Faculty of Education,
University of Uyo, Uyo, Nigeria
godwinstella22@gmail.com

Abstract
The study was conducted to examine the extent to which Internet of Things predicts database security in banking sector in Uyo Metropolis of Akwa Ibom State, Nigeria. Two specific objectives, research questions and null hypotheses were formulated to guide the study. A correlational research design was adopted for the study. The population of the study consisted of 20 Banks Managers and 20 assistants in Uyo Metropolis of Akwa Ibom State in all the 20 banks in Uyo Metropolis. The sample size of this study was 40 Bank Managers. The census technique was adopted by the researcher to use all respondents. Two structured instruments were designed by the researcher titled "Internet of Things Questionnaire (IOTQ) and Database Security in Banking Questionnaire (DBSBQ)". The instrument was subjected to face validation by three experts. A trial testing reliability technique was adopted to establish the internal consistency of the instruments. The instruments were administered on eighty respondents from Banks Managers outside Uyo Metropolis. The data obtained were subjected to analysis using the Cronbach alpha statistical tool which yielded a co-efficient of 0.84 and 0.76 respectively. The data for this study were collected using a structured questionnaire by the researcher. Linear Regression statistical tool was used to answer the research questions and test the null hypotheses at 0.05 level of significance. The finding of this study revealed that there is the Internet of Things significantly predicts database security in banking sector in AkwaI bom State, it was concluded that password, authentication and authorization are significantly predict database security in banking sector in Uyo Metropolis of Akwa Ibom State, Nigeria. It was recommended among others that, banking system should not be left behind in term of security system, and should keep a sharp eye when there any vulnerability in authentication and authorization that may lead to confidentiality, availability and integrity issues.

Keywords: Internet of Things, banking sector, Database Security, Communication and Risk Management

Introduction

Nowadays, internet-based information architecture allows the exchange of services and goods between all elements, equipment, and objects connected to the network. The IoT refers to the networked interconnection of those everyday objects, which are often equipped with some kind of intelligence. In this context, Internet can be also a platform for devices to communicate electronically and share information and specific data with the world around them. (Santomero and Seater, 2016). So, IoT can be seen as a real evolution of what was as known as Internet by adding more extensive

interconnectivity, a better perception of the information and more comprehensive smart services. IoT (internet of things) is a network of devices, appliances, vehicles and others that are embedded with sensors, electronics, software, connectivity and actuators; enabling them to connect and exchange data. IoT devices share data in a wired or wireless network. Inventions of IoT have endless possibilities. It can bring a huge of difference to the world. The impact of IoT is felt most in the business world becaus it has changed the methods of different business operations and so the way the economy is being run. It helps optimize operations, reduce costs, enhance productivity and improve lives (Santomero and Seater, 2016).

The Internet of Things refers to an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world. In the Internet of Things, devices and objects have communication connectivity, either a direct connection to the Internet or mediated through local or wide area networks. The Internet of Things (abbreviated as 'IoT') is a way for devices that can communicate and exchange information by connecting to the Internet. The IoT is an emerging global Internet-based technical architecture facilitating the exchange of goods in a global supply-chain network (Weber, 2010). As the technology trend shifts towards providing faster data rates and lower latency connectivity the Internet is expected to double in size every year and cloud computing can play a key role in that growth. Cloud computing is one of the enabling platforms to support IoT. Most “things” of the real world will be integrated into the virtual world by enabling anytime, anywhere full connectivity.

With the emergence of Wi-Fi (faster speeds of the internet) at lower costs, IoT has emerged as a method to exchange information rapidly by connecting various electronic devices across different locations. This is also called 'Inter-Networking' as it is absolutely based on the internet (Said and Masud, 2013).

The IoT can be seen as a combination of sensors and actuators providing and receiving information that is digitalized and placed into bidirectional networks able to transmit all data to be used by a lot of different services and final users (CharithPerera et. al., 2014).

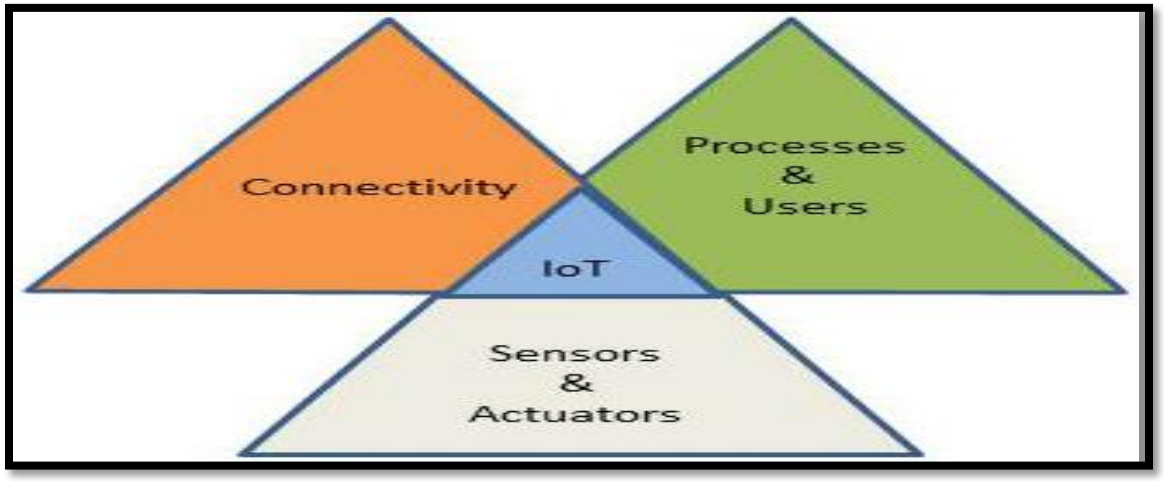

Figure: 1. TheIoT Concept.

Source: CharithPereraet. al. (2014).

Multiple sensors can be attached to an object or device in order to measure a broad range of physical variables or phenomena and then transmit all data to the cloud. The sensing can be understood as a service model. The architecture of IoT systems can be divided into four layers: Object sensing layer, data exchange layer, information integration layer, and application service layer (Ma, 2011). Smart devices can be already connected through the traditional Internet. However, the IoT incorporates the sensing layer which reduces the requirements on the capability of those devices and enables the interconnection among them. Sensor data consumers communicate with sensors or sensors through the information integration layer that is responsible of all the communication and transactions.

Meanwhile, new requirements and challenges to data exchange, information filtering, and integration, the definition of new services to users, as well as the complexity of the network architecture Moreover, the use of cloud technologies is exponentially growing. New infrastructure platforms and software applications are offered in the frame of the IoT. Some of the major advantages and benefits of the IoT will be the creation of innovative services with improved performance and value-added solutions along with the reduction of data acquisition costs of existing services and the opportunity to create new revenue streams in a context of a sustainable business model. These applications can be oriented to consume businesses, commercial survey activities, and the industrial and scientific community by harnessing the application developers.

The IoT sensors can be smart sensors, actuators, or wearable sensing devices. For example, companies like Wemo, revolve and Smart Things offer smart hubs and mobile applications that enable people to monitor and control thousands of smart devices and appliances inside buildings using their smartphones (Rushden, 2012) as indicated in Figure 2

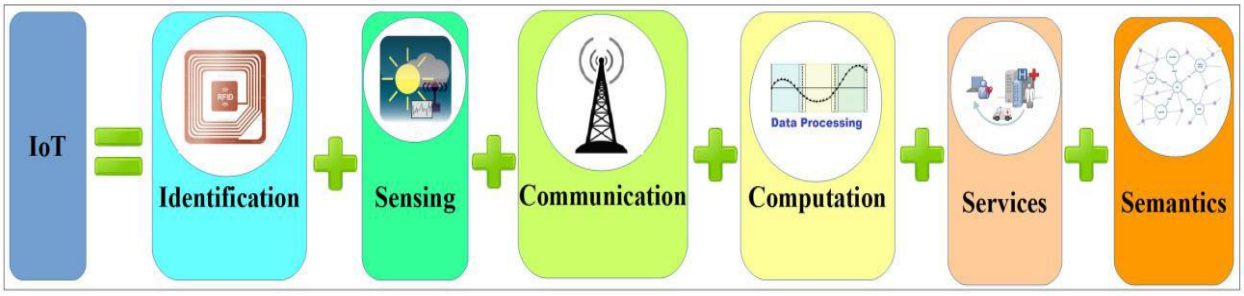

Figure 2. The IoT elements
Source: Rushden, U. (2012).

The advancement in Technology has played an important role in improving service delivery standards in the Banking industry. In its simplest form, Automated Teller Machines (ATMs) and deposit machines now allow consumers to carry out banking transactions beyond banking hours. Misuse of debit/credit cards can be prevented by having IoT-enabled security systems at points of use, such as ATMs, which have more personal and secure methods of authorization. Citigroup is testing ATMs that use eye-scanning technology to authenticate transactions. Banks constantly aim to expand their network of offices and ATMs, while also managing the existing units with maximum efficiency.

Using IoT-enabled monitoring to track the number of customer units per day, the average queue time can be measured to determine the optimal number of personnel and counters at each branch. Decisions regarding new branches can also be made easier by using the distribution data of customers with respect to geography. The same can be done to optimize the number and location of cash dispensing machines based on usage (Vijay, 2019).

Collecting debt from individual and enterprise borrowers involves considerable effort and overhead costs for lending financial institutions. Monitoring the operations and supply chain activity of debtor businesses using IoT sensors and networks can help FSIs to determine their readiness to pay without involving excessive overhead costs, associated with cheque failures. Similarly, an IoT network of ATMs, card readers other point-of-sale devices can be used to assess a borrower's expenditure and income for determining their ability and intent to repay and further expenditure by defaulters can be curbed until repayment (Vijay, 2019).

Database security may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via a dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer or network. However, electronic banking system users still face security risks with unauthorized access to their banking accounts. Moreover, electronic banking system users are also concerned about non-reliability which requires reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transactions can be altered to change the apparent sender. Therefore, it is extremely important to build in non-reputability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.

Authentication is defined as the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party. Authentication in an Internet Banking Environment which provided risk management practices for financial institutions offering Internet-based products and services. Authentication is the process of confirming one's identity. Two-factor authentication or 2FA is a way of login where a user is required to provide additional information to sign in than just the password. Using only the password to login enables malicious attackers to have easy access into the system as it represents a single piece of information only (Sabzevar and Stavrou, 2018). In authentication systems, all the transmission of data from a user's smart object to the online server can be exposed to unwanted personnel through interception. As such, from a security standpoint, the most common authentication systems fail to guarantee a fail-safe method for keeping the login information away from the hands of the public for maintaining privacy and security for the user. With the increasing use of mobile devices by consumers for banking, and shopping (Acharya, et. al., 2013) etc. the need for security concerns have emerged which in turn has created an interest in multi-factor authentication. In case of multi-factor authentication, which requires more than one form of authentication for verification of legitimacy, provides an additional layer of

protection against security breach. Here apart from providing username and password by the user, an additional authentication code is sent to the user's mobile device (Sabzevar and Stavrou, 2018) for verification. These factors taken together provide increased security of accounts. Yet such multi factor authentication systems are not applicable in the Internet of Things architecture.

Internet banking systems must authenticate users before granting them access to particular services. More precisely the banking system must determine whether a user is, in fact, who he or she claims to be by asking for direct or indirect proof of knowledge about some sort of secret or credential. With the assumption that only an authentic user can provide such answers, successful authentication eventually enables users to access their private information.

Authentication is not enough to grant users access on its own. Authorization is the next step in the procedure. Authorization is the process by which a computer system or individual grants access to a user for various reasons. The user must first authenticate him to the system. The system will then check the user's authorization and decide if that user has sufficient access to the resource he is trying to access. Only then will the system grant the user access to the resource.

Authorization requires that every transaction in the bank takes place after confirming the identity of the person initiating the transaction. This applies to customers logging in to online or mobile banking systems, to those visiting the bank in person, or those using credit/debit cards at POS terminals and ATM's. It also applies to bank employees who have access to customers and banks data. While earlier authentication simply required an Id and a password or PIN, many banks have now implemented two-factor and multi-factor authentication to ensure that the person is actually who he/she claims to be. Banks are also using biometric authentication techniques to verify customers' identity including behavioural biometrics when they interact with banking systems like IVR (Sabzevar and Stavrou, 2018).

Confidentiality and the integrity of the data in the system would likely been violated whenever there are security data breaches, done by unauthorized person. The data might loss its confidentiality when this unauthorized person view, alter or steal the personal information of the customer or the information security of the organization uses. The integrity of the system can also be affected, when these irresponsible people alter and changing the data information in the system, for example exchange a sum of money to their own account (Prinz, 2019)

In order to maintain segregation of duties, banks need to strictly control authorisation and access privileges. Failure to provide adequate authorisation control could allow individuals to alter their authority, circumvent segregation and gain access to e-banking systems, databases or applications to which they are not privileged. In e-banking systems, the authorisations and access rights can be established in either a centralised or distributed manner within a bank and are generally stored in databases. The protection of those databases from tampering or corruption is therefore essential for effective authorisation control (Press, 2017). The study of Roland (2004) revealed that authentication "requires users to prove that they really are who they say they are" before authorization can takes place, and it also governs what the user can access

The bank authority is prompted to Enter the password using the keypad, the password entered by the bank authority is matched with the predefined set password, consecutively three attempts will be given for entering the correct password, failing to enter the correct password then that person will be considered as unauthorized user and photo will be captured and red led starts blinking and alarm will turn on.

Using passwords for authentication is the simple idea. Assign a unique identifier to a user and instruct that user to supply a password to correlate to that identifier. The administration is also pretty simple. Almost all computer systems have built-in applications to handle passwords. The user identifiers and passwords can be stored in a database allowing the entire process to be completed with the user as the only source of human input (He, 2013)

Surely many problems can be identified with this technique. Username and password combinations have a fundamental flaw stemming from human psychology. Passwords should be easy to remember and be easy enough to provide swift authentication. On the other hand, in terms of security the password should be difficult to guess, changed from time to time, and unique to a single account. (Sabzevar and Stavrou, 2018) Because of these requirements, many people feel the need to physically record their password (often times in close proximity to the authentication device). Furthermore, as technology increases, attacks targeting passwords are becoming easier to implement. High powered computers make it quite efficient to initiate dictionary and brute force attacks to obtain the password.

Passwords are highly susceptible to man in the middle attacks and if someone simply watches you enter the code. Since passwords are still vastly implemented in computer systems, there are some best practices for their creation. Passwords should be alphanumeric, meaning that they require both letters and numbers to be valid. They should also have a minimum length. Six characters seem to be a generally accepted minimum but more and more systems are moving to 8 characters minimum. For added security, passwords should also encompass special characters like the asterisk (*), semi-colon (;), or dollar sign ($) (Roland, 2014).

A password is a secret word or alphanumeric text that is shared by the verifier and the customer. It is usual for the verifier to keep the passwords protected on their system by storing them in encrypted or hashed form and in this form, they may still be used in the authentication process (Nwaze, 2016). So, the verifier usually has encoded copies of the passwords. Passwords are normally made up from the characters available on a standard keyboard. In Nigeria today, most banks conduct their transactions with the use of username-passwords, pass phrases or PIN numbers (figure 3).

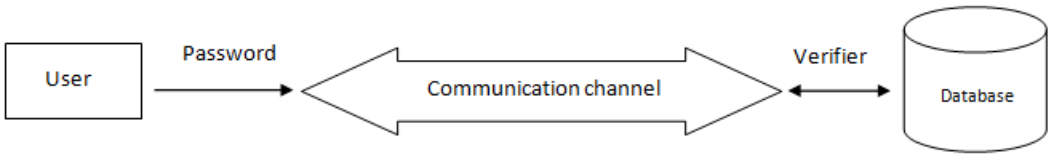

Figure 3. Password Model

Source: Nwaze (2016)

Nwaze (2016) examine Information Communication Technology, password and data Prevention in the Banking industry in Nigeria, their responses were critically analyzed and the study concluded that the introduction of password Number with the aid of internet of things technology is an effective tool that will reduce the incidence of fraud to the barest minimum in Nigeria.

Statement of the Problem

The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer or network. However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the electronic banking system users also concern about non-reputability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non-reputability which means that the identity of both the sender and the receiver can be attested to by a trusted third party. This scenario gave the researcher the impetus to examine the extent internet of things predict database security in banking sector in AkwaIbom State.

Purpose of the Study

The main purpose was to examine the extent internet of things predict database security in banking sector in AkwaIbom State. Specifically, the study sought to:

i. Examine the extent authentication predicts database security in banking sector in Akwa Ibom State.
ii. Examine the extent authorization predicts database security in banking sector in Akwa Ibom State.
iii. Examine the extent password predicts database security in banking sector in Akwa Ibom State.

Research Questions

The following research questions were adopted to guide the study:

i. What is the extent authentication predicts database security in banking sector in Akwa Ibom State?
ii. What is the extent authorization predicts database security in banking sector in Akwa Ibom State?
iii. What is the extent password predicts database security in banking sector in Akwa Ibom State.?

Research Hypotheses

The following null hypotheses were tested at 0.05 level of significance:

i. Authentication does not significantly predict database security in banking sector in Akwa Ibom State.
ii. Authorization does not significantly predict database security in banking sector in Akwa Ibom State.
iii. Password does not significantly predict database security in banking sector in Akwa Ibom State.

Research Method

Design of the Study

The study adopted a Correlational design. The design will enable the researcher.

Population of the Study

The population of the study consisted of 20Bank Managers, 20 assistants in 20 banks in Uyo Metropolis of Akwa Ibom state which include: Access Bank Nigeria Limited, Diamond Bank Nigeria Limited, Ecobank Nigeria Plc, First Bank Nigeria Plc, First City Monument Bank (FCMB) Plc, Guaranty Trust Bank plc, Heritage Bank, Keystone Bank Limited (Formerly Bank PHB), Skye Bank Nigeria Ltd., Stanbic IBTC Bank Ltd., Sterling Bank Nigeria Ltd., Union Bank of Nigeria Plc., United Bank For Africa Plc. (UBA), Wema Bank Plc, Unity Bank, Zenith Bank Plc and Polaris bank.

Sample size of the study

The sample size of this study was 40Bank Managers. Census technique was adopted by the researcher to use all respondents.

Instrumentation

Two structured instruments were designed by the researcher titled “Internet of Things Questionnaire (IOTQ) and Data-Based Security in Banking Questionnaire (DBSBQ)”. Four-point rating scale was adopted: strongly Agree (SA) =1, Agree (A) =2, strongly disagree (SD) =3, Disagree(D) =4.

Validation of the Instrument

The instrument was subjected to face validation by three experts.

Reliability of the Instrument

Trial testing reliability technique was adopted to establish the internal consistency of the instrument. The instruments were administered on twenty respondents (8) from Banks from Managers outside Uyo Metropolis. The data obtained were subjected to analysis using the Cronbach alpha statistical tool which yielded a co-efficient of 0.84 and 0.76 respectively.

Method of Data Collection

The data for this study were collected using a structured questionnaire, personally administered by the researcher.

Method of Data Analysis

Linear Regression statistical tool was used to answer the research questions and test the null hypotheses at 0.05 level of significance. The probability value (p) was used to test the null hypotheses; the p-value was compared with 0.05 when ($p \leq 0.05$) less than or equal to 0.05, the null hypothesis (Ho) is rejected. On the other hand, when the p-value is greater than ($p > 0.05$) the 0.05, the null hypothesis is retained.

Results and Discussion

Research Question 1

What is the extent to which authentication predicts database security in the banking sector in Akwa Ibom State?

Table 1: Result of the Extent to which Authentication Predicts Database Security in Banking Sector in Akwa Ibom State

Variable	R	R^2	Adjusted R Square	Std. Error	Remark
Authentication and database security	.714	.702	.599	.19946	Very strong Prediction

Field Survey, 2021

The result in Table 1 indicates the strength of the extent to which authenticationpredicts database security in banking sector in AkwaIbom State. The result indicates a Very strong prediction with r-value.714. This implies that authenticationis effective in predictingdatabase security in banking sector in AkwaIbom State. However the table further shows the coefficient of determination as .702 indicating that 70.2% of the variation in database security in banking sector in AkwaIbom State can be attributed to authentication.

Research Question 2

What is the extent to which authorization predicts database security in the banking sector in Akwa Ibom State?

Table 2: **The Result on the Extent to whichAuthorization Predicts Database Security In Banking Sector In AkwaIbom State**

Variable	R	R^2	Adjusted R Square	Std. Error	Remark
Authorization database security	.897	.756	.653	.28430	Very strong prediction

Field Survey, 2021

The result in Table 2 indicates the strength of the extent to which authorization predicts database security in the banking sector in Akwa Ibom State. The result indicates a Very Strong prediction with r-value 897. This implies that authorization is effective in predicting database security in the banking sector in Akwa Ibom State. However, the table further shows the coefficient of

determination as .756 indicating that 75.6% of the variation in database security in the banking sector in Akwa Ibom State can be attributed to authorization.

Research Question 3

What is the extent to which password predicts database security in the banking sector in Akwa Ibom State?

Table 2: **The Result on the Extent to which Password Predicts Database Security in Banking Sector in AkwaI bom State**

Variable	R	R^2	Adjusted R Square	Std. Error	Remark
Password and database security	.675	.455	.441	.38223	Very strong prediction

Field Survey, 2021

The result in Table 3 indicates the strength of the extent to which password predicts database security in the banking sector in Akwa Ibom State. The result indicates a Very Strong prediction with r-value of .675. This implies that password is effective in predicting database security in the banking sector in Akwa Ibom State. However, the table further shows the coefficient of determination as .455 indicating that 45.5% of the variation in database security in banking sector in AkwaIbom State can be attributed to password.

Hypothesis 1

Authenticationdoes not significantly predict database security in banking sector in AkwaIbom State.

Table 4: Simple linear Regression Analysis of authenticationand Database Security in Banking Sector

Source of variation	**Sum of Squares**	**df**	**Mean Square**	**F**	**p-value**	**Remark**
Regression	67.938	1	47.938	108.422	.002	**Sig.**
Residual	76.107	38	.469			
Total	134.045	40				

Field Survey, 2021

The result in Table 4 shows the how authenticationpredicts database security in banking sector in AkwaIbom State. The table further indicates the F. Value as 108.422, and a p-value of .002. Since the p-value .002 is less than 0.05 (.002< 0.05) the null hypothesis is rejected and therefore, be concluded that authenticationsignificantlypredict database security in banking sector in AkwaIbom State

Hypothesis 2

Authorization does not significantlypredict database security in banking sector in AkwaIbom State

Table 4: Simple linear Regression Analysis of Authorizationand Database Security in Banking Sector

Source of	**Sum of Squares**	**df**	**Mean**	**F**	**p-value**	**Remark**

variation			Square			
Regression	55.630	1	55.630	67.446	.000	**Sig.**
Residual	62.415	38	.468			
Total	117.045	40				

Field Survey, 2021

The result in Table 4 shows how authorization predicts database security in banking sector in AkwaIbom State. The table further indicates the F. Value as 67.446, and a p-value of .000. Since the p-value .000 is less than 0.05 (.000 < 0.05) the null hypothesis is rejected and therefore, be concluded that authorization significantly predict database security in banking sector in Akwa Ibom State**.**

Hypothesis 3

Password does not significantly predict database security in banking sector in Akwa Ibom State

Table 4: Simple linear Regression Analysis of Passwordand Database Security in Banking Sector

Source of variation	Sum of Squares	df	Mean Square	F	p-value	Remark
Regression	14.745	1	14.745	31.783	.000	Sig.
Residual	17.630	38	.464			
Total	32.375	39				

Field Survey, 2021

The result in Table 4 shows how authorization predicts database security in banking sector in AkwaIbom State. The table further indicates the F. Value as 31.783, and a p-value of .000. Since the p-value .000 is less than 0.05 (.000 < 0.05) the null hypothesis is rejected and therefore, be concluded that authorization significantly predicts database security in banking sector in Akwa Ibom State**.**

Findings of the Study

i. The result indicates that authentication is effective in predicting database security in banking sector in Akwa Ibom State.
ii. The result indicates that authorization is effective in predicting database security in banking sector in Akwa Ibom State.
iii. The result revealed that password is effective in predicting database security in banking sector in Akwa Ibom State.
iv. That authentication significantly predicts database security in banking sector in Akwa Ibom State.
v. That authorization significantly predicts database security in banking sector in Akwa Ibom State.
vi. That password significantly predicts database security in banking sector in Akwa Ibom State.

Discussion of Findings

Research question 1 indicates that authentication is effective in predicting database security in banking sector in Akwa Ibom State, with a corresponding hypothesis that authentication significantly predict database security in banking sector in Akwa Ibom State. This implies that authentication is the automation of processes, controls, and information production using computers, telecommunications, software, and ancillary equipment such as automated teller machines and debit cards. It is a term that generally covers the harnessing of electronic technology for the information needs of a business at all levels. This finding is supported by the finding of Crosby and Vafa (2013) who concluded that authentication in an Internet Banking Environment provided risk management practices for financial institutions offering Internet-based products and services. The finding also conforms with the finding of Ghosh, et.al., (2010) whose finding revealed that LTE-A (LTE Advanced) is an improved version of LTE including bandwidth extension which supports up to 100 MHz, downlink and uplink spatial multiplexing, extended coverage, higher throughput and lower latencies.

Research question 2 indicates that authorization is effective in predicting database security in banking sector and that authorization significantly predicts database security in banking sector in Akwa Ibom State. This is because to protect the data in a security system, administrators should be able to, among other things, implement detailed user access privileges, and select the information that can be shared internally with partners and authorities, and control how long data is kept. This finding is supported by the finding of Roland (2014) revealed that authentication "requires users to prove that they really are who they say they are" before authorization can takes place, and it also governs what the user can access.

Research question 2 indicates that password is effective in predicting database security in banking sector and that password significantly predicts database security in banking sector in Akwa Ibom State. This is because when it comes to your finances, password protection is essential to keeping your personal information secure. Without a strong password, you put yourself at risk for fraud. This finding supports the finding of Reyns (2013). who reported that Loss of password or stolen identification, resulting from identity theft is the ticket for the criminal or unauthorized individual to simply get the authentication needed for their own benefits. From the case example provided, the loss of credit card information for the financial institution is mostly due to the lack of authentication and poor authorization itself which can lead to data breaches. Without proper authentication and authorization, an individual can act by entering the system illegally, and thus taking any information they want. That is why authentication and authorization being the utmost importance to protect any information system, especially when running a financial institution.

Conclusion

Based on the findings of the study, it was concluded that; there is a significant relationship between authentication, authorization and password and database security in banking sector in AkwaIbom State.

Recommendations

i. Financial industry such as bankshould provide the best security systems that can meet customer's expectation and attract prospective customers to use internet to keep their personal data, information and most importantly their money.
ii. Although there is always vulnerabilities occur around the time, banking system should have a backup plan or other shields in order to handle any malicious behavior, that intend to violate the customer's information.
iii. Banking system should not be left behind in term of security system, and should keep a sharp eye when there any vulnerability in authentication and authorization that may lead to confidentiality, availability and integrity issues.

References

Acharya S., Polawar, A, and P. Pawar P. (2013). Two factor authentication using smartphone generated one time password, IOSR *Journal of Computer Engineering*, (IOSR-JCE), 11(2): 85-90.

CharithPereraet. al. (2014).Sensing as a Service Model for Smart Cities Supported byComputer Law & Security Review 26: 23-30.

Crosby, G. V. and Vafa, F. (2013). Wireless sensor networks and lte-a network convergence. In 38th Conference on Local Computer Networks (LCN). IEEE, Sydney, NSW, pp. 731–734.

Ghosh S, et al. (2010) Translational competence of ribosomes released from a premature termination codon is modulated by NMD factors. *RNA* 16(9):1832-47

He, R. C. (2013)..Proximity MIT Card Raises, Allays Security Concerns.*The Tech*, 123(62).

Ma H. D. (2011). "Internet of things: Objectives and scientific challenges". *Journal of Computer Networks*, vol. 5(1):1–17.

Press, G. (2017), "Equifax and SAS leverage AI and deep learning to improve consumer

Prinz, A., (2019). Money in the Real and the Virtual World; E-Money, C-Money, and the Demand for CB-Money, Netnomics, 1: 11-35.

Reyns B.W. (2013). Online routines and identity theft victimization: further expanding routine activity theory beyond direct-contact offenses. J. Res. Crime Delinquency.50(2):216–238.

Roland, J. (2014). *CCSP Self-study: Securing Cisco IOS networks (SECUR)*. Indianapolis, IN: Cisco Press.

Rushden, U. (2012). Belkin brings your home to your fingertips with WeMo Home Automation System," *Press Room Belkin*

Sabzevar, A.P. and Stavrou A (2018). "Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).

Said O. and Masud M. (2013). "Towards internet of things: survey and future vision," *International Journal of Computer Networks*, vol. 5(1):1–17.

Santomero, A.M., and Seater J.J., (2016). Alternative Monies and the Demand for Media of Exchange, *Journal of Money, Credit and Banking*, 28: 942-60.

Santomero, A.M., and Seater J.J., (2016).The Market for Electronic CashCards, *Journal of Money, Credit and Banking*, 34: 299-314.

Vijay K. S, (2019). IoT Applications in Finance and Banking.*International Journal of Research and Analytical Reviews,* (IJRAR), 6(2): 911-953.

Weber, R. H, (2010). Internet of Things - New Security and Privacy Challenges.