Biometrics and Fraud Control in the Akwa Ibom State Civil Service

Ubong E. Umoh
Department of Political Science & Public Administration,
University of Uyo, Uyo
Tel: +2348033860687; Email: father.umoh@gmail.com

&

Michael E. Ekpo
Department of Political Science & Public Administration,
University of Uyo, Uyo
Tel: +2348037609650; Email: ekpomichael@ymail.com

Abstract:

Fraud has been on the increase in the Akwa Ibom State civil service due to the lack of proper identification mechanisms for employees who commit identity deception. This led to the adoption of biometrics to control the incidences of identity deception and corruption. This study set out to assess the effects of biometrics on fraud control in selected ministries, departments and agencies (MDAs) of the Akwa Ibom State civil service. To achieve this objective, a survey research design was adopted and data was gathered from a primary source. Findings indicated that there is a significant relationship between employee identity numbers, electronic payroll system and fraud control in Akwa Ibom State Civil Service. From what was found, feasibility concerns, lack of privacy concerns, application issues, data leaks, and the issue of harnessing EIN with NIN, among others, posed great challenges to the implementation of biometrics. It was concluded that the biometrics system successfully established an accurate and digitized database of pensioners, and eliminated duplicate payments, ghost pensioners and underpayments. It was therefore recommended that government should ensure that every employee in the civil service has an Employee Identity Number (EIN) to ensure continuity, maintenance and adequacy in employees' records.

Keywords: Biometrics, Fraud Control, Civil Service, Employee Identity Number, Payroll System

1. Introduction

The civil service constitutes a major pillar in determining the development and stability of a state. This is because the sector is the engine for the processing of the vastly acquired and expanded government responsibilities of executing public policies and projects and rendering essential services to the people. It is in recognition of this function that various administrations have attempted to reposition the sector for effective and efficient service delivery through various reforms (Olugbemi, 2017). While high productivity in the civil service is a major aim and a determining factor for the success and existence of the state, the bid to attain higher productivity has remained a mirage as fraud, forgery, nepotism, corruption and bureaucratic inefficiency continue to raise serious concerns. These hinder the smooth operations of the entire civil service and have negatively affected the efficient delivery of public goods and services to the citizens (Darma & Ali, 2014).

The civil service, being a principal determinant of the effectiveness and productivity of any government, cannot function without the workforce (Umoh, 2022). In other words, the success or failure of the civil service depends heavily on the effectiveness and productivity of the workers. Workers therefore must be effectively maintained and coordinated and their duties clearly defined

to avoid redundancy. To achieve this, there must be effective manpower forecast and planning. To have effective manpower forecast and planning, there must be a central database to determine existing and potential workers concerning their skills, talents, capabilities, potentials, strengths and weaknesses. It is therefore important that digital biometric identity systems be used by the government with a "do no harm mandate", and the establishment of regulatory enforcement and restorative frameworks ensuring data protection and privacy needs (Umoh, 2022).

The civil servants in Akwa Ibom State, in particular, have all been captured through biometric technology to enable the government to control fraud and the menace of ghost workers in the civil service. In the past years, specifically, between 2016 and 2019, Akwa Ibom State recorded an increase in its wage bill without a corresponding increase in the workforce. This resulted in the State's over-bloated wage bill for civil servants, with over nine thousand (9000) ghost (fake) workers on the payroll. This situation aroused government curiosity to ascertain the actual workforce through various exercises such as biometric capturing, personnel verification and the use of table payment. It was discovered that most workers were receiving salaries at more than one pay point, thus, the need to properly identify all staff through biometric and verification exercises became imperative. Consequently, the biometric programme was introduced in Akwa Ibom State public service on 15th April 2017 when the State Governor, Udom Emmanuel disapproved the bloated salary bill presented to him. Pieces of evidence from these exercises showed that many workers whose names appeared on the payroll were fictitious. This is a fraudulent act and constitutes a criminal offence going by the law.
(AISG, 2020)

Specifically, all civil servants in Akwa Ibom State now have a Biometric Identity Number to be uniquely identified as civil servants. This is because ghost worker fraud has been a chronic problem. Billions of naira are pumped out annually from the government treasury through salary payments to non-existing employees who are fraudulently listed in the payroll. Some of these employees include retired civil servants, the deceased or pure fictitious names. One major reason behind the rise in unqualified and non-eligible individuals on the payroll is the absence of accountability which allows corrupt civil servants to manipulate government expenditures through the placement of ghost workers on the payroll. There was therefore the need to put a mechanism in place to check these problems.

2. Statement of the Problem

The civil service provides the machinery and acts as a springboard for the development, and consolidation of programmes and policies of the government. However, these realities are far from being achieved in Akwa Ibom State Civil Service largely due to widespread corruption. It was observed that some unscrupulous civil servants included names of non-existing workers (ghost names) in the payroll of the government for pecuniary gains. This accounted for the loss of billions of naira due to over-bloated recurrent expenditure at the expense of capital expenditure and significantly weakened the State's capacity to function optimally. This practice was common at the State Ministries, Departments and Agencies (MDAs), as well as the local government level. In each of these levels, names of non-existing workers were stuffed up the payroll as ghosts that were paid salaries for doing nothing (Alade & Oguntuase, 2019). Furthermore, each of the MDAs tended to work in isolation, each with its database of beneficiaries often not digitized which could not be merged with others. These databases typically contained data entry mistakes as well as duplicate and dead entries causing substantial mis-targeting of beneficiaries and pilferage in the delivery of public services and controlling fraudulent activities (Magnet, 2018). The duplication of work due to parallel identity registries created significant inefficiencies: First, the MDAs duplicated biometric enrolment, to uniquely identify each employee. Second, the MDAs duplicated fiscal spending. Third, without a modern, integrated identity ecosystem, the delivery

and management of services, both public and private, are affected. These seriously affected the identity management database of civil service in Akwa Ibom State – the reason for the adoption of a biometric identity system in the civil service.

According to Babalobi (2008), fraud in the civil service is a major factor in the wastage and mismanagement of public funds, blockage of merit employment, leakage of government resources and sabotage. In present-day society, there is a problem of inequality in the distribution of wealth where only a few privileged members of society amass the wealth, leaving a greater percentage with no option of survival. As such, some civil servants turn to salary fraud in an attempt to achieve the objective of a better life. Over the years, previous and current governments at all levels have unconsciously encouraged fraud because of the unwillingness of the government to arrest and prosecute the syndicates involved in corrupt practices (Toakodi, 2014). The syndicates have increased the monthly wage bill to a staggering N5.46 billion for civil servants alone, a trend that has gravely undermined the capacity of the state government to carry out its developmental functions effectively (Dickson, 2020). This is because payroll fraud appears to have blocked channels to the socio-economic development of the state. Biometric technology was therefore adopted to combat fraud and security breaches, secure confidential data, reduce costs and improve the overall employee experience. It is because of the above that this paper aims at finding out the major challenges of biometrics in fraud control in some selected MDAs of Akwa Ibom State Civil Service.

Two null hypotheses were developed to guide the paper:

1. There is no significant relationship between employee identification numbers and fraud control in Akwa Ibom State Civil Service.
2. There is no significant relationship between the electronic payroll system and fraud control in Akwa Ibom State Civil Service.

3. Theoretical Framework

This paper adopts the Max Weber "Ideal Bureaucratic Model" to explain the relationship between biometrics and fraud control in the civil service. The model owes its existence to Max Weber's magnum opus *Economy and Society* published in 1922. This is because, in modern times, the complexity within civilization is ever-increasing and therefore the demands from the administration are also getting complex.

The model has its foundation in the legal-rational authority which characterizes the modern liberal states. The legal-rational authority upholds that individuals or institutions have powers emanating from the legal offices that they hold. Once they leave, the power is lost as the power is associated with the office and not the office holder. The writing of constitutions and documents, establishment of offices and institutions and holding of elections are all in conformity to this kind of authority practised by political systems in mature states. Weber refers to this legal-rational authority as the bureaucracy (Weber, 1905).

This paper adopts this model on the assumption that a man who naturally dislikes work but wants economic reward must be regulated by a set of rules and order in his workplace. This use of coercive authority would enhance efficient performance in organizations (Mulder, 2017) (Kumar, 2019). The Akwa Ibom State civil service is a large organization whose activities are accountable for and also operates in a specialized form. hence bureaucracy is relevant to the service.

In application, Weber's bureaucratic theory summarizes that the civil service is efficient in achieving objectives such as service delivery if and only if it is bureaucratic with proper means of identification. The civil service spells out a schedule of duties for every worker which also makes fraudulent activities to be traceable and easily controlled. This is achieved largely because the

theory came out with terms such as chain of command, unity of command, span of control and functional specificity in the provision of services.

Fraud in the civil service can be controlled to a significant extent if:

1. It has a legal-rational leader;
2. Positions are hierarchically organized;
3. Division of labour and specialization are emphasized;
4. Tasks are performed under laid down procedures and methods.
5. There are proper and unique means of identifying every employee in the workplace.

The pursuance of these requirements makes organizations a well-defined hierarchy of control with clearly outlined functions for each unit. This makes fraud traceable, while in turn, making output the ultimate objective of an organization in service delivery.

4. Conceptual Clarification

4.1 Fraud

To Taiwo and Akintola, (2017), fraud is a deliberate deception carried out to secure something by taking unfair advantage of others. This can be done through cheating dishonestly or duplication or imposition.

Benjamin (2018) defines fraud as a conscious and premeditated action taken by a person or group of people to derive selfish personal monetary gain. It involves the use of deceit and trickery to forge or falsify documents and signatures to steal.

Common features which give a clear idea of what fraud is are criminal acts, illegal acts, tortuous acts, deceptive acts, and concealed acts. These are the most alarming fraudulent acts found in the daily administration of civil service (Adeleke, 1996).

There are different ways in which government authorities have classified fraud depending on their perspectives and the criteria used. They include internal (fraud committed among the members of the organization), external (fraud committed wholly by persons and organization external to the organization), management (frauds committed by the employees in the top echelon, that is, top management level staff that are aimed largely at deceiving the shareholders) and employees' fraud (fraud committed by employees below management position).

To combat and control fraud in the civil service, this research posits that these acts must be tackled with utmost seriousness.

4.2 Fraud Control

Office of Mental Health, New York State Bureau of Audit (2021) provides that fraud control involves checks and balances mechanisms to ensure no one person has control over all parts of a financial transaction; reconciliation of the agency's bank accounts every month; restriction of the use of agency's credit cards and verification of all charges made to credit cards or accounts; provision of Board of Directors' oversight on agency operations and management; preparation of all fiscal policies and procedures in writing and obtaining of the approval of the Board of Directors; ensuring that agency assets and resources are used only for official business; protection of petty cash funds and other cash funds; protection of cash and check collections; avoidance or discouragement of related party transactions.

4.3 Biometrics

The term biometrics is derived from the Greek words, “bio” meaning “life” and “metric” meaning “measure”. In other words, biometrics means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. It is the

technical term for body measurements and calculations. It refers to metrics related to human characteristics. It is used to identify individuals in groups that are under surveillance. It is the measurement and statistical analysis of people's unique physical and behavioural characteristics. Components of biometric devices include a reader or scanning device to record the biometric factor being authenticated; software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data; and a database to securely store biometric data for comparison (Amoore, 2021).

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals which are often categorized as physiological and behavioural. Physiological characteristics are related to the shape of the body such as fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to typing rhythm, gait and voice (Jain, 2019).

5. Empirical Literature

There are several empirical evidence of biometric and fraud control in the civil service. Simon Marchand (2021) observed that biometric security has become a vital defence against a rising tide of fraud. But the range of biometrics technologies available to brands and fraud prevention leaders extends far beyond the fingerprint and facial recognition solutions now common in consumer devices. At the heart of the problem with traditional methods of authentication is that they do not identify the actual human being that is interacting with a service or a device. Instead, they identify what they have (a token, or a phone), or what they know (their password, personal information, or memorable answers). He concluded that to prevent fraud, biometric modalities to be adopted should include physical biometrics, such as facial and fingerprint and voice biometrics; linguistic biometrics such as voice and digital channels; behavioural biometrics which is all about profiling of individual characteristics.

In another related research, the Association of Certified Fraud Examiners (ACFE) (2020) reports suggested five ways biometrics can be used to fight fraud. Such ways include addressing the weakest link in security (passwords); strengthening authentication without increasing friction for users; closing gaps in the re-verification process to fight fraud; detecting identified fraud during digital onboarding; ensuring the presence of the authorized user with biometric liveness. These factors make organizations worldwide lose an estimated 5 per cent of their annual revenue to fraud.

Machand (2021) in another study on why biometrics is essential to effective fraud prevention observed that when the pandemic forced organizations to send customer service agents to work from home, fraudsters quickly seized the new opportunity presented by isolated employees. Social engineering and bribery attempt rapidly increased as fraudsters targeted agents lacking their usual support from colleagues and managers. While fraudsters adapted fast, most organizations were not nearly as quick; many failed to take the necessary steps to bolster security and authentication processes, which led to many fraud cases. He suggested layered security as a way of salvaging the insecurity issues. Layered security involves combining fraud prevention measures like environment detection and anti-spoofing with multimodal biometrics, all underpinned by an AI-powered risk engine that aggregates data from the various layers to generate a risk score for any given customer engagement. This enables seamless, secure authentication across all the voice and digital channels that customers use to contact brands.

Joseph (2020) investigated the prevention of fraud through biometrics. He argued that many fraud prevention strategies are using biometric technologies. As some of the strategies, he suggested that organizations should add a layer of defence to fraud prevention and detection by combining behavioural biometrics with digital identity intelligence to make better fraud and risk decisions;

improve online fraud detection through behavioural security since behavioural biometrics allows organizations to detect high-risk scenarios and make better fraud decisions. It adds an extra layer of intelligence to identity authentication and represents a powerful tool in the fight against cybercrime. Behavioural biometrics provides an additional layer of defence to risk assessment without creating a negative user experience. To improve behavioural biometrics or security, Joseph (2020) suggested the adoption of LexisNexis behavioural biometrics. This, he concluded can help to separate human from non-human traffic like bots, identify "good" trusted customers' profiles, reliably profile fraudsters, detect session anomalies and build trust relating to good customers.

Kazembe et al. (2013) investigated the development of a biometric e-fraud prevention system. The biometric fraud prevention application was designed to stop purveyors of e-fraud from accessing bank accounts other than theirs. Before committing an online transaction, the system will ask for a biometric feature to be entered on a relevant device such as a face scanner, hand pattern scanner, fingerprint reader or any biometric feature reader. The result of the test showed that once data is entered, the data will be matched with a template in the database and the result can be a rejection or acceptance of the transaction. The key advantage of biometrics is that no two people share common biometric features and it takes a lot of effort to steal a fingerprint. Biometrics has been reliably used in the world at large in forensic investigations and every law enforcement agency uses the fingerprint and once detected, their verity is irrefutable. Sensor hardware such as fingerprint scanners, iris scanners and face scanners from different vendors are tested to improve system interoperability.

Biambo (2019) reviewed the impact of cyber security on fraud prevention in the Nigerian civil service. It was found that advanced biometrics can be incorporated to strengthen the security of computer networks in public offices. Thus, every employee needed to go through biometric authentication to verify their identity before accessing files or initiating transactions within the system. This measure eliminates the chances of an unauthorized party entering the network to commit fraud and other identity-related crimes. He concluded that enhancing cyber security in offices helps to improve the authentication process, makes transactions within and outside the office more secure and successful, protects employees' identities, allows the movement of authorized personnel, keeps information safe as well as aids in employee background checks.

Cole (2021) carried out a study on using biometric KYC to keep fraudsters out of a system. The study revealed that synthetic identity fraud, based on the skilful creation of fictional identities, is a significant and fast-growing source of losses to fraud. Consequently, identity fraud and its derivative crimes cost banks, retailers, healthcare providers, governments, and ultimately consumers and taxpayers around the globe hundreds of billions of dollars every year, and this figure continues to grow. From the perspective of a bank, government agency, or any organization aiming to broadly reduce its exposure to identity fraud, a more universal approach is needed to have a broad impact. This has been discovered to be so because of the following findings: 1. Much of identity fraud is committed using 'synthetic' identities that are not stolen but created; 2. Biometric verification does not verify the authenticity of identity data. Biometric verification on a device helps prevent a fraudster from using a stolen device to falsely claim the identity of the owner, but does not prevent them from establishing accounts with fraudulent information; 3. Penetration of smartphones is growing rapidly but is still on the order of only 36% globally. In places where many people still do not use smartphones, other mechanisms are necessary to prevent identity fraud more universally; 4. Authentication on smartphones is device-specific and constrained to operate as implemented by the device, operating system and application suppliers. While organizations aim to standardize architecture and interfaces, biometric functionality and performance will not be universal or configurable on these devices, and will not necessarily meet

the security requirements of a particular application.
Owusu-Oware et al. (2018) conducted a study on biometric technology for fighting fraud in national health insurance in Ghana. The study sought to understand how developing countries can deploy biometric technology to fight fraud in National Health Insurance (NHI). The findings showed that the use of biometric technology can fight fraud in NHI by helping to (1) eliminate multiple identities and fake IDs through online biometric enrollment of members; (2) eliminate impersonation and ghost patients through biometric verification at the point of service delivery; (3) reduce fraudulent provider bills. The findings also showed that deploying biometric technology to fight NHI fraud requires integrated social and technical systems; social systems such as the use of clinicians to detect inflated provider bills and technical systems such as the e-claims system that complement the biometric technology. The study also demonstrated the use of a socio-materiality lens in unpacking the social and technological dynamics involved in deploying biometric technology for NHI. For practice and policy, the study showed that with appropriate operational policies, biometric technology can be deployed effectively to reduce fraud.

6. Biometric Programme and Fraud Control in Akwa Ibom State

Biometrics was introduced basically for the control of fraud in the civil service of Akwa Ibom State. The major areas of fraud control using biometric applications considered in this paper are biometric employee identification numbers and biometric payroll.

6.1 Employee Identification Number and Fraud Control

The Employee Identification Number (EIN) is a ten-digit unique number assigned by the Civil Service Commission of Akwa Ibom State to all the staff for identification. These numbers (usually written like P700066373) are used for tax administration and records of employee progress in the service. The identification number allows streamlined, accurate record-keeping, and preservation of confidential information about the employee (Umoh, 2022).

The EIN is required to be presented by registrable employees before several basic transactions can be undertaken in the civil service of Akwa Ibom. Specifically, every registrable staff is required to state their EIN while engaging in transactions relating to insurance policies, pensions and health insurance schemes, credit transactions, deductions/payment of taxes, enrolment into primary, secondary and tertiary schools and continuous professional studies for staff development (Business Day Newspaper, 2019).

6.2 Electronic Payroll System and Fraud Control

A payroll, which includes a list of employees or staff receiving wages or salaries with the amount due to each, consists mainly of two sections: (a) Payroll payment and (b) payroll deductions. Payroll payments consist of the annual basic salary, the monthly basic salary, grade level, and allowances of each staff, while the payroll deductions consist of deductions that are made out of the employee's total emolument such as tax deductions and other deductions. The usual or operational payroll technique in the civil service in Nigeria has been manual since independence, referred to as the return mechanized voucher system (Elekwa & Eme, 2013).

The electronic payroll system in Akwa Ibom State civil service was introduced in 2000 to curb the menace of payment by hand. There were records of missing money and embezzlement of public funds, especially in the local government system. Ministries and agencies could not ascertain how to pay some figures in staff salary recorded in Kobo and small fractions of Naira. But the introduction of the electronic system enables every employee to get his incentives in full without any missing fraction. This system disburses funds automatically and simultaneously to every employee at once. All that is required is for the employee to have a Biometric (Bank) Verification Number (BVN) (Umoh, 2022).

6.3 Challenges of Biometric Application in the Civil Service

Although the use of biometric technology has been adjudged to be of great importance to the success, growth and development of the civil service, there are still a few concerns and challenges in collecting and using the biometric system in Akwa Ibom State. The challenges include:

Feasibility concerns: According to Ramakumar (2018), the biometric programme is being implemented without any cost-benefit or feasibility studies to ascertain whether the programme would meet its stipulated goals. The government obscured the security aspects of the programme, which was to weed out fraud and illegal alien staff but focused more on the benefit schemes.

Lack of privacy concerns: The biometrics seems secure on the surface because the employee is the only one with the fingerprint, but that does not necessarily make it more secure than passwords. To Thomas (2017), the system allows the profiling of staff's public and private affairs.

Application issues: Despite the modern processes, there are cases where enrollments are lost in the system without explanation. Many employees complain of not being enrolled because of cuts on their fingers while some were dictated by the system as "captured already" (Eugene, 2018).

Data leaks: The detailed personal information being collected is of extremely high importance to an employee. Major financial transactions are linked with information collected in biometrics. Government departments and various other agencies that collect this information such as banks cannot be trusted to maintain the secrecy of all this collected information. For instance, the NITDA Act (2007) confirmed more than 20 websites are used to hack into workers' personal information in Akwa Ibom State.

The issue with harnessing EIN with NIN: The government is trying to harness Employee Identification Number (EIN) with National Identification Number (NIN) to verify the authenticity of workers as citizens of the state. Many employees who registered for NIN between the period of 2000 and 2006 are finding it difficult to register again, especially if there is a variation in their Bank details (Umoh, 2022).

Inadequate primary technology such as electricity: The biometric architecture of all programs requires constant power to function optimally in the storage, processing, retrieving and verification of these data. This has been one of the major challenges to the success of the biometric system in the state. For the government to prevent disruption that could occur during verification and identification processes, it has to ensure an adequate power supply without which the full potential of biometric technology cannot realize (Hope, 2021).

7. Materials and Methods

This paper adopts the survey design. Data were obtained through questionnaire administration on three selected ministries (Local Government and Chieftaincy Affairs; Finance; and Education), three departments (Establishment, Civil Service Commission; Office of the Accountant General; and Office of the Auditor General) and two agencies (General Services Office, Governor's Office Annex, Uyo; Local Government Service Commission, Uyo) (MDAs) of Akwa Ibom State civil service.

The population of this study comprises all civil servants in the selected ministries, departments and agencies (MDAs) of Akwa Ibom State which was twenty-three thousand, nine hundred and twenty-six (23,926), as of September 2022 (Department of Establishment, Akwa Ibom State, 2022).

The researcher scientifically selected a sample of 368 respondents using Andrew Fisher's formular:

$$N = \frac{Z^2Pq}{d^2}$$

To ensure fairness and unbiased representation and analysis, the study sample MDAs and sample respondents were drawn through simple random sampling and cluster sampling techniques. The sampling procedure began with the cluster sampling technique which was used to divide the Akwa Ibom State civil service into three (3) clusters (MDAs), that is, ministries, departments and agencies. A simple random sampling technique through the balloting method was used in the second stage to select three (3) ministries out of eighteen (18), two (2) agencies out of forty (40) and three (3) departments from each of the three clusters. This allowed the researcher to gather data on a diverse array of clusters, which provided an overview of the entire population of the civil service. Sample Size was divided to cut across all clusters, thus = $\frac{368}{8} = 46$

Sample size per cluster (MDA) = 46. Within each of these clusters, 46 questionnaires were divided and administered to the following categories of respondents: (a) 16 questionnaires were administered to management staff within each MDA. (b) 30 questionnaires were administered to junior and casual staff. The idea and strategy were to ensure that responses given must not be biased and should represent the views of all staff as well as contain respondents who are educated and enlightened on variables.

Two sets of variables were required and tested in this study- the dependent (Y) and independent (X) variables. The dependent variable was fraud control while the independent variables were biometric employee identification numbers and the electronic payroll system.

8. Analysis and discussion

8.1 Analysis of Data

Out of the three hundred and sixty-eight (368) copies of the questionnaire distributed, three hundred and fifty-one (351) were returned in good condition. This represents 95.4%, indicating a strong response, which is significant enough to carry out the analysis. Data obtained were analyzed using simple percentages while the hypotheses formulated were tested using Regression Analysis and Pearson Product Moment Correlation Coefficient (r) as shown below:

Hypothesis One: "There is no significant relationship between employee identification number and fraud control in Akwa Ibom State Civil Service". Data for this test was derived from questions 1, 2, 3, 5 and 6 of the questionnaire. Regression analysis was used to test this hypothesis.

Table 1: Contingency Table for H ypothesis One

Question No.	Responses		$(Y-\overline{Y})$	$(X-\overline{X})$	$(X-\overline{X})(Y-\overline{Y})$	$(Y-\overline{Y})^2$	$(X-\overline{X})^2$
	Yes (Y)	**No (X)**					
1	66	-	-11	3.5	38.5	121	12.25
2	32	5	23	-1.5	34.5	529	2.25
3	60	3	-5	0.5	2.5	25	0.25
5	31	8	24	-4.5	108	576	20.25
6	40	2	15	1.5	22.5	225	2.25
All variables	101	3	-46	0.5	23	2116	0.25
	? Y=330 (94%) $\overline{Y}$ **=55**	**? X=21 (6%)** $\overline{X}$ **= 3.5**			**? = 229**	**? = 3592**	**? = 37.5**

Source: Author's computation from questionnaire (2022)

The regression equation is: $Y_{\cdot} = a + b\overline{x} + e$ (Udofia, 2010) = $Y_{\cdot} = 33.65 + 6.10\ (x) + e$

Where: we obtain "b" from:

$$b = \frac{?\ (X - \overline{X})(Y - \overline{Y})}{?\ (X - \overline{X})^2} = \frac{229}{37.5} = 6.10$$

We then obtain "a" from:

$$a = \overline{Y} - b\bar{x} = 55 - 6.10\ (3.5) = 33.65$$

We use the formula to obtain "t":

$$t = \frac{b\sqrt{\sum x - \bar{x})2}}{\sigma y} \qquad t = 6.10\frac{\sqrt{(37.5)^2}}{10}$$

$$= \quad 22.88 \text{ (calculated value)}$$

Where: $\delta y = \frac{\sqrt{\sum(Y-\overline{Y})^2}}{N} = \frac{\sqrt{3592}}{6} = 10$

Degree of Freedom = N-2 = 6-2 = 4 under 5 (two tailed test) = 2.45 (table value)

The calculated value (22.88) is greater than the table value (2.45), thus the b value of 6.10 is significant. We, therefore, accept the alternative hypothesis (Hi) and reject the null hypothesis (Ho). Thus, there is a significant relationship between employee identification number and fraud control in Akwa Ibom State Civil Service.

Hypothesis Two: "There is no significant relationship between electronic payroll system and fraud control in Akwa Ibom State Civil Service". Questions 7, 8, 9, 10 and 11 of the questionnaire

were used for the test. Pearson Product Moment Correlation Coefficient (r) was used to test this hypothesis.

Table 2: Contingency Table for Hypothesis Two

QUESTION NO.	X	Y	XY	X^2	Y^2
7	17	3	51	289	9
8	10	2	20	100	4
9	70	4	280	4900	16
10	28	5	140	784	25
11	18	3	54	324	9
All Variables	180	11	1980	32400	121
	? x= 323 (92%)	**? y= 28 (8%)**	**? xy= 2525**	**? x^2= 38797**	**? y^2= 184**

Source: Author's computation from questionnaire (2022)

"r" formula = $$\frac{N\sum XY-(\sum X)(\sum Y)}{[N(\sum X^2)-(X)^2][N(\sum y^2)-(\sum y)^2]}$$

$$r=\frac{6(2525)-(323)(28)}{\sqrt{[6(38797)-(323)^2][6(184)-(28)^2]}}$$

$$r=\frac{6106}{2027.4}=3.0$$

To test the strength of the relationship, t-statistics is applied thus:

$$t=\frac{r\sqrt{N-2}}{\sqrt{1-r^2}}$$

$$t=\frac{3.0\sqrt{6-2}}{\sqrt{1-3.0^2}}=2.7 \text{ (Computed Value)}$$

Degree of freedom = N-2 = 6-2 = 4 under 5 (two tailed test) = 2.45 (table value)

The computed t-value of 2.7 is greater than the table value of 2.45 at a five per cent level of significance. Hence, the null hypothesis (Ho) is rejected. This means there is a significant relationship between the electronic payroll system and fraud control in Akwa Ibom State Civil Service.

8.2 Discussion

The result of the test of the first hypothesis indicated that there is a significant relationship between employee identity number (EIN) and fraud control in Akwa Ibom State Civil Service. In support of this finding, while Umoh (2022) posited that EIN allows streamlined, accurate record keeping, and preservation of confidential information about the employee, Business Day Newspaper (2019) reports that every staff is required to state their EIN while engaging in transactions relating to insurance policies, pensions and health insurance schemes to control fraud.

The results of the test of hypothesis two revealed that there is a significant relationship between the

electronic payroll system (EPS) and fraud control in Akwa Ibom State Civil Service. To support this finding, Rietsema (2020) held that, even with the most conscientious and careful human resource employees, without EPS there are bound to be errors with tax compliance, bonus calculations, and more. Pay cheques can be delayed if the payroll officer is busy, but with EPS, manual entry risks and intentional errors/fraud can be controlled.

9. Conclusion and Recommendations

This paper revealed that two main concerns prompted the government to consider a unique identity for all civil servants. The first was to prevent fraud through multiple identities. The other was to expand benefits coverage to those who had no identity documents or whose names were omitted from the government payroll, in the case of public servants. The essence of introducing a biometric program into the Akwa Ibom State civil service was to improve efficiency, prevent fraud and enable digital innovation. This made information about all active staff easy to access. The biometric ID system in Akwa Ibom State forms a cornerstone of the government's vision of digital civil service in the quest for fraud prevention. The biometric programme has been adjudged to provide a system of convenience which makes employees a sense of belonging and protection in the service which in turn improves workers' efficiency and productivity. Although there is a high level of technical problems which constrains the effective application of biometric technology, the system has been used to successfully establish an accurate and digitised database of pensioners, and eliminate duplicate payments, ghost pensioners and underpayments. Thus, it has been concluded that biometric implementation has a significant impact on the Akwa Ibom state civil service.

To solve the problems discovered in this paper, the following are recommended:

1. Government should ensure that Employee Identity Numbers (EIN) are adequately protected since they are linked to their financial records.
2. Government should regularly conduct more serious evaluations on the effectiveness of the Electronic Payroll System (EPS) since it has been observed that monitoring and evaluation still lack internal support within the government MDAs.
3. Government should also ensure that a biometric attendance system (electronic time book) is provided and made functional in all government offices. Fingerprints of employees should be updated or upgraded regularly to accommodate some employees whose fingers may not be recognized by the system due to cuts or burns.
4. Proper funding for the biometric programme should be provided to reduce the chances of fraud among those handling the programme. Proper legislation/law that guides the usage and control of biometric technology in the state with penalties meted out against defaulters should be established.

References

Adeleke, I. (1996). The impact of forensic accounting on fraud detection. Bayero University.

Akwa Ibom State Government (AISG) ICT Department, ministry of information & strategy (2020). Akwa Ibom State Government discovers over 9000 Ghost Workers. https://akwaibomstate.gov.ng/

Alade, I. and Oguntuase, O. (2019). Nigeria: National identity management in Nigeria: Matters arising. https://www.mondaq.com/Nigeria/Government-Public-Sector/831396/National-Identity-Management-In-Nigeria-Matters-Arising (Retrieved on 2nd January, 2020)

Amoore, L. (2021). Plans and situated action: The problem of human-machine communication. Cambridge University Press.

Association of Certified Fraud Examiners (ACFE) (2020). Reports to the nation on occupational fraud and abuse on five ways biometrics help fight fraud. Broadway Suite.

Babalobi, M. (2008). Biometrics are too hot to handle: Despite high hopes, bankers are still all talk when it comes to identification technology. Bank Technology News, 14(9): 30–33.

Benjamin, A. (2018). Biometrics and the challenges of privacy in Akwa Ibom State. Journal of Public Economics, 90(5): 853-870.

Biambo, A. (2019). Biometric Cyber-security and fraud prevention. (Unpublished PhD Seminar Paper) University of Uyo.

Business Day Newspaper (2019). National identity management in Nigeria: Matters arising. https://businessday.ng/legal-business/article/national-identity-management-in-nigeria-matters-arising/

Cole, J. (2021). Biometric KYC (Part I) – Keeping fraudsters out of your system. Aware Publication.

Darma, M. & Ali, O. (2014). New security technology and social identities. Journal of Race, Nation and Culture, 18(5): 593–607.

Department of Establishment, Civil Service Commission, Akwa Ibom State, (2022). Staff strength of Akwa Ibom State civil service as at September, 2022.

Dickson, E. J. (2020). Bank fraud in Nigeria: Underlying causes, effects and possible remedies, African Journal of Accounting, Economics, Finance and Banking Research, 6(6): 62.

Elekwa, N. E. & Eme, O. K. (2013). An analysis of computerized accounting and payrolling system on monthly emolument in Nigerian local government. International Journal of Accounting Research, 1(3): 16.

Eugene, I. (2018). Issues in body identifications. Routledge.

Gideon, F. (2012). U.S. warns Nigeria over online fraud schemes.

http://www.crime-research.org/news/2002/09/Mess2801.htm

Hope, U. C. (2021). Biometric technology usage in securing e-governance in Nigeria: Benefits and challenges.
https://www.researchgate.net/publication/326154080_BIOMETRIC_TECHNOLOG

Y_USAGE_IN_SECURING_E-GOVERNANCE_IN_NIGERIA_BENEFITS_AND_CHALLENGES

Jain, A. K. (2019). Introduction to biometrics. Springer.

Joseph, G. (2020). Behavioural biometrics. https://risk.lexisnexis.com/global/en/products/behavioral-biometrics

Kazembe, T. R., Scott, M. S. & Jere, N. R. (2013). Investigation and development of a biometric e-fraud prevention system. Telkom Centre of Excellence.

Kirmani, M. (2019). Impact of biometric attendance system on secondary and higher secondary educational institutions across J&K, India. Oriental Journal of Computer Science & Technology, 10(2): 291-297.

Kumar, V. (2019). Bureaucratic theory by Max Weber – a review study. Journal of Advances and Scholarly Researches in Allied Education, 11 (23): 1-6.

Marchand, S. (2021). Fraud never sleeps: Why biometrics is essential for effective fraud prevention. Nuance Communications, Inc.

Magnet, S. (2018). When biometrics fail: Gender, race, and the technology of identity. Duke University Press.

Mulder, P. (2017). Bureaucratic theory by Max Weber. https://www.toolshero.com/management/bureaucratic-theory-weber/

National Information Technology Development Agency Act (2007). About the law. https://lawpadi.com/national-information-technology-development-agency-act-2007/

Office of Mental Health (OMH) (2021). Top ten internal controls to prevent and detect fraud. Holland Avenue Albany.

Olugbemi, L. (2017). The biometrics revolution. Center for Global Development.

Owusu-Oware, E., Effah, J. & Boateng, R. (2018). Biometric technology for fighting fraud in national health insurance: Ghana's experience (Paper presentation). 24th Americas Conference on Information Systems. University of Ghana.

Ramakumar, M. (2016). Social identities and recognization. Journal for the Study of Race, Nation and Culture, 18(5): 593–607.

Rietsema, D. (2020). Payroll system. https://www.hrpayrollsystems.net/payroll-systems/

Taiwo, F. and Akintola, P. (2017). The description of biometric objects. MIT Press.

Thomas, I. (2017). Normative issues in the socio-technical coding of the body. Routledge.

Toakodi, A. (2014). Corruption in the civil service: A Study of salary fraud in Bayelsa state, Nigeria. (Unpublished Postgraduate Research Paper) University of Abuja

Udofia, E. P. (2010). Fundamentals of social science statistics. Immaculate Publishing Limited

Umoh, U. (2022). Biometric exercise in Akwa Ibom State civil service: Lessons to learn. (Unpublished PhD Seminar Paper) University of Uyo.

Weber, M. (1905). The protestant ethic and the spirit of capitalism. Courier Corporation.

Appendix

Administered Questionnaire

	VARIABLES	YES	
Employee Identity Number and Fraud Control in Akwa Ibom State Civil Service			
1.	Employee Identity Number (EIN) ensures continuity, maintenance and adequacy in employee's records for unique identification		
2.	EIN guarantee employee job security **against breaches**		
3.	With EIN computerized record keeping, redundancy of information are reduced.		
4.	EIN aids to identify which employees are in actual need of particular government services		
5.	EIN curb the menace of ghost workers by uniquely identifying all the genuine employees in the civil service		
6.	Employee ID can be used to track employee payroll tax remittances, excise tax returns and other vital deductions		
Electronic Payroll System and Fraud Control			
7.	Electronic Payroll System (EPS) control manual entry risks and input errors from tax compliance, bonus calculations, etc		
8.	With EPS, every employee gets correct pay cheques as well as alert of incentives at the same time depending on the banks		
9.	EPS help streamline and automate the direct deposit process, making timely payroll even easier.		
10.	EPS allows all employees to view and update their own financial information.		
11.	EPS helps in the identification and elimination of errors and misclassifications of those working in the service- contractors, employees, ghost employees, etc.		