JOURNAL AFRICAIN DES SCIENCES
VOL. 3, **3** (2026) 42-50

https://jafrisci.org

ISSN (online) : 3107-0949 ; ISSN (print) : 3107-0930

OPEN ACCESS

ARTICLE DE RECHERCHE

Article Info.:
Reçu : le 07/02/2026
Accepté: le 30/03/2026
Publié : le 03/04/2026

TRAÇABILITÉ DES DONNÉES DANS UN ENVIRONNEMENT CLOUD POUR L'ASSAINISSEMENT DES AGENTS D'UNE ADMINISTRATION PUBLIQUE : APPLICATION À LA GESTION DES FONCTIONNAIRES DE L'ÉTAT EN RÉPUBLIQUE DÉMOCRATIQUE DU CONGO

Bob Bokanga Boseko [1,*], Simon Badibanga Ntumba [1], Blaise Luhepa Muhala1 [3], Pierre Motumbe Kasengedia [2], Noella Mayuma Fwifu [3]

https://doi.org/10.70237/jafrisci.2026.v3.i3.05

Résumé

La qualité des données administratives conditionne la fiabilité des systèmes de gestion des agents publics. Pourtant, la dispersion des sources, l'absence d'historisation et l'insuffisance des contrôles favorisent des irrégularités administratives et salariales. Cet article propose une architecture de traçabilité des données en environnement cloud pour soutenir l'assainissement de la gestion des agents d'une administration publique, appliquée au cas des fonctionnaires de l'État en République démocratique du Congo. La solution repose sur une architecture en trois couches intégrant la centralisation des données, le contrôle d'accès et la journalisation des opérations. Elle permet de suivre les modifications, d'auditer les actions sur les dossiers et de détecter diverses anomalies. L'évaluation expérimentale a permis d'identifier 101 278 dossiers litigieux, 56 813 doublons, 43 869 matricules d'emprunt et 2 237 incohérences salariales. Ces résultats montrent l'intérêt de la traçabilité pour renforcer la fiabilité, la transparence et le contrôle des données administratives.

Mots-clés: Traçabilité, cloud computing, assainissement administratif, gouvernance des données, contrôle d'accès, détection d'anomalies, fonctionnaires, administration publique, RD Congo.

Abstract

The quality of administrative data is a key condition for the reliability of public employee management systems. However, the fragmentation of data sources, the lack of change history, and insufficient control mechanisms often lead to administrative and payroll irregularities. This article proposes a cloud-based data traceability architecture to support the cleanup of public administration employee records, with an application to the management of state civil servants in the Democratic Republic of the Congo. The solution relies on a three-layer architecture combining data centralization, access control, and operation logging. It enables the monitoring of modifications, the auditing of actions performed on records, and the detection of various anomalies. Experimental evaluation identified 101,278 disputed records, 56,813 duplicates, 43,869 borrowed registration numbers, and 2,237 payroll inconsistencies. These results highlight the value of traceability for improving the reliability, transparency, and control of administrative data.

Keywords: Traceability, cloud computing, administrative cleansing, data governance, access control, anomaly detection, civil servants, public administration, DR Congo.

1. Introduction

Dans une administration publique, une donnée erronée n'est jamais un simple défaut technique. Elle peut devenir un agent payé à tort, un dossier modifié sans preuve, une décision budgétaire fondée sur une information altérée, ou encore un contrôle rendu impossible faute d'historique fiable. À mesure que les administrations se numérisent, la qualité de la gestion publique dépend donc de plus en plus de la capacité des systèmes d'information à centraliser, sécuriser et rendre vérifiables les données qu'ils manipulent. Dans ce mouvement, le cloud computing s'est imposé comme un levier majeur de modernisation, en raison de sa souplesse, de sa capacité de mutualisation et de son potentiel pour soutenir la transformation numérique des organisations gouvernementales [1][2].

Cependant, la migration vers le cloud ne résout pas, à elle seule, les difficultés structurelles liées à la gouvernance des données. Héberger des informations administratives dans un

Correspondance : *bob.boseko@gmail.com* ***(B. B. Boseko)***

Copyright : © The Author(s) Published under a Creative Commons Attribution 4.0 International Licence (CC BY 4.0)

[1] *Mention de Mathématiques, Statistique et Informatique, Université de Kinshasa, Kinshasa, RD Congo*
[2] *Département de Réseaux et Télécommunications, Institut Supérieur des Techniques appliquées, Kinshasa, RD Congo*
[3] *Département d'Intelligence Artificielle et Technologies Innovantes, Centre de Recherche sur l'Enseignement de la Mathématique, Kinshasa, RD Congo*

environnement distribué ne garantit ni leur qualité, ni leur intégrité, ni leur auditabilité. Les travaux récents montrent au contraire que la valeur d'une architecture cloud dépend étroitement des mécanismes de gouvernance mis en place : gestion des droits, contrôle des accès, assurance qualité, traçabilité des opérations, et vérification de l'intégrité des données stockées [3][4].

Cette exigence devient particulièrement critique lorsqu'il s'agit de gérer les fichiers administratifs et salariaux des agents publics. Dans ce type d'environnement, la dispersion des sources, la non-synchronisation des bases, l'absence de piste d'audit robuste et la faiblesse des mécanismes de contrôle créent un terrain favorable à l'apparition de doublons, de matricules irréguliers, de modifications non autorisées et de paiements indus. Les recherches récentes sur la détection d'anomalies dans les environnements cloud soulignent justement le rôle central des journaux d'événements et des mécanismes de surveillance pour repérer les comportements suspects ou les incohérences systémiques [5].

Dans le cas des administrations publiques, la traçabilité doit dès lors être pensée comme une fonction centrale du système et non comme un simple module de journalisation ajouté posteriori. Des études récentes confirment cette évolution : certaines proposent des architectures où la traçabilité de bout en bout est intégrée dès la conception [7], d'autres montrent que l'absence de traçabilité constitue un frein majeur au partage sécurisé des informations entre services publics [8]. Dans le même temps, les réflexions contemporaines sur la gouvernance publique rappellent que la transparence, la responsabilité et le contrôle des irrégularités sont devenus des enjeux structurants de la performance administrative et financière [9].

Or, malgré l'abondance des travaux sur l'adoption du cloud, la gouvernance des données, l'audit de l'intégrité ou encore la détection d'anomalies, peu d'études articulent explicitement ces dimensions autour d'un même objectif : l'assainissement du fichier des agents publics dans une administration d'un pays en développement, et plus particulièrement dans un contexte africain [1][9].

C'est dans cette perspective que s'inscrit le présent article.
Il propose une approche de traçabilité des données dans un environnement cloud pour soutenir l'assainissement des agents d'une administration publique, avec application à la gestion des fonctionnaires de l'État en République démocratique du Congo. L'article poursuit trois objectifs : (i) formaliser le problème de l'assainissement du fichier des agents comme un problème conjoint de gouvernance des données, de sécurité et d'auditabilité ; (ii) proposer une architecture applicative reposant sur la centralisation cloud, le contrôle d'accès et la journalisation des opérations ; (iii) évaluer l'apport de cette architecture à partir d'indicateurs portant sur les irrégularités détectées, la traçabilité des actions et l'impact financier associé.

2. État de l'art

La littérature récente sur la traçabilité des données en environnement cloud appliquée au secteur public peut être organisée autour de quatre axes majeurs : l'adoption du cloud dans les administrations, la gouvernance et l'intégrité des données, les architectures de traçabilité et d'auditabilité, puis la détection d'anomalies au service de la transparence administrative.

Un premier ensemble de travaux s'intéresse à l'adoption du cloud dans les organisations gouvernementales. Ces recherches montrent que le cloud est perçu comme un levier de modernisation des services publics grâce à sa flexibilité, à sa capacité de mutualisation et à son potentiel de transformation numérique. Toutefois, elles soulignent aussi que son adoption reste fortement conditionnée par des facteurs organisationnels, réglementaires, sécuritaires et humains [1][2][11].

Un deuxième axe porte sur la gouvernance, la qualité et l'intégrité des données dans le cloud. Les travaux récents insistent sur le fait que la valeur d'une infrastructure cloud dépend moins du simple hébergement que de la capacité à encadrer le cycle de vie des données : règles de qualité, responsabilités, contrôle des accès, auditabilité et garanties d'intégrité [3][10][4].

Un troisième axe concerne les architectures de traçabilité elles-mêmes. La littérature récente tend à considérer la traçabilité non plus comme une simple journalisation secondaire, mais comme une propriété architecturale intégrée dès la conception. Cette idée apparaît aussi bien dans les systèmes de partage sécurisé de fichiers en e-gouvernance que dans des plateformes à traçabilité de bout en bout [6][9][27][28].

Un quatrième axe s'intéresse à la détection d'anomalies et à l'accountability publique. Dans les environnements cloud, les journaux d'événements deviennent une source stratégique pour détecter des comportements suspects, des opérations incohérentes ou des irrégularités de traitement [5][9].

Cependant, malgré cette richesse, la littérature présente encore une lacune importante : les travaux existants traitent généralement séparément l'hébergement cloud, la sécurité, la traçabilité ou l'analyse des irrégularités, sans les articuler dans un même dispositif opérationnel orienté vers la fiabilité des dossiers administratifs et salariaux. C'est précisément dans cet espace que se situe notre travail.

Tableau 1 : Synthèse critique des travaux récents

Axe	Apport clé	Limite
Adoption du cloud public	Modernisation, flexibilité, mutualisation	Ne traite pas directement l'assainissement des dossiers administratifs
Gouvernance et intégrité des données	Qualité, contrôle d'accès, auditabilité	Reste général, peu centré sur les fichiers RH et la paie
Traçabilité et auditabilité	Traçabilité conçue comme propriété architecturale	Peu orienté vers la gestion publique africaine
Détection d'anomalies	Exploitation des logs pour repérer les irrégularités	N'intègre pas une architecture unifiée pour l'assainissement

3. Problématique et hypothèse

Malgré l'abondance des travaux consacrés à l'adoption du cloud, à la gouvernance des données, à l'audit d'intégrité et à la détection d'anomalies, la littérature étudiée montre qu'il existe encore peu de propositions intégrées capables de répondre directement au problème concret de l'assainissement du fichier des agents publics dans une administration d'un pays en développement.
La problématique de cette recherche peut donc être formulée comme suit : comment concevoir un système de traçabilité des données, déployé dans un environnement cloud et fourni selon

une logique de service centralisé, capable d'améliorer simultanément la fiabilité des données administratives, la transparence des opérations et l'assainissement du fichier des fonctionnaires de l'État ?

L'hypothèse générale défendue dans cet article est la suivante : la mise en œuvre d'un système de traçabilité déployé dans le cloud, consommé sous forme de service applicatif de type SaaS, et combinant centralisation des données, contrôle d'accès fondé sur les rôles, journalisation chaînée et détection des irrégularités, permet d'améliorer de manière significative la qualité des données, l'auditabilité des opérations et la capacité d'assainissement administratif.

Cette hypothèse implique que la valeur du système ne réside pas uniquement dans le stockage cloud, mais dans l'intégration cohérente de mécanismes de gouvernance, de sécurité, de traçabilité et d'analyse au sein d'une même architecture de service.

4. Méthodologie

4.1. Approche méthodologique générale

La méthodologie adoptée dans cette recherche repose sur une approche mixte, combinant analyse qualitative, modélisation du système et validation quantitative. Ce choix s'explique par la nature du problème traité. L'assainissement du fichier des agents publics ne peut pas être réduit à une simple question de stockage informatique ; il s'agit d'un problème à la fois organisationnel, sécuritaire, informationnel et budgétaire [22][23]. Les recherches récentes sur les approches mixtes montrent justement leur intérêt lorsqu'il s'agit d'étudier des systèmes socio-techniques complexes en articulant compréhension contextuelle et validation instrumentée [12][24][25].

4.2. Démarche globale de l'étude

L'étude suit une progression en cinq étapes, résumée dans la Figure 1.

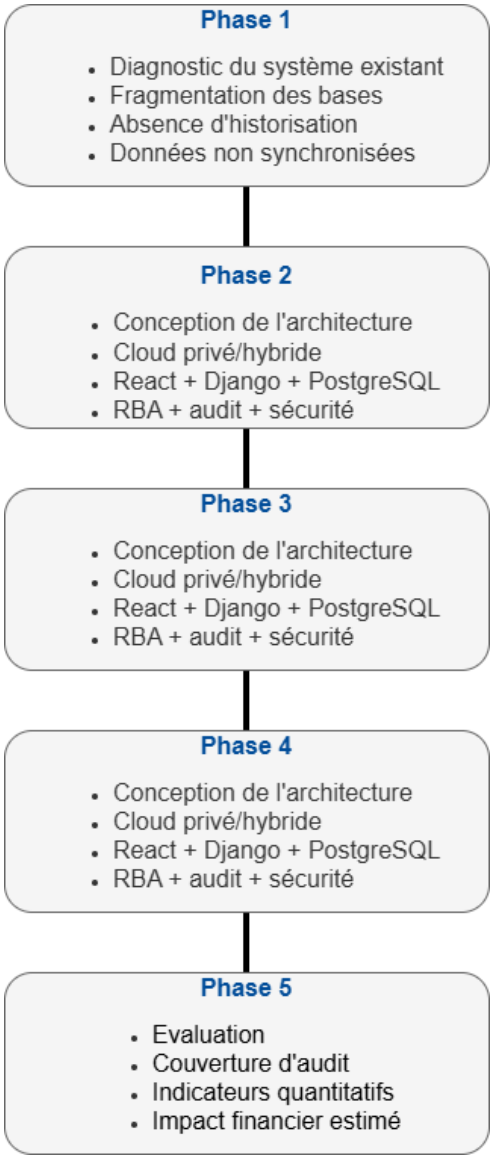


Figure 1. *Workflow méthodologique de l'étude*

La première étape consiste à analyser le système existant de gestion des agents publics. Elle vise à identifier les faiblesses structurelles : multiplicité des bases non synchronisées, absence d'historisation des modifications, présence de doublons, agents fictifs, incohérences administratives et difficulté de maîtrise de la masse salariale.

La deuxième étape est consacrée à la conception de l'architecture cible. L'objectif est d'inscrire les données dans une architecture sécurisée où chaque opération peut être attribuée, vérifiée et retracée dans le temps [21].

La troisième étape correspond à l'implémentation d'un prototype fonctionnel permettant d'importer les données issues des fichiers administratifs et de paie, de gérer les dossiers, d'appliquer les règles de sécurité, et de journaliser les opérations réalisées par les utilisateurs.

La quatrième étape porte sur la détection des anomalies :

doublons, matricules d'emprunt, agents fictifs et incohérences salariales [20].

La cinquième étape est celle de l'évaluation, fondée sur des indicateurs quantitatifs portant sur le nombre d'irrégularités détectées, la couverture de la traçabilité et l'impact financier potentiel [12].

4.3. Architecture proposée du système

L'un des éléments centraux de la méthodologie est l'architecture du système proposé, représentée dans la Figure 2.

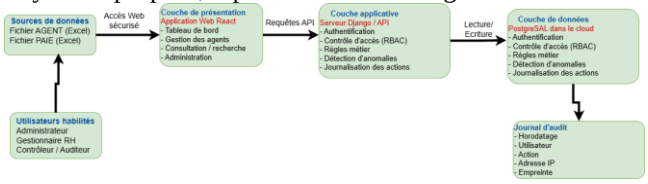


Figure 2. *Architecture proposée du système de traçabilité des données dans le cloud*

Le prototype repose sur une architecture client-serveur en trois couches. La première couche est la couche de présentation, matérialisée par une application Web développée avec React. La deuxième couche est la couche applicative, implémentée avec Django, qui traite les requêtes, applique les règles métier, gère l'authentification, le contrôle d'accès et la journalisation des opérations. La troisième couche est la couche de données, constituée d'une base PostgreSQL hébergée dans le cloud. La communication entre les couches est sécurisée par HTTPS[17] [18].

Au regard de son mode d'accès et de son usage, la solution proposée peut être positionnée prioritairement comme un Software as a Service (SaaS) administratif déployé dans le cloud. Les utilisateurs habilités accèdent au système via une interface Web, sans installation locale, tandis que les fonctionnalités de gestion des dossiers, de contrôle d'accès, de journalisation et d'audit sont centralisées au niveau du service [19].

D'un point de vue fonctionnel, l'architecture s'organise autour de quatre flux principaux : (i) un flux d'accès utilisateur via le navigateur et l'interface React ; (ii) un flux applicatif où Django applique les traitements et les règles de gestion ; (iii) un flux de données où PostgreSQL centralise les tables des fonctionnaires, des paies, des administrations et des banques ; (iv) un flux de traçabilité dans lequel chaque opération significative génère un enregistrement d'audit.

4.4. Formalisation du mécanisme de traçabilité

Pour renforcer la rigueur de la proposition, chaque opération effectuée sur un dossier administratif est modélisée comme un événement de traçabilité :

$$\tau_{\{i\}} = \left(u_{\{i\}}, r_{\{i\}}, a_{\{i\}}, o_{\{i\}}, t_{\{i\}}, ip_{\{i\}}, h_{\{i-1\}}, h_{\{i\}}\right)$$

où u_i désigne l'utilisateur, r_i le rôle, a_i l'action réalisée, o_i l'objet concerné, t_i l'horodatage, ip_i la source réseau, h_{i-1} l'empreinte de l'événement précédent et h_i l'empreinte de l'événement courant.

L'empreinte du nouvel événement est calculée par :

$$h_{\{i\}} = H\left(u_{\{i\}} | r_{\{i\}} | a_{\{i\}} | o_{\{i\}} | t_{\{i\}} | ip_{\{i\}} | h_{\{i-1\}}\right)$$

Cette logique est illustrée dans la Figure 3.

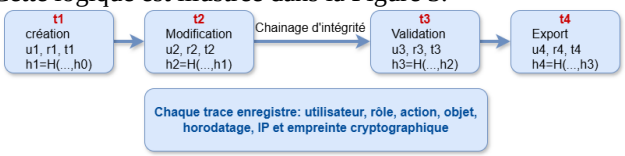


Figure 3. *Modélisation du chaînage logique des événements de traçabilité*

La figure 3 montre que chaque événement est lié au précédent par une empreinte dérivée, ce qui transforme la simple journalisation en un mécanisme de traçabilité plus robuste. Dans le contexte de la gestion des fonctionnaires, cela signifie qu'une création, une modification, une validation ou une exportation peut être retrouvée, attribuée et replacée dans une séquence cohérente [13].

Afin de rendre la proposition plus opérationnelle, le mécanisme de traçabilité est résumé par l'algorithme suivant, qui formalise l'enregistrement chaîné de chaque événement administratif.

4.5. Contrôle d'accès et gouvernance des opérations

Le système proposé associe la traçabilité à une gestion des droits fondée sur les rôles (RBAC). Cette articulation est essentielle, car une trace n'a de valeur que si elle est reliée à un cadre d'autorisation explicite.
Formellement, si Perm(r) désigne l'ensemble des permissions associées au rôle r, une opération n'est autorisée que si :

$$(a, o) \in Perm(r)$$

Algorithme 1 : Enregistrement chaîné d'un événement de traçabilité

```
Entrées  : u (utilisateur), r (rôle), a (action), o (objet),
t (horodatage), ip (adresse IP), h_prev (empreinte précédente)
Sortie   : h_curr (empreinte courante)
_____________________________________________________
1. payload  ←  concat(u, r, a, o, t, ip)
2. h_curr   ←  H(payload || h_prev)
3. log      ←  (u, r, a, o, t, ip, h_prev, h_curr)
4. stocker log dans Journaux_audit
5. retourner h_curr
```

Algorithme 2 : Détection des irrégularités administratives et salariales

```
Entrées  : table AGENT, table PAIE
Sorties  : listes des dossiers litigieux, doublons,
           matricules d'emprunt, incohérences salariales
─────────────────────────────────────────────────────────
importer AGENT et PAIE dans la base centralisée
pour chaque dossier d dans AGENT faire
    vérifier l'unicité de l'identité et du matricule
    comparer le matricule de d avec les enregistrements de PAIE
    vérifier les règles de cohérence administrative et salariale
    si duplication détectée alors
        classer d comme doublon
    sinon si discordance matricule/paie alors
        classer d comme matricule d'emprunt
    sinon si violation des règles salariales alors
        classer d comme incohérence salariale
    sinon
        marquer d comme dossier régulier
    journaliser la décision prise sur d
fin pour
calculer les indicateurs globaux et l'impact financier estimé
retourner les catégories détectées
```

Cette règle permet d'encadrer les actions possibles sur les dossiers administratifs et de distinguer les opérations normales des tentatives non autorisées. Les recherches récentes sur la sécurité des flux de données en RBAC montrent que ce lien entre rôle, permission et intégrité des opérations est central pour maîtriser la confidentialité et la sécurité dans les systèmes critiques [14].

4.6. Données utilisées et implémentation expérimentale

Le prototype s'appuie sur deux fichiers sources : un fichier AGENT, contenant les informations administratives des fonctionnaires, et un fichier PAIE, contenant les données salariales associées. Ces deux sources sont importées dans une base PostgreSQL hébergée dans un environnement cloud sécurisé, où elles sont structurées en tables logiques.

L'implémentation expérimentale suit une logique réaliste : importation de données existantes, centralisation dans une base relationnelle, exploitation via une interface Web, puis journalisation systématique des opérations.

4.7. Indicateurs méthodologiques et logique d'évaluation

La méthodologie se prolonge par une phase d'évaluation adossée à des indicateurs concrets : nombre de dossiers réguliers, nombre de dossiers litigieux, taux de doublons, taux de matricules d'emprunt, couverture de l'audit, impact financier mensuel estimé.
Le taux d'une anomalie c est mesuré par :

$$R_{\{c\}} = Nc/N$$

où Nc représente le nombre de cas de la catégorie c, et N le nombre total de dossiers analysés.

La couverture de la traçabilité est mesurée par :

$$Cov_{\{audit\}} = Nlog/Nops$$

Ces indicateurs permettent de relier la traçabilité à des effets observables sur la qualité des données et sur la dépense publique.

5. Matériels et méthodes

5.1. Environnement technologique

Le prototype développé repose sur une architecture Web distribuée intégrant des technologies modernes de développement applicatif et de gestion de bases de données. L'objectif était de concevoir un environnement capable de centraliser les données administratives et salariales, d'assurer leur traçabilité et de permettre leur exploitation via une interface accessible aux utilisateurs habilités.

Tableau 2 : Technologies utilisées dans le prototype

Composant	Technologie	Rôle dans le système
Interface utilisateur	React	Interface Web pour la consultation et la gestion des agents
Backend applicatif	Django	Traitement des requêtes, règles métier, API
Base de données	PostgreSQL	Stockage centralisé des données administratives
Protocole de sécurité	HTTPS	Sécurisation des échanges
Journalisation	Logs applicatifs	Traçabilité des opérations
Hébergement	Infrastructure cloud	Centralisation et accessibilité du système

5.2. Sources de données utilisées

L'expérimentation repose sur deux ensembles de données administratives : le fichier AGENT, contenant les informations administratives des fonctionnaires (identifiant, nom, administration, statut, etc.), et le fichier PAIE, contenant les données relatives à la rémunération des agents. Ces fichiers constituent les principales sources d'information pour la gestion des fonctionnaires. Ils sont importés dans la base de données PostgreSQL et structurés sous forme de tables relationnelles exploitables par l'application.

5.3. Structure des données

Après importation, les données sont organisées en plusieurs tables relationnelles : Fonctionnaires, Paies, Administrations, Banques et Journaux_audit. La table Journaux_audit joue un rôle central dans le système, car elle enregistre toutes les opérations significatives effectuées sur
les données.

Tableau 3 : Exemple de structure de la table de traçabilité

Champ	Description
id_log	Identifiant de la trace
utilisateur	Utilisateur ayant effectué l'action
role	Rôle associé à l'utilisateur
action	Type d'opération réalisée
objet	Élément concerné
horodatage	Date et heure de l'action
adresse_ip	Adresse IP de l'utilisateur
empreinte	Empreinte cryptographique

5.4. Implémentation des mécanismes de sécurité

Afin de garantir l'intégrité et la confidentialité des données administratives, plusieurs mécanismes de sécurité ont été intégrés au prototype : authentification des utilisateurs, gestion des rôles et des permissions, chiffrement des communications via HTTPS, journalisation des actions, et sauvegarde régulière de la base de données. Ces mécanismes sont conformes aux recommandations récentes sur la sécurité des architectures cloud [15].

6. Résultats et discussion

6.1. Cadre de lecture des résultats

L'évaluation du système proposé a été menée à partir des données administratives et salariales importées dans le prototype. Les résultats doivent être interprétés comme des indicateurs de contrôle et d'assainissement, et non comme une partition exhaustive et strictement disjointe de tous les dossiers. En effet, certaines catégories relèvent d'un statut global de certification, tandis que d'autres correspondent à des signaux d'irrégularité plus ciblés, susceptibles de recouvrir partiellement un même dossier.

L'analyse porte sur trois dimensions complémentaires : (i) la détection des irrégularités administratives, (ii) la robustesse de la traçabilité, (iii) l'impact budgétaire potentiel du dispositif.

6.2. Résultats quantitatifs principaux

Le tableau 4 présente les résultats suivants : nombre initial de fonctionnaires de 1 425 086, dont 761 725 certifiés réguliers, 101 278 agents certifiés litigieux, 56 813 doublons, 43 869 matricules d'emprunt, 2 237 cas de salaires incohérents, 392 faux matricules, 112 cas de cumul et 92 agents fictifs.

Tableau 4 : Résultats quantitatifs

Indicateur	Nombre	Taux sur l'effectif initial
Fonctionnaires certifiés réguliers	761 725	53,45 %
Agents certifiés litigieux	101 278	7,11 %
Fonctionnaires doublons	56 813	3,99 %
Matricules d'emprunt	43 869	3,08 %
Salaires incohérents	2 237	0,16 %
Faux matricules	392	0,03 %
Fonctionnaires cumulards	112	0,01 %
Agents fictifs	92	0,01 %

6.3. Visualisation des irrégularités détectées

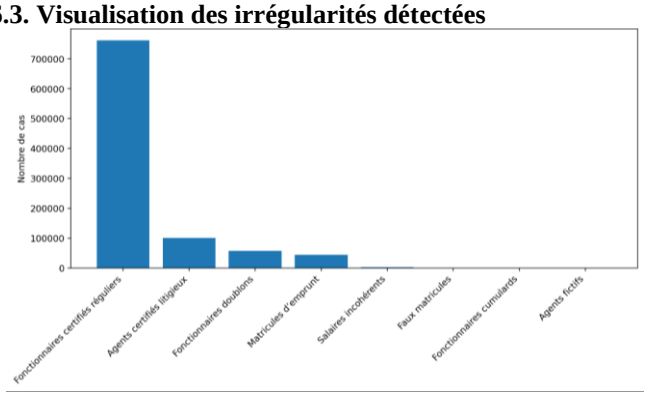


Figure 4. *Principales catégories détectées par le système*

La Figure 4 montre clairement que les agents litigieux, les doublons et les matricules d'emprunt dominent la structure des anomalies détectées. Ce résultat indique que le cœur du problème administratif n'est pas seulement la fraude brute, mais aussi la désynchronisation des identités, la redondance des dossiers et l'instabilité des mécanismes d'identification.

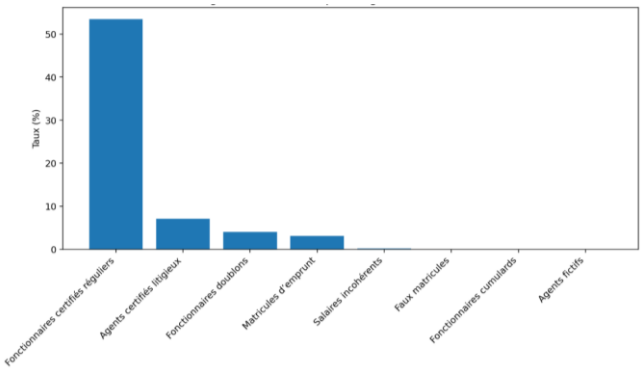


Figure 5. *Poids de chaque catégorie sur l'effectif initial*

La Figure 5 normalise les résultats par rapport à l'effectif initial. On observe que les agents litigieux représentent environ 7,11 % de l'effectif initial, les doublons 3,99 %, et les matricules d'emprunt 3,08 %. Pour un système censé porter des données sensibles de gestion publique, ces ordres de grandeur sont suffisamment élevés pour justifier un mécanisme de traçabilité robuste et permanent.

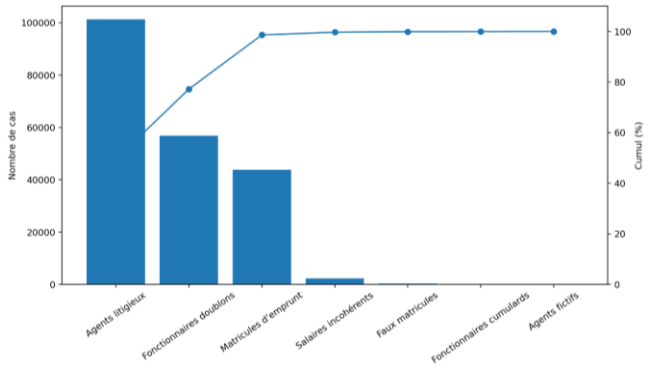


Figure 6. *Analyse de Pareto des irrégularités détectées*

L'analyse de Pareto confirme que la grande majorité de la charge d'irrégularité est portée par un petit nombre de catégories dominantes. Cette lecture suggère qu'une stratégie d'assainissement prioritaire centrée sur les dossiers litigieux, les doublons et les matricules d'emprunt produirait le plus fort gain administratif à court terme.

6.4. Robustesse de la traçabilité et auditabilité

Le système proposé affirme que la traçabilité par logs couvre 100 % des actions auditées, avec conservation des informations liées aux modifications, à la date et à l'adresse IP. Le système n'est pas seulement un outil d'importation ou de consultation, mais un véritable dispositif de reconstruction des opérations administratives.

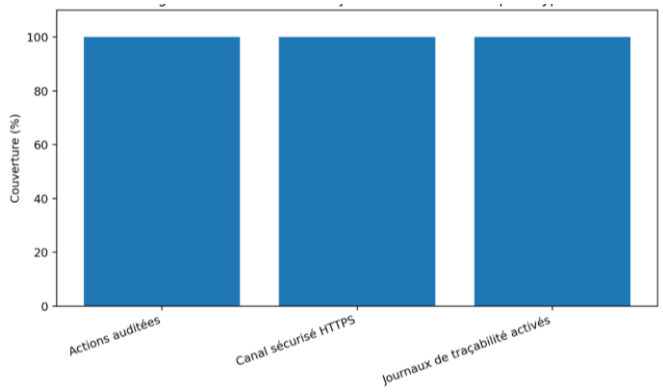


Figure 7. *Indicateurs de traçabilité décrits dans le prototype*

Dans notre cas, la traçabilité joue trois rôles simultanés : (i) elle attribue les actions à des utilisateurs identifiés ; (ii) elle permet l'audit a posteriori des manipulations ; (iii) elle transforme les opérations administratives en objets vérifiables. Ce troisième point est particulièrement important dans une administration publique, où l'enjeu n'est pas seulement de savoir qu'une donnée existe, mais de pouvoir expliquer qui l'a créée, modifiée, validée ou exportée, et à quel moment.

6.5. Impact financier des irrégularités détectées

Le prototype propose une estimation de l'impact financier mensuel en retenant un salaire moyen de 300 000 CDF pour trois catégories : agents litigieux, agents fictifs et fonctionnaires doublons. L'exposition budgétaire mensuelle ainsi calculée atteint 47 454 900 000 CDF, soit environ 16 millions USD par mois.

Tableau 5 : Impact financier mensuel estimé

Catégorie	Nombre	Impact mensuel
Agents litigieux	101 278	30 383 400 000 CDF
Agents fictifs	92	27 600 000 CDF
Fonctionnaires doublons	56 813	17 043 900 000 CDF
Total	**158 183**	**47 454 900 000 CDF**

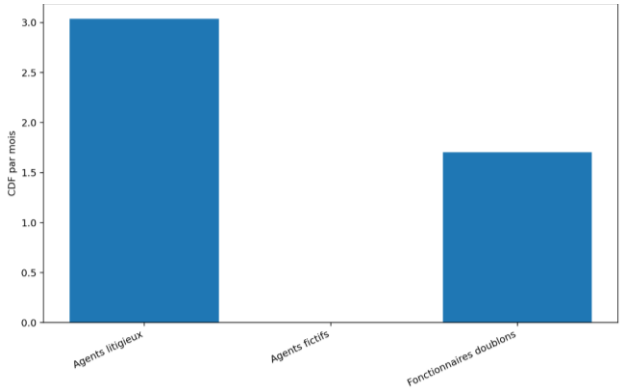


Figure 8. *Impact financier mensuel des irrégularités retenues*

6.6. Projection annuelle et analyse de sensibilité

En annualisant l'estimation mensuelle, on obtient :

$$I_{\{annuel\}} = 12 \times I_{\{m\}} = 12 \times 47{,}454{,}900{,}000$$

d'où :

$$I = 569{,}458{,}800{,}000\ CDF$$

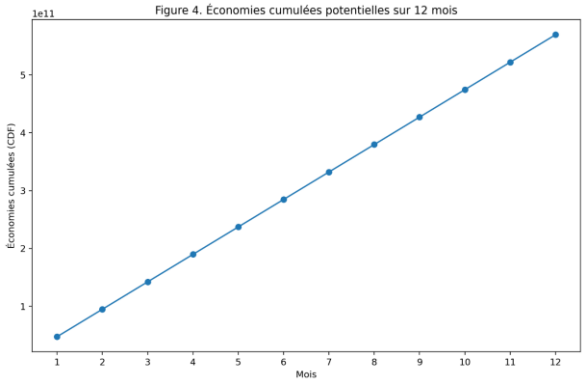


Figure 9. *Économies cumulées potentielles sur 12 mois*

Cette projection permet de repositionner l'apport du système proposé. La traçabilité n'est plus seulement un mécanisme technique de conservation des logs ; elle devient un instrument de pilotage budgétaire. À l'échelle annuelle, même en restant dans l'hypothèse prudente, l'enjeu financier devient considérable. Il faut d'ailleurs souligner que cette estimation reste conservatrice, car elle n'intègre pas explicitement d'autres catégories comme les matricules d'emprunt ou les salaires incohérents.

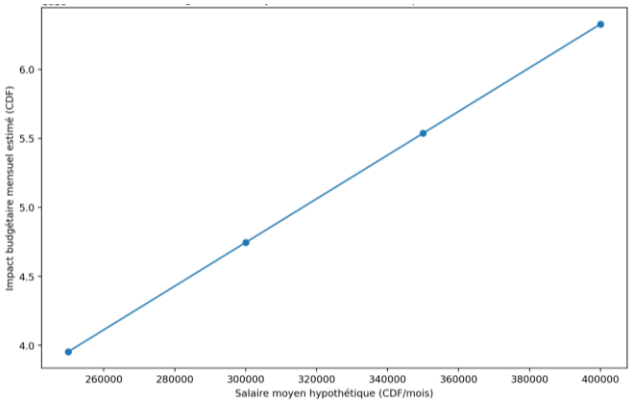


Figure 10. *Analyse de sensibilité de l'impact financier*

6.7. Discussion

Les résultats obtenus permettent de défendre quatre arguments principaux.

Premièrement, le système est pertinent pour l'assainissement administratif. L'identification de plus de 100 000 dossiers litigieux et de plusieurs dizaines de milliers de doublons ou de matricules d'emprunt montre que la centralisation cloud, lorsqu'elle est couplée à la traçabilité, agit comme un révélateur structurel de dysfonctionnements administratifs.

Deuxièmement, la traçabilité renforce la gouvernance, pas seulement la sécurité. Dans ce travail, la traçabilité n'est pas réduite à une fonction de cybersécurité. Elle devient un mécanisme de gouvernance publique, car elle soutient la transparence, la responsabilisation des acteurs et la justification des opérations [9].

Troisièmement, les logs doivent être contextualisés pour être réellement exploitables. Les recherches récentes sur la détection d'anomalies dans les environnements cloud insistent sur le fait que les logs bruts ne suffisent pas : il faut les replacer dans une structure temporelle et contextuelle [5][16].

Quatrièmement, l'intérêt budgétaire est un argument fort pour la décision publique. L'estimation mensuelle de 47,45 milliards CDF transforme une contribution technique en argument de politique publique, permettant de justifier l'investissement dans une architecture sécurisée au nom de la maîtrise de la masse salariale et de la rationalisation budgétaire [6][9].

7. Conclusion et perspectives

Cet article a montré que la traçabilité des données dans un environnement cloud peut constituer un levier concret d'assainissement du fichier des agents publics. À partir du cas de la gestion des fonctionnaires de l'État en République démocratique du Congo, nous avons proposé une architecture en trois couches combinant centralisation des données, contrôle d'accès, journalisation des opérations et auditabilité.

Les résultats obtenus mettent en évidence un volume important d'irrégularités : 101 278 dossiers litigieux, 56 813 doublons et 43 869 matricules d'emprunt, ainsi qu'un impact budgétaire mensuel estimé à 47 454 900 000 CDF pour les catégories monétisées. Ces résultats montrent que la traçabilité ne doit pas être considérée comme une simple fonction technique de suivi, mais comme un instrument de gouvernance, de transparence et de maîtrise de la masse salariale.

Ce travail peut être prolongé dans plusieurs directions. D'abord, il serait pertinent d'intégrer des méthodes avancées de détection d'anomalies fondées sur l'analyse contextuelle et temporelle des logs. Ensuite, un déploiement institutionnel à plus grande échelle nécessiterait un cadre plus explicite de gouvernance des données. Enfin, une autre perspective importante serait d'étendre l'auditabilité du système vers des mécanismes de preuve renforcée et vers des outils d'aide à la décision publique assistés par l'IA.

Références

[1] Brzozowska-Rup, K., Nowakowska, M., & Zdradzisz, M. (2024). Cloud computing in the Polish public administration: current state and development prospects. Technological Forecasting and Social Change, 205, 123500. DOI: 10.1016/j.techfore.2024.123500

[2] Alkhasawneh, R., Che Cob, Z., & Abdul Latif, A. B. (2025). Cloud Computing Adoption in Government Organizations in Developing Countries. International Journal of Public Administration in the Digital Age. DOI: 10.4018/IJPADA.368246

[3] Bernardo, B. M. V., et al. (2024). Data governance & quality management — Innovation and breakthroughs across different fields. Journal of Innovation & Knowledge, 9(4), 100598. DOI: 10.1016/j.jik.2024.100598

[4] Wang, H., Zhang, Y., Wang, X. A., & Yang, X. (2024). An improved identity-based public audit protocol for cloud storage. Heliyon, 10(16), e36273. DOI: 10.1016/j.heliyon.2024.e36273

[5] Jilcha, L. A., Kim, D.-H., & Kwak, J. (2025). Temporal Decay Loss for Adaptive Log Anomaly Detection in Cloud Environments. Sensors, 25(9), 2649. DOI: 10.3390/s25092649

[6] Gabrielli, G., Magri, C., Medioli, A., & Marchini, P. L. (2024). The power of big data affordances to reshape anti-fraud strategies. Technological Forecasting and Social Change, 205, 123507. DOI: 10.1016/j.techfore.2024.123507

[7] Cejudo, A., et al. (2025). Scalable Big Data Platform With End-to-End Traceability for Health Data Monitoring in Older Adults. JMIR Medical Informatics, 13, e81701. DOI: 10.2196/81701

[8] Jlil, M., Jouti, K., Boumhidi, J., & Loqman, C. (2025). Improving traceability in e-governance file-sharing systems: the Moroccan justice system as a use case. International Journal of Information Security, 24, 9. DOI: 10.1007/s10207-024-00919-8

[9] Aldemir, C., & Uçma Uysal, T. (2025). Artificial Intelligence for Financial Accountability and Governance in the Public Sector. Administrative Sciences, 15(2), 58. DOI: 10.3390/admsci15020058

[10] Goswami, P., et al. (2024). Investigation on storage level data integrity strategies in cloud computing. Journal of Cloud Computing. DOI: 10.1186/s13677-024-00605-z

[11] Qatawneh, N. (2024). Building a framework to drive government systems' adoption of cloud computing through IT knowledge. Discover Sustainability, 5, 282. DOI: 10.1007/s43621-024-00427-8

[12] Storey, M.-A., et al. (2025). Guiding principles for

mixed methods research in software engineering. Empirical Software Engineering, 30, 138. DOI: 10.1007/s10664-025-10629-x

[13] Chen, F., et al. (2024). Public cloud object storage auditing: Design, implementation, and analysis. Journal of Parallel and Distributed Computing, 189, 104870. DOI: 10.1016/j.jpdc.2024.104870
[14] Logrippo, L. (2025). Data flow security in Role-based access control. Journal of Information Security and Applications, 90, 103997. DOI: 10.1016/j.jisa.2025.103997
[15] Ali, S., et al. (2025). Security and privacy in multi-cloud and hybrid cloud environments. Computers & Security, 157, 104599. DOI: 10.1016/j.cose.2025.104599
[16] Franzil, M., et al. (2026). Sharpening Kubernetes audit logs with context awareness. Computer Networks, 276, 111890. DOI: 10.1016/j.comnet.2025.111890
[17] Scommegna, L., Verdecchia, R., & Vicario, E. (2024). Unveiling Faulty User Sequences: A Model-Based Approach to Test Three-Tier Software Architectures. Journal of Systems and Software, 212, 112015. DOI: 10.1016/j.jss.2024.112015
[18] Serafin, P. (2024). Modern web technologies — frameworks, advantages, disadvantages and optimal applications. Computer Science and Mathematical Modelling, 19, 25–34. DOI: 10.5604/01.3001.0055.0854
[19] Cevallos-Salas, D., Estrada-Jiménez, J., & Guamán, D. S. (2024). Application layer security for Internet communications: A comprehensive review. Computers & Electrical Engineering, 119, 109498. DOI: 10.1016/j.compeleceng.2024.109498
[20] Thompson, Y., et al. (2025). Application of the data quality framework to administrative data on child maltreatment. Child Abuse & Neglect, 169, 107646. DOI: 10.1016/j.chiabu.2025.107646
[21] Buoncristiano, M., et al. (2024). Detective Gadget: Generic Iterative Entity Resolution over Dirty Data. Data, 9(12), 139. DOI: 10.3390/data9120139
[22] Frank, M., Kohn, V., & Holten, R. (2024). Q methodology and the sociotechnical perspective. Information Systems and e-Business Management, 22, 599–631. DOI: 10.1007/s10257-024-00679-x
[23] Kudina, O., & van de Poel, I. (2024). A sociotechnical system perspective on AI. Minds and Machines, 34, 21. DOI: 10.1007/s11023-024-09680-2
[24] Gregor, S., & Zwikael, O. (2024). Design science research and the co-creation of project management knowledge. International Journal of Project Management, 42(3), 102584. DOI: 10.1016/j.ijproman.2024.102584
[25] Moutinho, J., Fernandes, G., & Rabechini, R. Jr. (2024). Evaluation in design science. Evaluation and Program Planning, 102, 102366. DOI: 10.1016/j.evalprogplan.2023.102366
[26] Kleinsteuber, E., et al. (2024). Managing Provenance Data in Knowledge Graph Management Platforms. Datenbank-Spektrum, 24(1), 43–52. DOI: 10.1007/s13222-023-00463-0
[27] Dibowski, H. (2024). Full Traceability and Provenance for Knowledge Graphs. Formal Ontology in Information Systems. DOI: 10.3233/FAIA241309
[28] Johns, M., Baum, L., & Prasser, F. (2025). Tracking provenance in clinical data warehouses for quality management. International Journal of Medical Informatics, 193, 105690. DOI: 10.1016/j.ijmedinf.2024.105690