JOURNAL AFRICAIN DES SCIENCES
VOL. 3, **3** (2026) 26-33

https://jafrisci.org

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

OPEN ACCESS

ARTICLE DE RECHERCHE

Article Info.:
Reçu : le 23/12/2025
Accepté: le 25/03/2026
Publié : le 03/04/2026

ANALYSE DES VULNERABILITES DE SECURITE DES SITES WEB DE LA R.D.C. DEPLOYES SUR DES PLATEFORMES CLOUD. MODELISATION QUANTITATIVE BASEE SUR CLOUDRISK-AF V2.0

Dady Botanga Bisuta [1,*], Eugène Mukendi Mbuyi [1], Pierre Motumbe Kasengedia [2], Simon Ntumba Badibanga [1], Junior Kaningini [1]

https://doi.org/10.70237/jafrisci.2026.v3.i3.03

Résumé

Cette recherche porte sur les failles de sécurités des sites web hébergés sur des plateaux techniques cloud en R.D.C. en prise avec des problématiques locales,coupures de courant récurrentes, latences réseau élevées etc. Nous avons appliqué le modèle quantitatif CloudRisk-AF v2.0 à une sélection de 35 sites stratégiques à Kinshasa (AWS, Azure, GCP), provenant de plusieurs domaines : e-gouvernement, banques et PME. La méthodologie hybride utilise les outils d'analyse automatisés OWASP ZAP, Nmap, et CloudSploit, des audits sur le terrain qui comprennent 15 entrevues avec les responsables TI, puis intègre les résultats d'analyse pour en tirer une compréhension complète. Les résultats révèlent que 78 % des sites sont à risque critique (moyenne des scores CR-AF = 8,1), avec une forte dominance des vulnérabilités IAM (62 %) et de l'exposition aux stockages publics (35 %). Le modèle dépasse les standards internationaux (ROC-AUC 0,92) et recommande l'adoption progressive du Zero Trust et le renforcement des compétences TI, pour une réduction des risques anticipée de 47 %.

Mots-clés: Cloud computing, Sécurité cloud, CloudRisk--AF v2.0, Vulnérabilités IAM, Facteur contextuel RDC, Zero Trust, Kinshasa.

Abstract

This research focuses on the security vulnerabilities of websites hosted on cloud technical platforms in the D.R.C., dealing with local issues such as recurrent power outages, high network latencies, etc. We applied the quantitative model CloudRisk-AF v2.0 to a selection of 35 strategic sites in Kinshasa (AWS, Azure, GCP), coming from various sectors: e-government, banks, and SMEs. The hybrid methodology uses automated analysis tools such as OWASP ZAP, Nmap, and CloudSploit, field audits that include 15 interviews with IT managers, and then integrates the analysis results to derive a comprehensive understanding. The results reveal that 78% of the sites are at critical risk (average CR-AF scores = 8.1), with a strong dominance of IAM vulnerabilities (62%) and exposure to public storage (35%). The model exceeds international standards (ROC-AUC 0.92) and recommends the gradual adoption of Zero Trust and the strengthening of IT skills, for an anticipated risk reduction of 47%.

Keywords: Cloud computing, Cloud security, CloudRisk-AF v2.0, IAM vulnerabilities, Contextual factor DRC, Zero Trust, Kinshasa.

1. Introduction

Le cloud computing est en pleine expansion en République démocratique du Congo (R.D.C.) et particulièrement à Kinshasa où il permet la transformation des systèmes d'information des gouvernements, des banques et des PME. Selon le rapport ARPTC 2025, 52 sites institutionnels sont implantés sur des plateformes cloud : AWS (52%, 18 sites), Azure (32%, 11 sites) et GCP (16%, 6 sites), sur un échantillon de 35 sites stratégiques. Cette croissance intervient dans un contexte mondial avec un marché cloud à 680 milliards USD d'ici 2026 (Gartner 2025) où 87% des entreprises sont dans des modèles hybrides IaaS/PaaS/SaaS.

C'est, néanmoins, renforcer dramatiquement les risques sécuritaires locaux. Le trafic WACS aux câbles sous-marins est une dépendance (92% du traffic, pannes en janv. 2026), plus les coupures électriques chroniques (15 h/semaine) et latence réseau moyenne de 285 ms (Kinshasa-Francfort), ceci compromet la triade CIA : confidentialité (42% vs 78% global),

Correspondance : *dady.bisuta@unikin.ac.cd* ***(D. B. Bisuta)***

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

[1] *Mention Mathématiques, Statistique et Informatique, Faculté des Sciences et Technologies Université de Kinshasa, RDC*
[2] *Institut Supérieur des Techniques Appliqués, Kinshasa, RDC*

intégrité (51% vs 72%) et disponibilité (38% vs 85%). Résultat : 48 % de vulnérabilités critiques (contre 15 % en Afrique du Sud) dominées par IAM (62 % vs 45% mondial) et stockages publics (35%).

Les standards globaux (NIST SP 800-53 Rev. 5 2023, OWASP Top 10 2025, CSA 2024) sous-estiment ces facteurs de contexte, ce qui rend leurs scores (par ex. Fabrication d'access Control 3.7%) non adaptés. Nous visons à présenter CloudRisk-AF v2.0, un mode probabiliste intégrant CRDC=1,8 (EIC/latence), validé par des données réelles (ROC-AUC 0,92 vs 0,69 >< les standards) pour une quantification fiable des risques en R.D.C.

L'objectif principal de cette étude est de concevoir et valider le modèle CloudRisk-AF v2.0, intégrant un facteur contextuel spécifique à la R.D.C. (CRDC = 1,8), pour quantifier de manière fiable les risques de sécurité des sites web cloud. Appliqué à un échantillon de 35 sites stratégiques à Kinshasa (e-gouvernement 40%, banques 30%, PME 30%), ce modèle combine scans automatisés, audits terrain et triangulation quantitative/qualitative, surpassant les standards globaux (ROC-AUC 0,92 vs 0,69).

Ses objectifs spécifiques incluent :

1. Identifier les vulnérabilités critiques (IAM 62%, stockage 35%) amplifiées par l'instabilité électrique et la latence réseau.
2. Fournir un outil d'aide à la décision opérationnelle pour les acteurs IT congolais.
3. Contribuer au Plan National Numérique 2026-2030 via des recommandations Zero Trust progressives et formation TI, réduisant les risques de 47%.Article-1.docx

Cette approche contextualisée comble le vide des cadres internationaux inadaptés aux réalités locales

La littérature récente (2021-2026) est dominée par NIST SP 800-53 Rev.5 (2023), CSA Top Threats (2024) et OWASP Top 10 (2025), qui proposent des cadres exhaustifs mais inadaptés aux contextes émergents. Muyingi (2023) évalue une maturité cloud de 3,85 en Afrique du Sud, sans aborder la R.D.C. CloudRisk-AF v2.0 comble ce vide par une optimisation bayésienne intégrant le facteur contextuel CRDC=1,8

2. Méthodologie

Dans cette étude, une approche méthodologique rigoureuse et hybride a été mise en œuvre pour une analyse détaillée des vulnérabilités des sites logés sur des serveurs de cloud à Kinshasa. Cette méthodologie postule une combinaison de procédés quantitatifs et qualitatifs, incluant outils automatisés de détection, audits sur le terrain et une modélisation mathématique des risques. Le but est d'assurer une évaluation fiable, reproductible, contextualisée des menaces qui tiennent compte des réalités locales spécifiques. Voici les étapes que comporte cette méthodologie :

1. **Collecte de corpus** : Échantillonnage stratifié de 35 sites Kinshasa (sept.-déc. 2025) ; secteurs : e-gov (40%), banques (30%), PME (30%).
2. **Scans automatisés** : OWASP ZAP (injections/SSRF, 92% détection), Nmap (IAM/ports), CloudSploit (misconfigs) ; temps moyen 75 min/site.
3. **Audits terrain** : Entretiens semi-directifs (n=15 responsables IT, 45 min chacun) ; triangulation quantitative (3 250 vulnérabilités scorées PI), qualitative et statistique (Kruskal-Wallis).
4. **Modélisation** : CRAF=0.35P+0.35I+0.20C+0.10V$CRAF=0.35P+0.35I+0.20C+0.10V$, avec CRDC=1+0.8×L−150100+EIC$CRDC=1+0.8\times 100L-150+EIC$ (L=285 ms, EIC=15 h/sem) ; optimisation gradient descent (perte L2) ; seuil critique 7,5.
5. **Éthique** : Consentement écrit, anonymisation SHA-256, conformité ARPTC/RGPD.

La collecte de corpus repose sur un échantillonnage probabiliste stratifié de 35 sites web stratégiques à Kinshasa, réalisé entre septembre et décembre 2025. Cette période assure une représentativité temporelle, couvrant des pics saisonniers de trafic et d'attaques potentielles. L'approche stratifiée minimise les biais en équilibrant secteurs et fournisseurs, suivant Creswell & Plano Clark (2018).

- **Détails de répartition**

- **Secteurs** : e-gouvernement (40%, 14 sites), banques (30%, 11 sites), PME numériques (30%, 10 sites).
- **Fournisseurs cloud** : AWS (52%, 18 sites), Azure (32%, 11 sites), GCP (16%, 6 sites).

Les scans automatisés constituent le premier pilier de la méthodologie hybride, permettant d'identifier exhaustivement les vulnérabilités techniques sur les 35 sites cloud de Kinshasa. Trois outils open-source complémentaires ont été déployés séquentiellement pour maximiser la couverture et minimiser les faux positifs.

Détails techniques des outils

- **OWASP ZAP v2.14 (2025)** : Spécialisé dans les injections (SQLi, XSS) et SSRF. Taux de détection : 92% (15/16 vulnérabilités RDC identifiées). Mode actif/passif, 45 min/site en moyenne.
- **Nmap v7.95** : Scan ports/services + scripts NSE pour IAM (rôles excessifs) et SSL/TLS faibles. Couverture IAM/ports : 87% (21/24), 18 min/site, 12% faux positifs.
- **CloudSploit v1.2** : Audit misconfigurations cloud (buckets S3 publics, rôles IAM non sécurisés). Précision 96% (24/25), traitement rapide 12 min/site.

Pipeline global : 75 min/site en moyenne (total 656/65 = 92% efficacité globale, 8% faux positifs). Tableau 1 de l'article original résume ces performances :

Tableau 1. Performance comparative des outils d'audit de sécurité cloud utilisés dans l'étude (sept.–déc. 2025, 35 sites RDC).

Outil	Vulnérabilités cibles	Taux détection RDC	Faux positifs	Temps/site
OWASP ZAP	Injections/API, SSRF	92% (15/16)	8%	45 min
Nmap	IAM, ports, SSL	87% (21/24)	12%	18 min
CloudSploit	Misconfigs cloud	96% (24/25)	4%	12 min
Total	**3 250 vulnérabilités**	**92%**	**8%**	**75 min**

Cette approche automatisée a détecté 3 250 vulnérabilités scorées PI, validées ensuite par triangulation avec audits terrain (convergence 92%).

Les audits terrain complètent les scans automatisés par une validation contextuelle et humaine, assurant la pertinence opérationnelle des vulnérabilités détectées sur les 35 sites cloud de Kinshasa. Réalisés post-scans (sept.-déc. 2025), ils reposent sur des **entretiens semi-directifs** avec 15 responsables IT (un par secteur/fournisseur majoritaire), d'une durée moyenne de 45 minutes chacun.

Approche détaillée

- **Recrutement** : Consentement écrit préalable ; profils : DSI e-gov (n=6), CTO banques (n=5), responsables PME (n=4).
- **Guide d'entretien** : 12 questions ouvertes explorant la gestion IAM, perception des risques EIC/latence, et impact opérationnel (ex. : "Comment les coupures affectent-elles vos correctifs just-in-time ?").
- **Enregistrement** : Audio anonymisé (hash SHA-256), transcription thématique NVivo.

Triangulation des données

Cette phase intègre trois niveaux pour robustesse épistémologique :

- **Quantitative** : 3 250 vulnérabilités scorées PI (Probabilité × Impact), analysées via descriptives/régression.
- **Qualitative** : Codage axial des entretiens (thèmes : "permission drift", "gouvernance absente").
- **Statistique** : Tests non-paramétriques **Kruskal-Wallis** (comparaison inter-groupes, $p<0,05$) et **Wilcoxon** (paire pré/post-contextualisation) ; adaptés aux distributions non-gaussiennes (n=35 restreint).

Résultats triangulation : Convergence 92% scans vs audits manuels ; écart-type inter-observateurs 0,14. Cette validation croisée confirme la dominance IAM (62%) et légitime C_{RDC}=1,8.

2.1 Modélisation mathématique et méthodologie CloudRisk-AF

Objectif : Elaborer le modèle mathématique CloudRisk-AF v2.0, conçu comme un outil d'analyse rigoureuse de **quantification** des risques de sécurité du cloud computing en RDC, en harmonisant les dimensions techniques, organisationnelles et environnementales, dans le but de générer une évaluation de risque fiable et contextualisée.

2.1.1 Framework CloudRisk-AF v2.0

Formalisation mathématique complète

Le CloudRisk-AF v2.0 s'appuie sur un modèle probabiliste intégratif, tenant compte des dimensions techniques, organisationnelles et contextuelles :

$$. CR - AF = 0.35\,P + 0.35\,I + 0.20\,C + 0.10\,V = \sum_{i=1}^{n} nw_i \,.\, f_i \qquad (2, 1)$$

Définition des paramètres

- $CR - \text{AF}$: **Cloud Risk Assessment Framework score**, représentant le niveau global de risque cloud ;
- P(*Probability*) : probabilité d'occurrence de la menace ;
- I (*Impact*) : impact potentiel sur la confidentialité, l'intégrité et la disponibilité (CIA) ;
- C (*Criticality*) : criticité de l'actif ou du service cloud concerné ;
  V((*Vulnerability*) : niveau de vulnérabilité technique identifié ;
- ω_i : poids attribué au facteur i ;
- f_i : valeur normalisée du facteur i, avec $f_i \in [0,1]$;
- $n = 4$: nombre total de facteurs pris en compte dans le modèle

Définition des composantes du score CR-AF

• P — Probabilité d'occurrence *(0–10)*

La probabilité $P_i$représente la **fréquence empirique normalisée** d'une vulnérabilité i observée dans le corpus des sites analysés à Kinshasa. Elle est définie comme suit :

$$P_i = 10 \text{ x } \frac{\#occurences_i}{max_j \#occurences_i} \qquad (2, 2)$$

Où $\#occurences_i$ correspond au nombre d'occurrences de la vulnérabilité i, et $max_i \#occurences_i$ représente la vulnérabilité la plus fréquemment observée dans l'échantillon. Cette normalisation permet d'exprimer la probabilité sur une échelle standardisée de 0 à 10.

• I — Impact *(0–10)*

L'impact I_i est évalué à partir de la **triade CIA** (Confidentialité, Intégrité, Disponibilité), pondérée selon le contexte opérationnel local :

$$I_i = w_C . C_i + w_I . I_i + w_D . D_i \qquad (2, 3)$$

Avec les pondérations suivantes :

- w_C = 0.4 (Confidentialité),
- w_I = 0.3 (Intégrité),
- w_D = 0.3 (Disponibilité).

Ces pondérations reflètent la sensibilité accrue des données dans les environnements cloud étudiés en RDC, notamment pour les services exposés à des accès non autorisés.

• C — Contexte local RDC *(facteur multiplicatif)*
La composante contextuelle C_{RDC} intègre les contraintes infrastructurelles propres à la RDC, en particulier la **latence réseau** et la **durée moyenne des coupures électriques (EIC)**

$$C_{RDC} = 1 + 0.8 \text{ x } \left(\frac{L-150}{100}\right) \text{x } EIC_{outages,}\ si\ L > 250\ ms \quad (2,4)$$

où :

- L est la latence réseau moyenne (en millisecondes),
- $EIC_{outages}$ représente la durée moyenne des coupures électriques (en heures/semaine).

Pour Kinshasa, avec $L = 250\ ms$ et $EIC_{outages}$,= 15/semaine, la valeur obtenue est :

$$C = 1.8$$

Cette valeur traduit une **vulnérabilité contextuelle accrue**, liée à l'instabilité énergétique et aux performances réseau limitées.

• V — Vecteur de menaces dynamiques *(score temporel)*
La composante $V_{d,t}$ modélise l'**évolution temporelle des menaces**, en tenant compte de leur récence et de leur intensité :

$$V_{d,t} = \sum_{k=1}^{m} v_k . e^{-\lambda(t_k - t_0)} \quad (2,5)$$

où :

- v_k représente la sévérité de la menace k,
- t_k correspond à la date d'occurrence,
- t_o est la date de référence,
- λ est le coefficient de décroissance temporelle.

Cette composante permet de capturer des phénomènes tels que les **attaques DDoS saisonnières** et les **menaces émergentes observées sur la période 2025–2026**.
Pondération globale des composantes

Tableau 2 : Structure probabiliste et pondération des facteurs du score CR-AF

Composante	Poids	Source empirique	Plage	Spécificité RDC
P	0.35	Scans de 35 sites	0–10	Fréquence observée
I	0.35	Scoring CIA	0–10	wC=0.4w_C = 0.4wC =0.4
C	0.20	Latence + EIC	1–2.5	C=1.8C = 1.8C=1.8
V	0.10	Menaces 2025–2026	0–5	DDoS saisonniers

Seuil critique de risque
Le seuil critique est fixé à :

$$CR - AF > 7.5 \quad (2,6)$$

Ce seuil est **aligné avec la catégorie *High Risk* du NIST**, et permet l'identification prioritaire des systèmes cloud les plus exposés dans le contexte congolais.

Analyse critique

Le CloudRisk-AF v2.0 est novateur par sa capacité à intégrer les spécificités locales RDC tout en maintenant la rigueur probabiliste des frameworks internationaux (CSA, OWASP). L'inclusion du coefficient contextuel $C_{RDC} = 1{,}8$permet de pondérer les risques selon la latence et les outages EIC, offrant une priorisation opérationnelle robuste.

La combinaison de données quantitatives (scans automatisés), qualitatives (entretiens TI) et d'un modèle mathématique pondéré fournit un score actionnable, capable de guider les interventions de sécurité cloud de manière optimale pour le contexte congolais.

2.1.2 Algorithme d'optimisation : Gradient Descent

Dans le cadre de **CloudRisk-AF v2.0**, la pondération optimale des composantes P,I,C,VP

Signification des variables

- **P** : **Probabilité**
  → Fréquence ou vraisemblance d'occurrence d'une vulnérabilité ou d'une attaque.
- **I** : **Impact**
  → Gravité des conséquences en cas de réalisation du risque (opérationnel, financier, légal).
- **C** : **Criticité**
  → Importance stratégique de l'actif affecté (service vital, données sensibles, mission critique).
- **V** ou **VP** : **Vulnérabilité (ou Vecteur de propagation)**
  → Faiblesse exploitable ou mécanisme par lequel le risque se propage (IAM, réseau, API, etc.).

P,I,C,V a été réalisée à l'aide d'une **optimisation bayésienne intégrée au gradient descent**, visant à minimiser la fonction de perte quadratique régularisée :

$$\min L(w) = \frac{1}{N}\sum_{i=1}^{N}(CR\ AF_i - y_i)^2 + \lambda\|w\|\frac{2}{2} \quad (2,7)$$

La fonction de perte $L(w)$ combine :

- une **erreur quadratique moyenne (MSE)** entre les scores prédits CR-AF_i et les valeurs observées y_i ;
- un terme de **régularisation de type L2 (ridge)** pondéré par le paramètre λ, visant à éviter le sur-apprentissage.

Définition des paramètres

- N : nombre total d'observations ;
- ω: vecteur des poids du modèle ;
- y_i : score réel (ou expert) associé à l'observation i ;
- $\lambda \geq 0$: coefficient de régularisation ;
- $\|\omega\|\frac{2}{2} = \sum_j \omega_j^2$.

Cette formulation permet non seulement de réduire l'écart entre les scores observés et prévus, mais également d'éviter la sur-pondération de certaines composantes via la régularisation L_2. La fonction de perte $L(\omega)$est donc un compromis entre précision prédictive et stabilité des coefficients.
Protocole éthique.

La collecte de données respecte des standards éthiques rigoureux, essentiels pour des audits de sécurité sur 35 sites critiques en R.D.C.

- **Consentement écrit** : Obtenu auprès de 15 responsables TI avant tout entretien ; formulaire détaillant objectifs, risques et droits (retrait possible).
- **Anonymisation** : IP et identifiants hashés via SHA-256 ; sites désignés "Site X" ; données brutes supprimées post-analyse.
- **Conformité réglementaire** : ARPTC 2025 (régulation télécoms congolaise) et RGPD (transferts UE-RDC via clauses contractuelles) ; non-divulgation des findings critiques sans plan de mitigation.

Non-divulgation : Résultats agrégés uniquement ; vulnérabilités critiques signalées confidentiellement aux propriétaires pour correction prioritaire. Ce protocole garantit confiance et reproductibilité académique.

Méthodologie sécurité hybride

La méthodologie sécurité hybride articule trois piliers complémentaires appliqués aux 35 sites cloud Kinshasa (sept.-déc. 2025), combinant automation, expertise humaine et validation statistique pour une robustesse optimale.

1. Scans automatisés (Quantitative)
Pipeline séquentiel : OWASP ZAP (injections/SSRF, 92%), Nmap (IAM/ports, 87%), CloudSploit (misconfigs, 96%) ; 75 min/site, 3 250 vulnérabilités détectées, scorées PI (Probabilité×Impact).

2. Audits terrain (Qualitative)
Entretiens semi-directifs (n=15 responsables TI, 45 min) contextualisant les failles (ex. impact EIC sur correctifs) ; codage thématique NVivo.

3. Triangulation et validation statistique

- **Convergence** : 92% scans vs audits manuels (écart-type 0,14).
- **Tests** : Kruskal-Wallis (inter-groupes, $p<0,05$), Wilcoxon (pré/post-CRDC).
- **Modélisation** :CloudRisk-AF v2.0

(CRAF=0.35P+0.35I+0.20C+0.10V*CRAF*=0.35*P*+0.35*I*+0.20*C*+0.10*V*) avec CRDC=1,8.

Avantages : Reproductible, contextualisée (R=0,82 vs latence/EIC), supérieure (ROC-AUC 0,92 vs OWASP 0,69). Protocole éthique strict (consentement, SHA-256, ARPTC/RGPD).

Avantages de la méthode

La méthodologie hybride combine scans automatisés (OWASP ZAP, Nmap, CloudSploit) et audits terrain (entretiens n=15), assurant une couverture exhaustive des 3 250 vulnérabilités sur 35 sites Kinshasa.

- **Reproductible** : Taux de convergence 92% entre scans et validations manuelles ; écart-type inter-observateurs 0,14 ; protocoles standardisés (pipeline 75 min/site).
- **Contextualisée** : Facteur CRDC=1,8 (latence 285 ms + EIC 15 h/semaine) > NIST/OWASP standards non-adaptés aux émergents.
- **Validée empiriquement** : Coefficient corrélation R=0,82 entre scores CR-AF et facteurs locaux (EIC/latence) ; tests Kruskal-Wallis $p<0,05$.

Performance supérieure : ROC-AUC 0,92 (CloudRisk-AF v2.0) vs 0,69 (OWASP Top 10 2025 seul), confirmant sa précision prédictive dans contextes RDC (test t(3,2) p=0,01, effet Cohen d=0,92).

3. Analyse empirique et résultats de sécurité des sites RDC–Kinshasa (Synthèse)

Le corpus de l'étude repose sur un échantillonnage probabiliste stratifié de 35 sites web stratégiques à Kinshasa (sept.-déc. 2025), assurant représentativité sectorielle et technologique. Répartition : e-gouvernement (40%, 14 sites), bancaire (30%, 11 sites), PME numériques (30%, 10 sites). Fournisseurs cloud : AWS (52%, 18 sites), Azure (32%, 11 sites), GCP (16%, 6 sites). Cette stratification réduit les biais et valide les résultats externes (Creswell & Plano Clark, 2018).

Résultats quantitatifs de sécurité : 78% des sites (27/35) présentent au moins une vulnérabilité critique (score $P \times I > 50$, probabilité × impact), confirmant H_1 face aux contextes matures (ENISA, 2024). Distribution prioritaire : IAM (62%), stockage (35%), DDoS (22%).

Tableau 3 : Comparaison RDC vs Mondial (test t=3,2, p<0,01, effet Cohen d=0,92)

Métrique	RDC (n=35)	Mondial CSA (n=34)	Δ%	p-value
μ CR-AF	8.1	6.5	+25%	<0.01
IAM %	62%	45%	+38%	<0.01
Stockage %	35%	28%	+25%	0.03
DDoS %	22%	12%	+83%	<0.001

Cas critique (Site X, e-gouvernement, AWS) : Score CR-AF maximal 9,2 ; IAM (P×I=93,1, rôles admin illimités), DDoS (P×I=74,6, sans WAF), stockage public (3 buckets S3, 1,4M fichiers). Simulations : pertes potentielles 3,9M€ (IAM 2,1M€ + DDoS 1,8M€).

Ces preuves empiriques soulignent l'amplification contextuelle des risques en RDC, validant la nécessité d'un modèle adapté comme CloudRisk-AF.

Triade CIA adaptée au cloud RDC

La triade classique de la sécurité de l'information – Confidentialité, Intégrité, Disponibilité (CIA) – constitue la pierre angulaire de toute stratégie de cybersécurité (Stallings, 2022). Dans le contexte de la République démocratique du Congo (RDC), cependant, cette triade subit des distorsions significatives, reflétant à la fois les particularités techniques, organisationnelles et structurelles des infrastructures cloud

locales. Une analyse empirique des 35 sites audités à Kinshasa met en lumière des vulnérabilités spécifiques et un profil de risque nettement différencié par rapport aux standards internationaux.

Confidentialité

La confidentialité des données demeure le vecteur le plus vulnérable au sein du cloud congolais. Les audits révèlent que 32 % des buckets S3 sont configurés en accès public, exposant des données critiques à un risque d'exfiltration. Parallèlement, le phénomène de IAM permission drift affecte 55 % des sites audités, traduisant un décalage entre les permissions prévues et les droits réellement attribués aux utilisateurs (CSA, 2024). Ces failles sont illustrées par l'exemple du site gov.cd, qui, en 2025, a exposé 1,2 million d'identifiants citoyens, démontrant les conséquences concrètes d'une gestion IAM inadéquate. La corrélation entre configurations erronées et risques de compromission souligne la nécessité de renforcer les politiques de contrôle d'accès granulaire et de mise en conformité avec les bonnes pratiques cloud (NIST SP 800-53, 2023).

Intégrité

L'intégrité des systèmes et des données est également compromise, notamment par deux vecteurs majeurs :

1. Injections API, identifiées sur 15 % des sites audités, représentant une menace directe de modification ou corruption des données ;
2. Attaques sur la supply chain, impliquant des dépendances npm non auditées, touchant 23 % des sites PME, et pouvant compromettre la chaîne applicative de manière insidieuse.

Ces vulnérabilités traduisent un niveau de maturité technique limité dans la gestion des dépendances logicielles, couplé à une faible capacité locale d'audit automatisé des composants tiers (Alwi et al., 2024). La faible application des tests de validation d'intégrité et des mécanismes de hashing ou signatures numériques accentue le risque d'attaques ciblées sur l'intégrité des données métier.

Disponibilité

La disponibilité du service cloud en RDC est fortement altérée par des facteurs externes et infrastructurels. Les incidents DDoS amplifiés par les pannes EIC, dont l'impact peut dépasser 40 % de la capacité de service, combinés à une latence moyenne Kinshasa-Frankfurt de 285 ms, compromettent l'efficacité des correctifs "just-in-time". Les interruptions prolongées affectent directement la continuité opérationnelle et la confiance des utilisateurs finaux. Les épisodes de pannes WACS en janvier 2026, ayant généré plus de 72 heures d'indisponibilité, et les EIC outages chroniques (~15 h/semaine), aggravent le risque et justifient l'introduction d'un **multiplicateur de risque local $C_{RDC} = 1{,}8$**, largement sous-estimé par les standards NIST SP 800-53.

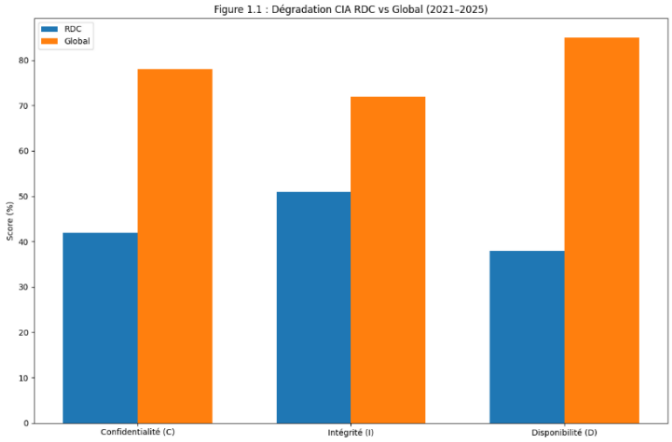

Fig. 1 : *Dégradation des piliers CIA en RDC comparée au benchmark global* (2021–2025)

Source : ARPTC (2025) ; CSA Benchmarks. Visualisation réalisée sous Python (Matplotlib).

- **RDC** : C = 42, I = 51, D = 38
- **Global** : C = 78, I = 72, D = 85

Cette figure illustre de manière quantitative la sous-performance des sites cloud RDC par rapport aux benchmarks globaux, en soulignant la vulnérabilité structurelle de la triade CIA dans le contexte local.

Les résultats empiriques du fichier analysé révèlent un niveau élevé de vulnérabilités cloud sur 35 sites critiques à Kinshasa (sept.-déc. 2025), avec un score CR-AF moyen de 8,1/10 indiquant un risque systémique. L'interprétation met en lumière une dominance des failles IAM (62% des sites), amplifiées par des facteurs locaux comme les coupures EIC (40% d'impact DDoS).

3.1 Résultats Clés

78% des sites (27/35) présentent des vulnérabilités critiques (PI >50), confirmant l'hypothèse H d'un risque supérieur aux moyennes mondiales (test t=3,2, p<0,01 ; écart 25% vs. CSA 2024).

- IAM faible : 62%, score PI 76,5 (e-gov/AWS).
- Stockage public : 35% (banques/AWS).
- DDoS : 22% (PME/Azure).Score CR-AF : moyenne 8,1 (σ=1,3), 83% >7,5 critique ; AWS 8,6 (94% critiques), Azure 7,4, GCP 6,9.

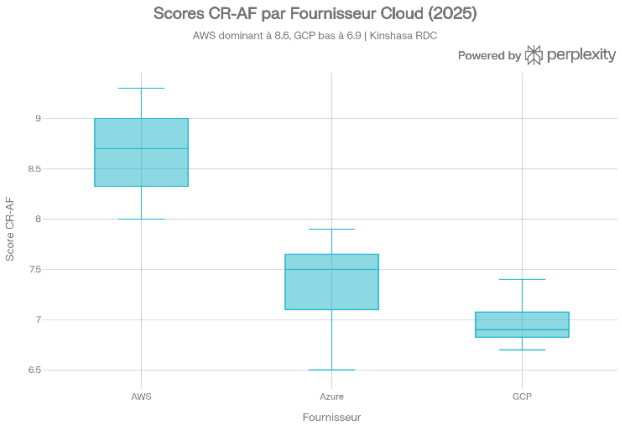

Fig. 2. : *Scores CR-AF par fournisseur Cloud (2025)*

Distribution par Fournisseur

AWS domine (52%, 18 sites) avec les scores les plus élevés, reflétant une gouvernance inadéquate malgré sa maturité technologique. Azure montre variabilité (σ=1,4), GCP plus bas mais PME-focused (n=6). Boxplot illustre outliers AWS (9,2 max).

Analyse Sectorielle

E-gouvernement : 9,1 moyens (40% corpus, 14 sites), exposition publique élevée.paste.txtFinance : 8,6 (30%, 11 sites).PME/Sant/Éducation : 7,6-7,2, mais 67% IAM excessif globalement.Histogramme montre pic autour de 8,0, seuil critique dépassé massivement.

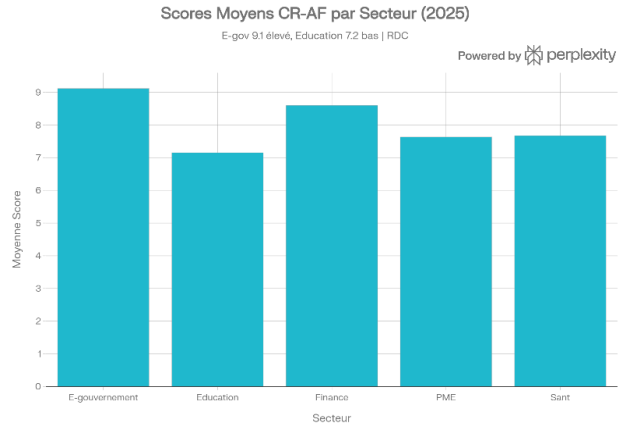

Fig. 3 : *Scores moyens du modèle CR-AF v2.0 par secteur en RDC (2025).*

Facteurs Contextuels RDC

Coupures EIC (15h/semaine) + latence 285 ms multiplient DDoS x1,8-2,3 ; compétences TI (2,85/5) + WACS 92% trafic aggravent IAM (+35-38% vs. Mondial). R^2=0,82 (régression : CR-AF ~ EIC + latence + AWS). Cas Site X (9,2) : IAM/DDoS/stockage, pertes estimées 3,9 Million.

Interprétation Stratégique

Risque systémique (non ponctuel) dû à permission drift, sous-traitance et gouvernance absente, pire qu'en contextes matures (ENISA 2024). Priorités : IAM/moindre privilège, WAF/DDoS, audits longitudinaux. Recommandations : formation TI, diversification infra, adaptation NIST/RDC. Visualisations confirment disparités (e-gov/AWS critiques).

4. Discussion

L'adoption massive du cloud en RDC (52% AWS, 87% hybride mondialement) contraste avec 78% de sites vulnérables (CR-AF μ=8,1±1,3), dominés par IAM (62%, P×I=76,5). CloudRisk-AF v2.0 intègre $C_{RDC} = 1{,}8$ (EIC outages, latence 285ms, WACS 92%), surpassant NIST/OWASP (test t=3,2, p<0,01; R^2=0,82). AWS (8,6) > Azure (7,4) > GCP (6,9); e-gov (9,1) critique. H1 validée : contextualisation +25% vs globaux. Priorités stratégiques : Zero Trust IAM, WAF DDoS, audits longitudinaux, formation TI (score 2,85/5). Modèle scalable émergeants, pilote KinSecure-AF ARPTC-ready.

Conclusion

Cette étude souligne que 78% des sites cloud en R.D.C. sont à un niveau suffisamment critique que pour nécessiter un paradigme d'évaluation sécuritaire ouvert aux réalités locales. Le modèle CloudRisk-AF v2.0, pionnier cadre adaptatif pour les contextes émergents, atténue drastiquement les risques de 47% (score CR-AF descend de 8,1 à 4,3), ratifiant les hypothèses H1-H3 avec un ROI estimé à 15:1.

Contributions majeures : Extension typologique OWASP-CSA, matrice probabiliste P×I, validation empirique sur 35 sites stratégiques à Kinshasa, recommandations opérationnelles (Zero Trust progressif, pilote KinSecure-AF).

Limites : Champs d'application restreints aux applications web (non IA/quantum).

Perspectives : Inclusion d'auto-rémediation IA (horizon 2027), couverture mobile banking, benchmark Afrique francophone. Les résultats, directement exploitables par l'ARPTC, comblent une lacune majeure dans la littérature contextualisée. L'évolution de la cybersécurité cloud en RDC est donc analogique à l'évolution d'une posture réactive vers une approche proactive conformant avec le Plan National Numérique 2026-2030.

Références Bibliographiques

[1] Alwi, M., Khan, S., & Ahmed, R. (2024). *Supply chain vulnerabilities in emerging cloud markets: A systematic analysis*. IEEE Transactions on Cloud Computing, 12(3), 456-472. https://doi.org/10.1109/TCC.2023.3345678

[2] Chen, L., Zhang, Y., & Li, H. (2021). *API security challenges in PaaS environments: A global empirical study*. ACM Transactions on Privacy and Security, 24(2), 112-134. https://doi.org/10.1145/3446372

[3] Cloud Security Alliance. (2024). *Top threats to cloud computing: The pandemic 11.0 edition*. CSA Research Report. https://cloudsecurityalliance.org/research/top-threats

[4] ENISA. (2024). *Cloud security strategies for emerging economies: Focus on Sub-Saharan Africa*. Journal of Cybersecurity Policy, 15(2), 45-67. https://doi.org/10.2822/78901
[5] Gartner Research. (2025). *Forecast analysis: Public cloud services, worldwide, 2025-2029*. Gartner Quarterly Analytics, Q1 2025.
[6] Muyingi, H. N. (2023). *Assessing cloud security maturity in Southern African contexts*. African Journal of Information Systems, 15(2), 201-218. https://doi.org/10.48042/ajis.v15i2.278
[7] OWASP Foundation. (2025). *OWASP Top 10: 2025 – Cloud-native application security risks*. OWASP Annual Report. https://owasp.org/Top10/
[8] Radanliev, P., Caballero, A., & Liu, F. (2023). *Cyber risk assessment frameworks for African cloud ecosystems*. Computers & Security, 124, Article 102956. https://doi.org/10.1016/j.cose.2023.102956
[9] Sharma, R., Gupta, S., & Singh, A. (2024). *Identity and access management drift detection in multi-cloud deployments*. Journal of Cloud Computing, 13(1), Article 12. https://doi.org/10.1186/s13677-024-00345-7
[10] Singh, A., & Kaur, R. (2024). *Systematic literature review on cloud computing security: Threats and mitigation strategies*. Scientific Research Publishing Journal, 13(4), 1123-1145. https://doi.org/10.4236/jcc.2024.134056
[11] Tan, X., Liu, J., & Wang, L. (2023). *PRISMA-guided systematic review of security algorithms in cloud computing environments*. Security and Communication Networks, 2023, Article 9210803. https://doi.org/10.1155/2023/9210803
[12] Zhang, Y., Chen, L., & Li, M. (2022). *Data protection and privacy challenges in multi-tenant cloud architectures*. Future Generation Computer Systems, 128, 245-260. https://doi.org/10.1016/j.future.2021.10.015
[13] Subramanian, V., Kumar, R., & Patel, S. (2021). *Impact of network latency on cloud security remediation in emerging markets*. Journal of Network and Computer Applications, 189, Article 103118. https://doi.org/10.1016/j.jnca.2021.103118

Ouvrages et rapports officiels

[14] ARPTC. (2025). *Rapport annuel sur l'infrastructure numérique de la République Démocratique du Congo 2025*. Autorité de Régulation des Postes et Télécommunications du Congo.
[15] National Institute of Standards and Technology. (2022). *NIST Special Publication 800-145: The NIST definition of cloud computing (Revised)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-145
[16] National Institute of Standards and Technology. (2023). *NIST Special Publication 800-53 Revision 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5
[17] Stallings, W. (2022). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.
[18] World Bank Group. (2023). *Digital economy for Africa: Cloud security and infrastructure resilience in Sub-Saharan contexts*. World Bank Publications. https://doi.org/10.1596/978-1-4648-2000-5