Editions Ishango - UAC
Revue Internationale Multidisciplinaire Etincelle

Ed. ishango

Article

Modèle conceptuel d'évaluation des risques des réseaux WLAN des universités

Héritier Nsenge Mpia*, Baelani Inipaivudu Nephtali, Lofandja Balongo Nelly

Faculté de Sciences Economiques et de Gestion, Université de l'Assomption au Congo, Butembo, P.O. Box 104, République Démocratique du Congo

* Correspondant : staniher@yahoo.fr

Abstract: L'adoption d'un réseau internet (WLAN) dans une université est une ressource pour les fondations de l'éducation dans les pays en développement. Malheureusement, le WLAN souffre souvent d'attaques de virus et d'attaques des personnes ou même les étudiants eux-mêmes essaient de briser le réseau. Il y a donc toujours une perte de données dans ces projets éducatifs. Il a été ainsi important de mener cette étude sur la modélisation d'un cadre conceptuel permettant d'évaluer les risques de WLAN des universités. Pour réaliser cette recherche, les auteurs ont fait usage de l'analyse exploratoire des facteurs (EFA) comme technique d'analyse des données. Les auteurs ont constitué un questionnaire d'enquête qui a permis de collecter les données primaires auprès des étudiants et administrateurs réseaux des universités Congolaises. Les données collectées représentent une compilation de 629 réponses. Le résultat de test Kaiser-Meyer-Olkin **(**KMO) a été de 0,82 et celui de Bartlett a atteint 0,0 pour la valeur de p et 2578,37 pour khi^2. Cela étant, les auteurs ont conclu que l'échantillon utilisé pour conduire l'EFA a été adéquat. Au terme de l'EFA, les auteurs ont observé que le niveau de sécurisation et la compétence des administrateurs sont deux facteurs qui permettent d'évaluer les risques d'un WLAN au sein d'une université. Toutefois, après avoir testé la fiabilité de ces facteurs obtenus en utilisant le test Alpha de Cronbach, les auteurs ont conclu que seul le facteur niveau de sécurisation est fiable car sa valeur Alpha a été de 84,05% alors que la compétence des administrateurs n'a atteint que 48,52%.

Citation: Mpia, H.N., Baelani, I.N., Lofandja, B.N. Modèle conceptuel d'évaluation des risques des réseaux WLAN des universités. *Etincelle*, 2023, Vol. 25, no. 1. https://doi.org/10.61532/rime251112

Reçu : 10/06/2023
Accepté : 01/10/2023
Publié : 13/10/2023

Mots clés: WLAN, sécurité réseau, universités congolaises, évaluation des risques, analyse exploratoire

1. Introduction

Pour que le secteur de l'éducation de la république démocratique du Congo (RDC) arrive à revitaliser, il doit adopter les technologies de l'information et de la communication (TIC). Malheureusement, investir dans l'éducation nationale congolaise n'a pas été une priorité absolue des gouvernants depuis des décennies. En effet, alors que le gouvernement congolais a alloué en moyenne 20% de son budget à l'éducation de 1969 à 1975, il n'a consacré que 0,4 % à l'éducation, 0,4% de 1993 à 2000 (Mokonzi & Mwinda, 2009). Ce budget s'avère être insuffisant pour améliorer les infrastructures éducatives de base du pays, sans parler de l'adoption de nouvelles infrastructures des TIC. De 2017 à 2022, le gouvernement a oublié totalement ce secteur qui constitue le moteur économique et un des facteurs d'employabilité des diplômés (Mpia, et al., 2022). Il est généralement admis que le système éducatif de la RDC a un besoin urgent des réformes. Nombreux établissements éducatifs de ce pays ne sont pas soutenus par des systèmes basés sur les TIC. Là où les TIC existent, elles sont entachées de plusieurs problèmes allant du manque d'approvisionnement stable en électricité à la rareté des éducateurs qualifiés en matière de TIC.

Pourtant, il est évident que les TIC peuvent jouer un rôle majeur dans l'éducation d'un pays. En effet, les TIC sont actuellement largement utilisées pour aider à l'éducation dans de nombreux pays en développement, et il semble qu'il y ait une demande croissante pour leur utilisation dans l'éducation de la part des décideurs et des parents dans les pays en développement (Wagner, 2005).

En outre, des recherches ne cessent de révéler que les TIC sont un outil puissant pour l'éducation dans tous les pays. Lorsqu'elles sont mises en œuvre de manière appropriée, les TIC peuvent catalyser et accélérer la réforme de l'éducation et le développement économique. La RDC peut grandement bénéficier d'un système éducatif soutenu par les TIC. C'est ainsi qu'aujourd'hui le gouvernement congolais s'efforce à intégrer les TIC dans des institutions académiques (Rangel-Pérez, et al., 2021). Cette intégration a des avantages, mais aussi des risques car l'intégration surtout des réseaux locaux sans fil (WLAN) peuvent s'avérer une ouverture aux failles des ressources d'une université. Le but principal de cette recherche n'a été pas d'examiner l'impact des TIC dans le système éducatif, mais plutôt de construire un cadre conceptuel illustrant les facteurs qui influencent les risques d'un réseau WLAN au sein des universités congolaises. La construction de ce cadre conceptuel a été fait en appliquant l'analyse exploratoire des facteurs (EFA). En effet, ceci pourra aider les universités de la RDC à émerger dans l'adoption des TIC tout en ayant conscience des risques que les technologies WLAN peuvent présentés afin de prendre des bonnes précautions car une organisation ne peut protéger au mieux ses informations que lorsqu'elle est en mesure d'évaluer les risques de sécurité (Ievgeniia, et al., 2021).

L'émergence des WLAN dans des universités congolaises se laisse voir de nos jours. On constate que plusieurs universités congolaises arrivent à adopter des WLAN en leur sein pour entrer dans la dynamique de la vision du ministère de l'enseignement supérieur et universitaire (ESU). En plus, de nos jours, il est devenu un effort impérieux pour des structures et organisations d'adopter des technologies modernes afin d'assurer leur productivité (Raquel, et al., 2022). Les réseaux, surtout sans fil, ont permis de briser les barrières que les utilisateurs dans une organisation rencontraient. La liberté d'accéder au réseau de l'entreprise sans être lié, la mobilité lors de l'accès à l'Internet, la fiabilité et la flexibilité accrues sont là des avantages qu'offrent un réseau au sein d'une université. La réduction du temps d'installation, les économies de coûts à long terme et l'installation de systèmes de communication sans fil constituent également des facteurs qui contribuent à l'énorme croissance des WLAN (AAbo-Soliman & Azer, 2018). Aujourd'hui, le WLAN est un choix à prendre en compte dans divers secteurs, y compris les entreprises, le gouvernement et le secteur de l'éducation. La norme IEEE 802.11 domine la technologie des réseaux sans fil. Cela s'explique par le faible coût du matériel et les débits de données élevés qui prennent en charge les applications actuelles (de 1 à 54 Mbps) ainsi que les extensions futures prometteuses (pouvant dépasser 100 Mbps) (Imran, et al., 2018). De plus en plus, les appareils portables sont souvent vendus avec un réseau local sans fil en standard. Toutefois, ce type de réseau s'avère être imbibé de plusieurs failles.

L'adoption progressive des WLAN au sein des universités constitue un atout pour les institutions académiques dans des pays en voie de développement. Malheureusement, les WLAN ont souvent présenté des problèmes de sécurité au sein des campus. Ces réseaux souffrent souvent des attaques des virus et des attaques des individus voire des étudiants eux-mêmes désirant de saboter les réseaux et s'y introduire. Ainsi, il y a souvent des pertes des données massives dans ces institutions (Zheng, et al., 2021). Cela étant, il a été urgent de conduire cette recherche sur la modélisation d'un cadre conceptuel d'évaluation des risques des WLAN des universités congolaises. En fait, les WLAN des universités courent le risque d'être piraté. Plusieurs travaux de recherche dans la revue de littérature existante ont porté sur l'amélioration du mécanisme de sécurité au sein de ces réseaux (Efstratios, et al., 2022). Pour ce faire, cette présente étude a porté sur la proposition d'un cadre

conceptuel offrant une vue globale des facteurs qui affectent les risques d'un WLAN d'une université en appliquant l'EFA. La revue de littérature existante a également révélé que les travaux antérieurs se sont plus focalisés sur l'identification des risques dans des réseaux, mais peu seulement ont abordé la notion des vulnérabilités des WLAN des universités. En plus, les recherches sur les WLAN en RDC sont quasi inexistantes. Par conséquent, cette recherche a trouvé sa valeur dans la mesure où elle s'est basée sur les WLAN des universités congolaises.

L'objectif principal de cette recherche a été de développer un modèle conceptuel d'évaluation des risques qu'accourent les WLAN des universités congolaises en utilisant l'EFA. Partant de cet objectif, les auteurs ont formulé des questions ci-après : 1) Quel est le modèle approprié pour évaluer les risques des WLAN des universités congolaises ? 2) Quelle est la fiabilité du modèle développé d'évaluation des risques des WLAN des universités congolaises ?

L'intérêt de cette recherche se situe au niveau où il y a aujourd'hui un taux croissant d'adoption des WLAN dans des universités congolaises. Ceci nécessite ainsi des études scientifiques afin d'éclairer sur les risques découlant des WLAN. La recherche et la communication de facteurs cohérents et fiables pour évaluer ces risques peuvent atténuer le problème de vulnérabilité des WLAN dans des universités de la RDC qui ne sont qu'en leur début d'adoption des TIC. Cette étude a cherché à combler les lacunes de la littérature existante en identifiant les facteurs contextuels qui peuvent être utilisés pour évaluer les risques des WLAN. C'est ainsi que les auteurs ont estimé que l'EFA serait une bonne technique pouvant aider à identifier ces facteurs. Cette technique d'analyse des données a été utilisée pour extraire des facteurs à partir les éléments ou variables de l'enquête. L'EFA étudie donc le nombre de facteurs entre les items collectés et quel item détermine quels facteurs (Orçan, 2018).

Le reste de ce manuscrit comprend quatre sections. La première section aborde aussi bien la revue de littérature théorique que la revue de littérature empirique pour distinguer cette étude des travaux existants afin d'identifier la démarcation qu'y existe. La deuxième section présente la méthodologie utilisée pour conduire à bon escient cette recherche en partant de la conception de la recherche aux méthodes appliquées pour vérifier la validité et la fiabilité de cette étude. La troisième section illustre les résultats et synthétise les données statistiques des variables démographiques des participants de cette recherche tout en concluant par la construction d'un cadre conceptuel graphique contenant des composant du modèle obtenu d'évaluation des risques des WLAN des universités congolaises. La dernière section constitue le sommaire de cette recherche et présente de façon brève les nouveautés de cette recherche. En plus, elle fait quelques recommandations pour des travaux futurs.

2. Revue de littérature

2.1. Revue de littérature théorique

Cette section a aidé les auteurs à faire comprendre les lecteurs les concepts clés de leur recherche, notamment la notion sur les composants de WLAN, la technologie de transmission dans la fréquence WLAN, l'allocation des fréquences WLAN, la topologie WLAN, l'application de WLAN ainsi que la sécurité de WLAN.

2.1.1. Notions sur les composants de WLAN

Les réseaux sans fil ont été un élément crucial de la communication au cours des dernières décennies et un changement de paradigme véritablement révolutionnaire, permettant des communications multimédias entre les personnes et les appareils à partir de n'importe quel endroit (cf. figure 1). Ils apportent des changements fondamentaux aux réseaux de données, aux télécommunications et aux réseaux intégrés (Mpia, 2018). Ils ont

rendu le réseau portable grâce à la modulation numérique, à la modulation adaptative, à la compression des informations, à l'accès sans fil et au multiplexage. Le WLAN prend en charge des applications passionnantes telles que les réseaux de capteurs, les maisons intelligentes, la télémédecine et les autoroutes automatisées (Mohammad, 2012). Les premiers utilisateurs de la technologie sans fil ont été principalement les militaires, les services d'urgence et les organismes chargés de l'application de la loi. À mesure que la société évolue vers une centralité de l'information, le besoin de disposer d'informations accessibles à tout moment et en tout lieu prend une nouvelle dimension. L'énorme concurrence dans l'industrie du sans-fil et l'acceptation massive des appareils sans fil ont entraîné une baisse significative des coûts associés aux terminaux et au temps d'antenne au cours des dix dernières années (Mohammad, 2012**)**.

Pratiquement inconnus, il y a encore quelques années, les WLAN sont, aujourd'hui, omniprésents dans notre société. Utilisant des ondes radio, les WLAN existent pourtant depuis des années, mais l'augmentation de la bande passante et la baisse des coûts a fait exploser leurs croissances. Il faut savoir que les premiers WLAN, comme Aloha, ARDIS et Ricochet, offraient des débits inférieurs à 1Mbit/s. Puis vint le standard 802.11 ratifié en 1997. Celui-ci a permis alors d'atteindre un débit compatible de 2Mbit/s. En 1999, on atteint la vitesse de 11Mbit/s grâce au standard 802.11b. Les 54Mbit/s ont été franchis, en 2003, avec le standard 802.11g. En attendant le standard 802.11n, prévu pour 2007, qui permettrait d'atteindre les 600 Mbit/s, un brouillon ("Draft-N") a été ratifié début 2006 qui permet un débit théorique de 300 Mbit/s soit trois fois plus qu'un réseau Fast Ethernet filaire dont le débit est de 100 Mbit/s (Xinming, 2022).

2.1.2. Les technologies de transmission dans la fréquence WLAN

Les technologies de réseau sont traditionnellement basées sur des solutions filaires. Mais l'introduction des normes IEEE 802.11 a eu un impact considérable sur le marché, de sorte que les ordinateurs portables, les PC, les imprimantes, les téléphones cellulaires, les téléphones VoIP, les lecteurs MP3 à la maison, au bureau et même dans les lieux publics ont intégré la technologie LAN sans fil (Sourangsu & Chowdhury). Les technologies sans fil à large bande offrent aujourd'hui aux utilisateurs un accès illimité à la large bande, alors qu'elles n'étaient auparavant proposées qu'aux utilisateurs de lignes filaires. Dans cette recherche, les auteurs ont examiné et résumé l'une des technologies émergentes à large bande sans fil, à savoir l'IEEE 802.11, qui est un ensemble de normes de couche physique pour la mise en œuvre de la communication informatique par réseau local sans fil dans la bande de fréquences 2,4, 3,6, 5 et 60 GHz. Elles corrigent les problèmes technologiques ou ajoutent des fonctionnalités qui devraient être requises par les applications futures. Bien que certaines des versions antérieures de ces technologies soient désormais obsolètes (comme HiperLAN), nous les avons tout de même incluses dans cette étude par souci d'exhaustivité (Sourangsu & Chowdhury).

La technologie sans fil de réseau WLAN est l'une des nombreuses technologies qui permettent aux gens de communiquer entre eux par voie aérienne, c'est-à-dire par radiofréquence. Avec la technologie WLAN 802.11b, seuls trois canaux ne se chevauchant pas sont disponibles, et Il n'existe pas de mécanisme standard permettant aux points d'accès de sélectionner dynamiquement le canal à utiliser afin de minimiser les interférences avec d'autres points d'accès (Dewi, 2011). L'image ci-dessous illustre l'évolution dans le temps des technologies WLAN :

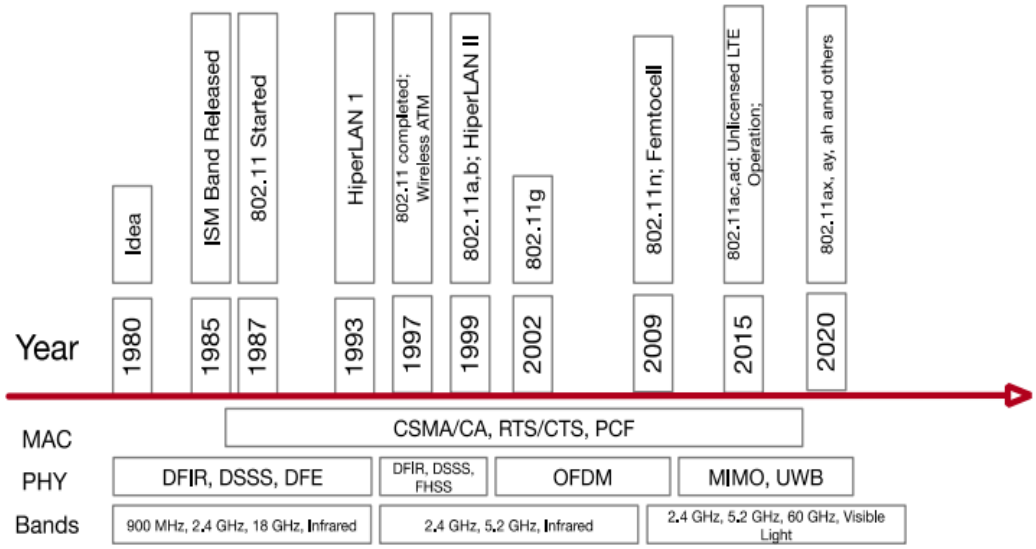

Figure 1. Evolution des technologies et des normes WiFi. Reproduite avec l'autorisation de la référence (Pahlavan & Krishnamurthy, 2022), Int J Wireless Inf Networks

2.1.3. Les risques de WLAN

Les réseaux sans fil présentent de nombreux avantages. La productivité s'améliore grâce à l'accessibilité accrue aux ressources d'information. La configuration du réseau est plus facile, plus rapides et moins coûteuses. Cependant, la technologie sans fil crée également de nouvelles menaces et modifie le profil de risque existant en matière de sécurité de l'information. Par exemple, comme les communications s'effectuent dans l'air en utilisant des fréquences radio, le risque d'interception est plus grand qu'avec les réseaux câblés. Si le message n'est pas crypté, ou s'il est crypté avec un algorithme faible, l'attaquant peut le lire, ce qui compromet la confidentialité. Bien que les réseaux sans fil modifient les risques associés à diverses menaces pour la sécurité, les objectifs généraux de sécurité restent les mêmes que pour les réseaux câblés : préserver la confidentialité, assurer l'intégrité et maintenir la disponibilité des informations et des systèmes d'information (Min-Kyu, 2008).

La technologie des réseaux sans fil, bien qu'elle présente les commodités et les avantages décrits ci-dessus, a sa part d'inconvénients. Dans une situation de réseau donné, les réseaux sans fil peuvent ne pas être souhaitables pour un certain nombre de raisons. La plupart d'entre elles sont liées aux limitations inhérentes à la technologie. Les inconvénients de l'utilisation d'un réseau sans fil sont les suivants : Sécurité, portée, fiabilité et vitesse. Les réseaux sans fil posent une série de problèmes aux gestionnaires de réseaux. Les points d'accès non autorisés, les Service Set Identifier (SSID) diffusés, les stations inconnues et les adresses MAC usurpées ne sont que quelques-uns des problèmes abordés dans le cadre de la résolution des problèmes liés aux WLAN. La plupart des fournisseurs d'analyse de réseau, tels que Network Instruments, Network General et Fluke, proposent des outils de dépannage WLAN dans le cadre de leur gamme de produits (Min-Kyu, 2008).

Les réseaux sans fil offrent de nombreuses possibilités d'accroître la productivité et de réduire les coûts. Ils modifient également le profil de risque global d'une organisation en matière de sécurité informatique. Bien qu'il soit impossible d'éliminer totalement tous les risques liés aux réseaux sans fil, il est possible d'atteindre un niveau raisonnable de sécurité globale en adoptant une approche systématique de l'évaluation et de la gestion des risques (Min-Kyu, 2008).

2.2. Revue de littérature empirique

La revue de littérature empirique permet au lecteur de se faire une idée sur des préoccupations des recherches antérieures ayant traité le même thème ou en rapport avec le sujet sous examen afin d'y identifier des lacunes (Paré, et al., 2015). Sur ce, tout travail scientifique étant une complémentarité, il s'avère que chaque auteur ayant abordé le sujet similaire au nôtre a tenté de proposer des solutions adéquates.

Sombatruang, et al. (2019), dans leur article intitulé *Factors influencing users to use unsecured Wi-Fi Networks: Evidence in the wild,* affirment que les preuves empiriques des risques liés aux réseaux Wi-Fi non sécurisés sont inquiétantes, non seulement parce que de nombreuses applications ne cryptent pas les données transmises, mais aussi parce que les gens continuent à utiliser les réseaux. Ce phénomène peut sembler surprenant. Ces chercheurs ont développé une application Android, *My Wi-Fi Choices*, qui recueille le niveau réel de la batterie et l'estimation du volume de données mobiles restant sur l'appareil mobile d'un participant à chaque fois qu'il se connecte à des réseaux Wi-Fi publics ouverts non sécurisés. Ils ont examiné si la probabilité perçue par les participants que le Wi-Fi public puisse être compromis (sur une échelle de 0 % à 100 %, 0 % étant le moins probable et 100 % le plus probable) affectait leur utilisation de Wi-Fi non sécurisé, puis considéré le Wi-Fi public comme un substitut raisonnable des réseaux Wi-Fi non sécurisés. Ils se sont également appuyés sur des travaux antérieurs qui ont évalué la compréhension par les utilisateurs des risques pour la vie privée et de la sécurité liés à l'utilisation du Wi-Fi public aujourd'hui. Deux grands facteurs ont été soulevés comme facteurs influençant les risques des WLAN : (1) l'utilisation de réseaux Wi-Fi non sécurisés (âge, éducation, niveau de revenu sont des variables liées à ce facteur) et (2) le niveau de données mobiles restantes (énergie restante dans la batterie) (Sombatruang, et al., 2019).

Waliullah et Gan (2014), dans leur travail intitulé *Wireless LAN security threats & vulnerabilities: A literature review*, insistent sur le fait que les WLAN ont gagné en popularité par rapport aux réseaux câblés en raison de leur flexibilité, de leur rentabilité et de leur facilité d'utilisation. Toutefois, le déploiement croissant des WLAN offre au hacker ou au pirate plus d'opportunités. Contrairement aux réseaux câblés, les WLAN transmettent les données dans l'air par transmission radiofréquence ou infrarouge. La technologie sans fil actuellement utilisée permet à un pirate de surveiller un réseau sans fil et, dans le pire des cas, d'affecter l'intégrité des données. Il existe un certain nombre de problèmes de sécurité qui posent des difficultés au praticien de la sécurité informatique, à l'administrateur du système, et à la sécurisation du réseau local sans fil (Waliullah & Gan, 2014). Dans ce sens, leur incapacité à contenir efficacement les signaux radio rend le WLAN vulnérable à une série d'attaques différentes de celles des réseaux câblés. Bien que les entreprises puissent positionner leurs points d'accès et utiliser des antennes pour concentrer leurs signaux dans une direction spécifique, il est difficile d'empêcher complètement la transmission sans fil d'atteindre un endroit indésirable comme les halls d'entrée, les zones semi-publiques et les parkings. Il est donc plus facile pour les intrus d'intercepter des données sensibles. Les WLAN dans leur implémentation intrinsèque permettent aux attaquants de surveiller un réseau sans fil et, dans le pire des cas, d'affecter l'intégrité des données. En plus, les facteurs humains (vol de données par des connaissances ou des collègues) constituent une des grandes failles des WLAN (Waliullah & Gan, 2014).

Jason (2020) dans son article intitulé *Analysis of security features and vulnerabilities in Public/Open Wi-Fi* souligne que, dans de nombreux établissements d'enseignement supérieur, des PA publics ouverts, appelés "hotspots", permettent aux étudiants d'accéder à l'Internet. Ces points d'accès peuvent être fournis par American Telephone and Telegraph (AT&T), Comcast et d'autres sociétés. En d'autres termes, si un étudiant est assis dans un espace commun sur le campus ou dans un café, il peut accéder à l'un de ces canaux pour se connecter à l'Internet. Malheureusement, ces PA ouverts permettent également à toute

personne se trouvant dans la zone de lire des données qui ne lui sont pas destinées. Les mêmes caractéristiques qui rendent ces points d'accès Wi-Fi gratuits pour les étudiants, les rendent également souhaitables pour les pirates informatiques, à savoir qu'il n'y a pas besoin d'authentification pour établir une connexion réseau. Cela crée une opportunité extraordinaire pour le hacker d'obtenir un accès illimité à des réseaux non sécurisés (Jason, 2020). De ce fait, si un pirate informatique veut voler les informations personnelles, financières ou l'identité d'un étudiant, il lui suffit d'une application de reniflage, comme Wireshark ou Kali Linux, qui intercepte et rassemble tout le trafic visible sur un canal. Étant donné que le Wi-Fi ouvert n'a pas de sécurité utilisant une clé pré-partagée (PSK) comme le WPA2, où chaque connexion est cryptée entre un réseau Wi-Fi et le client d'un utilisateur, le travail d'un pirate informatique a déjà fait son travail puisque tout est en clair et non crypté, et il peut simplement "renifler" le réseau et s'emparer des informations personnelles de l'étudiant (Jason, 2020).

Dans cette mouvance, Nasr, et al. (2019), dans leur étude « Wi-Fi Network Vulnerability Analysis and Risk Assessment in Lebanon», soulignent qu'il y a eu plus de 7 milliards de nouveaux appareils Wi-Fi entre 2019 et 2022. Cela signifie que plus de 7 milliards de nouveaux appareils Wi-Fi ont pu être vulnérables à des attaques Wi-Fi. L'objectif de leur déclaration était de faire une analyse approfondie qui a été réalisée sur les WLAN situés dans divers quartiers et régions commerciales et résidentielles du Liban. Sur la base de l'analyse des données acquises, des résultats statistiques seront générés, utilisés pour sensibiliser de la population au problème des attaques Wi-Fi. Pour ces chercheurs, il s'agit avant tout de remédier à l'énorme déficit de sensibilisation et de connaissances en matière de cyber sécurité dont souffre la société libanaise. Leur recherche a été de nature exploratoire et a utilisé une méthodologie de recherche quantitative (Nasr, et al., 2019). Tout au long du processus de réalisation de leur recherche, un *wardrive* a été réalisé et une enquête contenant une liste de questions relatives à la sensibilisation de la cyber sécurité a été distribuée, le tout dans le but d'évaluer les risques. Et les résultats générés par leur enquête et le wardrive ont permis de répondre à plusieurs questions de recherche et à estimer la gravité du problème en question. Ces chercheurs ont conclu que le manque de sensibilisation des gens aux questions de sécurité des WLAN peuvent augmenter les risques autant que possible. En plus, 30,2 % des participants à leur recherche ne savent pas ce qu'est un pare-feu, ce qui aide les attaquants à réaliser des attaques d'authentification (Nasr, et al., 2019).

Apres la revue de littérature empirique, il a été observé que trois facteurs sont prépondérants dans l'évaluation des risques des WLAN. Il s'agit du facteur interne des WLAN, du facteur humain, et du facteur niveau de sécurisation. Chacun de ces trois facteurs englobe ses propres variables telles que illustrées sur la figure 2. Partant des recherches antérieures, la présente étude a pu observer que le cadre conceptuel de la recherche antérieure peut se composer des variables indépendantes et dépendante ci-dessous :

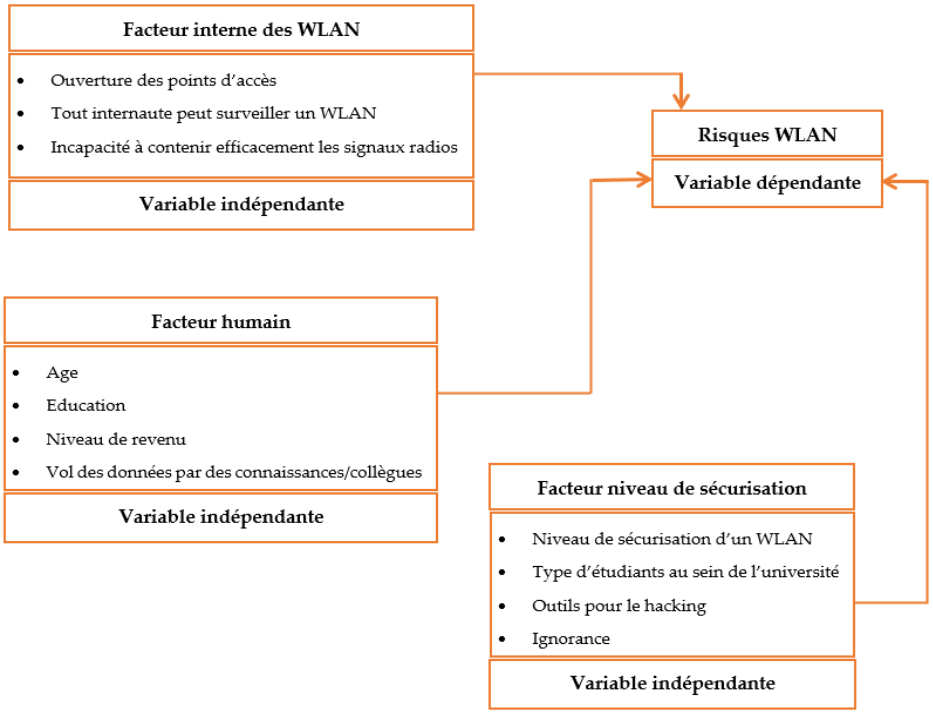

Figure 2. Cadre conceptuel graphique

3. Méthodes et matériels

3.1. Conception de la recherche

Cette recherche a utilisé un modèle d'enquête quantitative non expérimentale pour examiner et étudier les pratiques de sécurité par lesquelles les universités évaluent les risques des réseaux WLAN. La méthode d'une étude doit correspondre au plan du chercheur pour répondre au problème de recherche (Creswell, 2009). Le modèle de recherche quantitative de cette étude a été choisi pour répondre aux deux questions de recherche reprises dans l'introduction.

Les auteurs ont utilisé un modèle quantitatif pour quantifier les opinions des administrateurs réseaux des universités et des étudiants dans le but de généraliser les résultats à partir d'un échantillon plus large sur l'évaluation des risques qu'accourent les réseaux WLAN dans des universités congolaises. Cette étude a adopté une approche de recherche quantitative pour deux raisons majeures. Premièrement, la méthodologie quantitative produit des données analytiques objectives. Deuxièmement, elle offre la possibilité de généraliser les résultats à des cas et des populations similaires (Abuhamda, et al., 2021). Etant donné que les faits sociaux sont difficiles à comprendre objectivement, dans cette recherche nous avons utilisé l'analyse exploratoire des facteurs comme technique d'analyse de données pour identifier des groupes de variables similaires par l'extraction et la rotation des facteurs. Cette technique est un outil efficace pour analyser les relations entre les variables observées à partir d'un phénomène social et réduire le nombre de facteurs sous-jacents (Hadi, et al., 2016). Etant donné que cette étude a collecté les données primaires auprès des étudiants et des administrateurs réseaux des WLAN des universités, les auteurs ont utilisé l'enquête comme technique d'obtention des données à l'aide de questionnaires (Erdil, et al., 2021). Cette technique a été puisqu'elle permet d'obtenir des données concrètes et crédibles (Kabir, 2016). L'étude a extrait ainsi des variables clés telles que le sexe, l'âge, type d'institution (université ou institut supérieur), la dernière date qu'un réseau WLAN d'université a été piraté, etc.

3.2. Population et échantillonnage

La population désigne l'ensemble dont les éléments sont choisis parce qu'ils possèdent tous une même propriété et qu'ils sont de même nature. Il peut s'agir d'un ensemble des personnes classées suivant un critère donné ; tout comme d'un ensemble d'objets (Grawitz, 2001). Dans le présent travail, concrètement, la population cible a été des étudiants et administrateurs réseaux des WLAN des établissements de l'enseignement universitaires de la ville de Butembo. Considérant que la RDC souffre du manque des sources fiables de publication des données relatives aux effectifs des étudiants sur le plan national à cause de certains facteurs sociopolitiques et économiques (Mpia, et al., 2023), nous avons été buté au problème d'estimation réelle de la population afin de l'échantillonner proprement. Par conséquent, cette recherche a utilisé la technique d'échantillonnage stratifié disproportionné en choisissant au hasard des membres de chaque strate (Iliyasu & Etikan, 2021).

Les données primaires ont été recueillies auprès de personnes interrogées dans les deux types d'institution à savoir les universités et les instituts supérieurs. Les personnes interrogées étaient soit les étudiants soit les administrateurs des réseaux WLAN des institutions enquêtées. L'instrument d'enquête a été déployé à l'aide d'un formulaire Google qui a été distribué par courrier électronique avec un lien par une approche en boule de neige des réseaux d'amis. Au total, les auteurs ont collecté un échantillon de 629 données brutes dans les deux types d'institutions supérieures de la ville de Butembo. Toutes les questions avaient des réponses. Ce qui fait qu'il n'y a pas eu à amputer des données manquantes.

3.3. Instrument de recherche

L'instrument de recherche utilisé dans cette recherche a été le questionnaire. Le questionnaire est la technique la plus utilisée pour recueillir des données quantitatives primaires en recherche scientifique. Le questionnaire permet de collecter des données quantitatives d'une manière standardisée, ce qui garantit la cohérence interne des données en vue de leur analyse. Les questionnaires doivent toujours avoir un objectif clair en rapport avec les objectifs de l'étude, et il doit être clair dès le départ comment les résultats seront utilisés (Roopa & Rani, 2012).

Le questionnaire de cette recherche comprenait 19 questions. Les questions ont été conçues sur la base du cadre conceptuel construit dans la figure 2. Les participants ont été interrogés en trois sections. La première section contenait des questions destinées à évaluer les caractéristiques démographiques des participants. La deuxième section contenait des questions de recherche relatives aux risques dont les réseaux WLAN des participants ont déjà été victimes, et la dernière section abordait les questions sur les types de sécurités que ces institutions académiques ont pu déployer en leur sein. Quinze des questions étaient dyadiques et quatre questions utilisaient une échelle de Likert en 6 points. Chaque question a été encodée en forme abrégée afin de permettre des analyses statistiques avec des logiciels de traitement des données que nous avons utilisés et chacune des réponses des participants a été encodée en valeur numérique. Les 19 items qui ont constitué notre questionnaire de recherche, les formes abrégées des questions et le domaine d'encodage des réponses sont listés dans le tableau ci-après :

Table 1. Questions de recherche et leur encodage

Variable	Question de recherche	Format d'encodage
Genre	Quel est votre genre ?	0=Féminin, 1=Masculin
Age	Quel est l'intervalle de votre âge ?	1= De 21 à 25, 2 = De 26 à 30, 3 = De 31 à 35, 4 = De 36 à 40, 5 = De 41 à 45, 6 = Plus
Institution	Dans quel type d'institution œuvrez-vous ?	0=Institut supérieur, 1=Université
WLAN	Avez-vous un WLAN au sein de votre université ?	0 = Non, 1 = Oui
Victime_Perso	Avez-vous déjà été piraté personnellement?	0 = Non, 1 = Oui
Type_victime	Quel type des piraterie avez-vous déjà connu dans votre WLAN?	1 = Le vol de mot de passe, 2 = Les logiciels malveillants, 3 = Intrusions, 4 = Déni de service, 5 = Vol des données, 6 = Rien à signaler
Victime_WLAN	Est-ce que le WLAN de votre institution a déjà été piraté ?	0 = Non, 1 = Oui
Risque	Est-ce que votre institution a déjà connu des risques dans son réseau WLAN?	0 = Non, 1 = Oui
SSID	Votre WLAN a-t-il toujours le SSID par défaut ?	0 = Non, 1 = Oui
Password	Le mot de passe de votre WLAN peut-il être facilement déchiffré ?	0 = Non, 1 = Oui
Cle_securite	Des options d'authentification plus fortes sont-elles disponibles (par exemple, des clés privées) ?	0 = Non, 1 = Oui
Port	Existe-t-il des ports ouverts inutiles (par exemple, telnet, http, ftp) dans votre réseau?	0 = Non, 1 = Oui
Vulnerable	Ces ports ouverts sont-ils vulnérables à des exploits connus ?	0 = Non, 1 = Oui
Crypto	Existe-t-il des interfaces administratives cryptées (par exemple, ssh, https) ?	0 = Non, 1 = Oui
Alertes	Les alertes de sécurité ou les journaux ont-ils été activés (par exemple, syslog, traps) ?	0 = Non, 1 = Oui
Cause	Quelle a été la cause de piratage de votre WLAN?	1= Manque de sécurité, 2 = Inefficacité de l'administrateur réseau, 3 = Ouverture des ports, 4 = Manque d'audit, 5 = Utilisation des ressources de sécurité inadéquates, 6 = Rien à signaler
Date	Quelle est la dernière date que votre réseau a été piraté ?	1 = La semaine passée, 2 = Le mois passé, 3 = Le six mois passés, 4 = L'année passée, 5 = Plusieurs années passées, 6 = Jamais
Administrateur	Est-ce que votre institution a un administrateur réseau ?	0 = Non, 1 = Oui
Expertise	Est-ce que votre administrateur réseau est un expert en sécurité ?	0 = Non, 1 = Oui

3.4. Validité et fiabilité de l'instrument

Pour établir la validité de notre questionnaire, les auteurs ont modifié quelques questions de recherche après avoir été vérifié par un expert en science des données. Sur la base des commentaires de cet expert, nous avions revu la question "Est-ce que votre université a déjà eu des risques dans son réseau ?" en remplaçant université par institution afin d'éviter l'ambiguïté entre nos strata de recherche (Université et Institut supérieur) et l'item de ce questionnaire. En outre, la question "Quel est votre âge" a été modifié pour représenter sous forme de fourchette de valeurs les données précédemment numériques en la changeant par "Quel est l'intervalle de votre âge ?". Cela a permis de garantir la confidentialité de l'âge réel des participants à l'enquête.

Par contre, l'adéquation des données collectées à l'analyse exploratoire des facteurs a été mesurée à l'aide des tests de sphéricité de Kaiser-Meyer-Olkin (KMO) et de Bartlett. Signalons que l'hypothèse alternative pour le test de Bartlett a été observée, ce qui indique que la matrice de corrélation contient des informations significatives et que l'analyse factorielle peut être réalisée (Jowkar, et al., 2013) contrairement à l'hypothèse initiale qui stipule que toutes les variables étudiées sont corrélées entre elles (Persson & Khojasteh, 2021). Les auteurs ont également fait le test de fiabilité de l'instrument afin de garantir la répétabilité et l'exactitude des résultats obtenus à partir des données collectées (Ciampolini, et al., 2021). Les auteurs ont ainsi utilisé le test Alpha de Cronbach pour mesurer la fiabilité de la cohérence interne des questions du questionnaire.

3.5. Outils et matériels utilisés

Cette section est aussi importante dans la mesure où elle a aidé les auteurs à avoir une idée générale sur les outils choisis et le choix d'un outil et des matériels n'est pas un choix du hasard. Il est décidé par la nature de l'information qu'on veut obtenir pour atteindre un objectif donné. Le tableau 2 présente les outils et matériels utilisés et l'endroit où ils ont été appliqués :

Table 2. Outils et matériels utilisés

Phases	Langages	Outils, Frameworks, librairies
Collecte des données		Internet, Google form
Analyse exploratoire des données et prétraitements	Python	Jupyter Notebook, Pandas, Matplotlib, Seaborn, numpy
EFA	Python	Pandas, FactorAnalyzer, Dataframe, Seaborn

4. Résultats et discussion

4.1. Statistiques des données démographiques des répondants

Les données démographiques sur les profils des répondants à notre questionnaire sont présentés dans le tableau 3 ci-dessous :

Table 3. Données démographiques des participants

Variable	Fréquence	Pourcentage (%)
Age (n= 629)		
18 à 25 ans	213	33,9
26 à 30 ans	145	23,1
31 à 35 ans	125	19,9

36 à 40 ans	76	12,1
41 à 45 ans	36	5,7
Plus	34	5,4
Genre (n= 629)		
Masculin	426	67,7
Féminin	203	32,3
Type d'institution (n= 629)		
Université	602	95,7
Institut supérieur	27	4,3

Sur la base des données collectées pour cette recherche, la figure ci-dessous décrit le pourcentage et la proposition de chaque variable démographique:

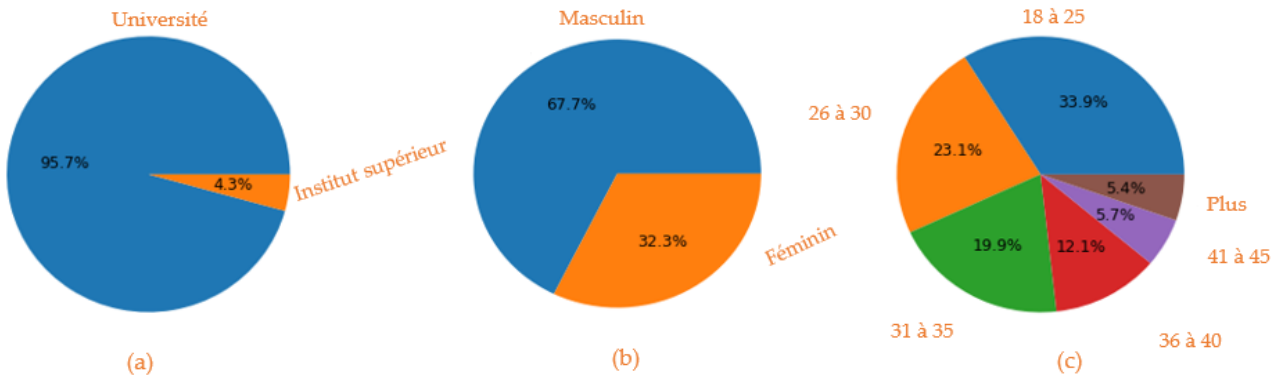

Figure 3. (a) Pourcentage en graphique de la variable Type d'institution. (b) Pourcentage en graphique de la variable Genre. (c) Pourcentage en graphique de la variable Age.

4.2. Résultats de la recherche

4.2.1. Quel est le modèle approprié pour évaluer les risques des WLAN des universités congolaises ?

Cette section est une réponse à la question qui a consisté à construire un cadre conceptuel, partant de ces facteurs capturés, pour obtenir des variables contextuelles qui constituent les risques des WLAN des universités congolaises. Pour répondre à cette question, les auteurs ont d'abord vérifié la fiabilité de l'instrument de recherche en utilisant le test Alpha de Cronbach (en utilisant python comme langage) afin de valider sa consistance interne. Le résultat de ce test a révélé que le questionnaire construit a été fiable car son score Alpha a été de 0,776. Ceci veut dire que tout autre chercheur peut utiliser l'instrument développé dans cette recherche et pourra obtenir des résultats similaires. Ensuite, les auteurs ont testé la pertinence des données collectées pour conduire l'EFA.

Sur ce, le test KMO et celui de Bartlett ont était utilisé. Les résultats du test de Bartlett étaient de 2578,37 pour le khi² et la valeur p = 0,000. Cela nous a permis de rejeter l'hypothèse nulle selon laquelle la matrice de nos données était identique. Le résultat du test KMO qui a été de 0,82 a indiqué que notre échantillon utilisé pour conduire l'EFA a été adéquat car les valeurs KMO comprises entre 0,8 et 1 indiquent que l'échantillonnage de recherche est adéquat (Younis, et al., 2021). Cette valeur a indiqué que les auteurs pouvaient procéder à l'analyse factorielle prévue.

Après avoir confirmé que nos données collectées étaient appropriées pour conduire l'EFA, les auteurs ont pu conduire l'EFA en utilisant Minimum residual comme méthode d'extraction des facteurs et Varimax comme méthode de rotation des facteurs. Ci-dessous se trouve le tableau

qui reprend les deux facteurs retenus avec les valeurs propres (Eigen value) pour chaque facteur, y compris les variances expliquées de chaque facteur et les pourcentage de variance.

Table 4. Facteurs extraits et les informations y référant

Facteur	Eigen value	Variance expliquée	% de Variance	Variance cumulative
Facteur 1	3,1842955	2,546036	31,83	0,318254
Facteur 2	1,22461044	0,789203	0,1	0,416905

Conformément à la règle empirique sur les facteurs à retenir en conduisant l'EFA (Mpia, et al., 2022), dans cette recherche, les auteurs n'ont retenu que les variables dont la valeur de *factor loading* (coefficient de saturation) était supérieure à 0,4, sachant que l'ensemble de données comportait 19 variables ou éléments. Après l'EFA, l'étude est passée de 19 variables à 7 variables qui sont expliquées par les deux facteurs retenus. Les résultats des *factor loadings* sont présentés dans la colonne 5 du tableau 5.

Table 5. Facteurs extraits et leurs relations avec les variables de la recherche

Facteur	Question de recherche	Variable	No. Item	Factor loading
1	Des options d'authentification plus fortes sont-elles disponibles (par exemple, des clés privées) ?	Cle_securite	11	0,734657
	Existe-t-il des interfaces administratives cryptées (par exemple, ssh, https) ?	Crypto	14	0,618512
	Les alertes de sécurité ou les journaux ont-ils été activés (par exemple, syslog, traps) ?	Alertes	15	0,983672
	Existe-t-il des ports ouverts inutiles (par exemple, telnet, http, ftp) dans votre réseau?	Port	12	0,703941
	Ces ports ouverts sont-ils vulnérables à des exploits connus ?	Vulnerable	13	0,694505
2	Est-ce que votre institution a un administrateur réseau ?	Administrateur	18	0,068697
	Est-ce que votre administrateur réseau est un expert en sécurité ?	Expertise	19	0,612371

Enfin, les auteurs ont construit le modèle d'analyse factorielle illustré dans la figure 4 décrivant les facteurs contextuels qui permettent d'évaluer des risques qu'accourent les WLAN des universités congolaises. La figure 4 montre, pour chaque facteur retenu, quelles variables de l'étude sont expliquées par le même facteur. Ces variables sont associées à leurs valeurs de factor loading absolues qui sont supérieures ou égales à une valeur seuil définie selon la règle empirique (par défaut > = 0,4).

Les auteurs ont étiqueté ces deux facteurs après interprétation des résultats de l'EFA. Partant de la compréhension de chaque variable qui leur sont associées, les auteurs ont étiqueté le facteur 1 Niveau de sécurisation et Facteur 2 a été nommé Compétence des administrateurs.

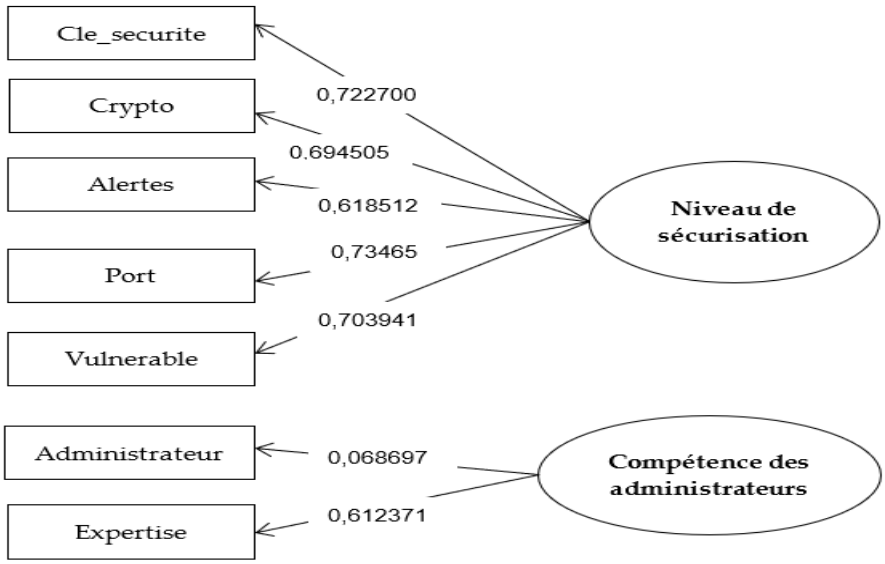

Figure 4. Modèle EFA d'évaluation des risques WLAN construit

4.2.2. Quelle est la fiabilité du modèle développé d'évaluation des risques des WLAN?

Cette section est une réponse à la seconde question de cette étude. Après la construction du modèle EFA, le test Alpha de Cronbach a été conduit sur les deux facteurs retenus. Les résultats ont révélés que le facteur niveau de sécurisation a atteint le score Alpha de 84,05%. Tandis que le résultat du test Alpha de Cronbach pour le deuxième facteur a été de 48,52%. Sur ce, comme le test Alpha doit être de 50% au minimum, les auteurs ont conclu que le deuxième facteur n'est pas fiable et est considéré comme facteur mineur, contrairement au premier facteur qui est considéré comme facteur majeur d'évaluation des risques WLAN des universités congolaises.

4.3. Discussion

Partant du cadre conceptuel (cf. figure 2), les recherches antérieures ont retenu trois facteurs permettant d'évaluer les risques WLAN notamment facteur interne des WLAN lié aux vulnérabilités du WLAN en soi, le facteur humain relatif à l'âge, le niveau d'éducation, et d'autres variables relatives au hackeur et le facteur niveau de sécurisation qui fait référence aux pratiques et outils déployés par une université afin de sécuriser son WLAN. Quant à ce qui concerne l'étude actuelle, la démarcation se situe au niveau où cette recherche a conduit l'EFA afin d'obtenir des facteurs fiables d'évaluation des risques des WLAN dans des universités congolaises. Toutefois, il a été observé que le facteur niveau de sécurisation a été retenu aussi bien par des chercheurs précédents que dans cette recherche avec un score de fiabilité de 84,05%.

5. Conclusion et recommandations

La réalisation de cette recherche a été une expérience très riche dans laquelle un cadre conceptuel d'évaluation des risques WLAN a été construit. Deux facteurs ont été obtenus dont l'un fiable et l'autre non fiable, respectivement facteur niveau de sécurisation et facteur compétence des administrateurs. La présente recherche apporte deux contributions essentielles. Premièrement, les données primaires collectées dans cette recherche contribuent aux connaissances existantes en matière d'analyse des données et data science, car elles constituent un outil de soutien aux chercheurs qui souhaitent mener des études d'analyse de données sur les risques des WLAN des universités. Deuxièmement, cette recherche, en proposant un cadre conceptuel des facteurs d'évaluations des risques WLAN, offre un cadre fiable contenant des facteurs contextuels qui influencent de manière pertinente les risques des réseaux WLAN dans des universités congolaises. Par conséquent, les

facteurs obtenus permettront aux pays similaires à la RDC de mettre en œuvre des systèmes de sécurité adéquats en utilisant ces facteurs comme prédicateurs contextuels afin d'être réalistes lorsqu'ils proposent des solutions pour palier des risques réseaux dans des universités. Cette étude apporte ainsi un soutien aux analystes de données et aux ingénieurs en apprentissage automatique en proposant des facteurs fiables et contextuels qui prédisent les risques des WLAN.

Concernant les travaux futurs, les nombreuses recherches menées depuis longtemps ont fait ressortir que plusieurs travaux de recherche dans la revue de littérature existante ont porté sur l'amélioration du mécanisme de sécurité au sein de ces réseaux (Efstratios, et al., 2022). Au vu des résultats de la présente étude, le cadre conceptuel proposé peut potentiellement orienter la recherche vers la validation empirique de l'effet sur l'amélioration de l'efficacité de la gestion des risques réseaux au sein des universités. En fait, il existe peu d'études empiriques sur l'analyse de la manière dont l'efficacité de la gestion des risques réseaux peut être améliorée dans des universités. La présente étude constitue un premier pas dans cette direction.

Contributions: Conceptualisation, H.N.M.; méthodologie, L.B.N.; validation, H.N.M. & B.I.N.; investigation, L.B.N.; ressources, L.B.N.; traitement des données, H.N.M.; écrire le manuscrit, H.N.M.; visualisation, B.I.N.; supervision, H.N.M. & B.I.N.; correction du manuscrit, H.N.M. Les auteurs ont lu et approuvé la version publiée de ce manuscrit.

Sponsor financier: Cette recherche n'a reçu aucun soutien financier.

Disponibilité des données: Les données ne sont pas disponibles.

Remerciement: Non applicable.

Conflits d'intérêt: Les auteurs déclarent aucun conflit d'intérêt.

Références

1. AAbo-Soliman, M. & Azer, M.A. (2018). Enterprise WLAN Security Flaws: Current Attacks and Relative Mitigations, Proceedings of the 13th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3230833.3230836.
2. Abuhamda, E.A., et al. (2021). Understanding Quantitative and Qualitative Research Methods: A Theoretical Perspective for Young Researchers. International Journal of Research, 8(2).
3. Ciampolini, V., et al. (2021). Cross-Cultural Adaptation and Psychometric Properties of the Portuguese Coaching Life Skills in Sport Questionnaire. Sage Open, 11(2). https://doi.org/10.1177/21582440211024224.
4. Creswell, J.W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches, 3rd ed., Thousand Oaks, CA: Sage Publications, Inc.
5. Dewi, L.C. (2011). Wireless technology development: history, now, and then. ComTech, 2(2).
6. Efstratios, C., Georges, K., & Constantinos, K. (2022). Your WAP is at risk: A vulnerability analysis on wireless access point web-based management interfaces. Security and communication Network. https://10.1155/2022/1833062.
7. Erdil, D.Ü., et al. (2021). Prioritizing Information Sources and Requirements in Students' Choice of Higher Education Destination: Using AHP Analysis. Sage Open, 11(2). https://doi.org/10.1177/21582440211015685.
8. Grawitz, M. (2001). Méthode des sciences sociales, 11e édition, Paris : Dalloz.
9. Hadi, N.U., et al. (2016). An easy approach to exploratory factor analysis: Marketing perspective. Journal of Educational and Social Research, 6(1).
10. Ievgeniia, K., et al. (2021). Information Security Risk Assessment. Encyclopedia, 1, 602-613. https://doi.org/10.3390/encyclopedia1030050.
11. Iliyasu, R. & Etikan, I. (2021). Comparison of quota sampling and stratified random sampling. Biometrics & Biostatistics International Journal, 10(1). https://doi.org/10.15406/bbij.2021.10.00326.
12. Imran, K., et al. (2018). Comparative Study of Existing and Forthcoming WLAN Technologies. International Journal of Computer Science and Network Security, 18(4).
13. Jason, E.J. (2020). Analysis of Security Features and Vulnerabilities in Public/Open Wi-Fi. 2020 Proceedings of the Conference on Information Systems Applied Research Virtual Conference, 13(5333).
14. Jowkar, A.A., et al. (2013). A factor analysis of identifying the customer behavior patterns: A case study in Tehran. European Online Journal of Natural and Social Sciences, 2(3).

15. Kabir, S.M. (2016). Basic Guidelines for Research: An Introductory Approach for All Disciplines, Chittagong: Book Zone Publication.
16. Min-Kyu, C., et al. (2008). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering, 3(3).
17. Mohammad, A.M. (2012). Introduction to Wireless Networks. IGI Global. https://doi.org/10.4018/978-1-4666-1797-1.ch001.
18. Mokonzi, G. & Mwinda, K. (2009). République démocratique du Congo Fourniture efficace de Services dans le domaine de l'enseignement public : Une étude d'AfriMAP et de l'Open Society Initiative for Southern Africa, Open Society Initiative for Southern Africa, Johannesbourg.
19. Mpia, H.N, Mburu, L.W., Mwendia, S.N. (2023). CoBERT: A Contextual BERT model for recommending employability profiles of information technology students in unstable developing countries. Engineering Applications of Artificial Intelligence, 125. https://doi.org/10.1016/j.engappai.2023.106728.
20. Mpia, H.N. (2018). De la vulnérabilité des informations numériques dans les réseaux informatiques : Cas de l'infiltration à travers le rootkit. Etincelle, 21(1). https://doi.org/10.61532/rime211111.
21. Mpia, H.N., Mwendia, S.N. & Mburu L.W. (2022). Predicting Employability of Congolese Information Technology Graduates Using Contextual Factors: Towards Sustainable Employability. Sustainability, 14(20), 13001. https://doi.org/10.3390/su142013001.
22. Nasr, E., et al. (2019). Wi-Fi Network Vulnerability Analysis and Risk Assessment in Lebanon. MATEC Web of Conferences, 281, 05002. https://doi.org/10.1051/matecconf/201928105002.
23. Orçan, F. (2018). Exploratory and Confirmatory Factor Analysis: Which one to use First ? Journal of Measurement and Evaluation in Education and Psychology, 4, 414-415. https://doi.org/10.21031/epod.394323.
24. Pahlavan, K. & Krishnamurthy, P. (2021). Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. Int J Wireless Inf Networks, 28.
25. Paré, G. et al. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, 52(2). https://doi.org/10.1016/j.im.2014.08.008.
26. Persson, I. & Khojasteh J. (2021). Python Packages for Exploratory Factor Analysis", Structural Equation Modeling: A Multidisciplinary Journal. https://doi.org/10.1080/10705511.2021.1910037.
27. Rangel-Pérez, C., et al. (2021). The Massive Implementation of ICT in Universities and Its Implications for Ensuring SDG 4: Challenges and Difficulties for Professors. Sustainability, 13(22), 12871. https://doi.org/10.3390/su132212871.
28. Raquel, P.E, Elena, U.G & Manuela, C.E. (2022). Adoption of information Technology by Microenterprises. Evidence from the Democratic Republic of Congo (DRC). European Journal of Sustainable Development, 11(3).
29. Roopa, S. & Rani, M.S. (2012). Questionnaire Designing for a Survey. J Ind Orthod Soc, 46(4).
30. Sombatruang, N., et al. (2019). Factors Influencing Users to Use Unsecured Wi-Fi Networks: Evidence in the Wild. WiSec '19: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Association for Computing Machinery. https://doi.org/10.1145/3317549.3323412.
31. Sourangsu, B. & Chowdhury, R.S. (2013). On IEEE 802.11: Wireless LAN Technology. International Journal of Mobile Network Communications & Telematics (IJMNCT), 3(4). https://doi.org/10.5121/ijmnct.2013.3405.
32. Wagner, D.A., et al. (2005). Monitoring and Evaluation of ICT in Education Projects. A Handbook for Developing Countries, Information for Development Program (InfoDev), Washington DC.
33. Waliullah, M. & Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilities: A Literature Review. International Journal of Advanced Computer Science and Applications, 5(1).
34. Xinming, L. (2022). The Standard of Wireless Network Technology and Its Application in Router. Highlights in Science, Engineering and Technology, 27.
35. Younis, J., et al. (2021). The Impact of Human Resource Practices on Nurses' Turnover Intention: An Empirical Study of Hospitals in North Lebanon. Journal of Business Theory and Practice, 9(4). https://doi.org/10.22158/jbtp.v9n4p8.
36. Zheng, R et al. (2021). Assessing the security of campus networks. Sensors, 21, 306. https://doi.org/10.3390/s21010306.