Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Evaluating VPN Users' Trust Among Information Technology Professionals and Nonprofessionals in Lagos, Nigeria

Ahmad Adisa Adebayo
Department of Information Technology, Communication and Information Science, University of Ilorin, Nigeria.

Received 30 Jan. 2026; accepted 2 Jun. 2026; available Online 23 Jun. 2026

Abstract

This paper investigates the factors that lead to trust in Virtual Private Networks (VPNs) among the IT professionals and non-professional users in Lagos, Nigeria, regarding the perception of security, privacy, and usability. Using the Technology Acceptance Model (TAM), the study uses an exploratory qualitative design and an interpretivist paradigm to examine how users build trust in VPN technologies. The interviews were semi-structured and included 30 participants (10 professionals and 20 non-professionals), with data being analysed thematically. The results have identified four foundational determinants of VPN trust: technical configuration and encryption protocol, provider reputation and reliability, trust gap between paid and free VPNs and user education and awareness. IT professionals were highly technical savvy and placed trust in the strength of encryption, the configuration of protocols and industry standards. Non-professionals on the other hand evaluated trust with mainly experiential signals like brand familiarity, peer referrals, and perceived anonymity. Both sampled indicated higher confidence with paid VPNs because of better security guarantees and the mitigation of data exploitation. The paper identifies a continued knowledge gap that breeds misinformation about VPN functionality that adds to disconnect between perceived and actual security. It suggests enabling better regulation, transparency among the providers, and multi-level user education measures to enhance informed adoption of VPN. The paper ends by giving limitations of the study in terms of self-reported figures and those based on experience.

I. Introduction

Network infrastructure is commonly distributed across multiple locations, including corporate branches, data centers, and cloud-based infrastructure [1]. VPN systems are an essential part of such setups, as they serve as the glue that ensures the connection of the different locations safely through the encryption and authentication of the communication between endpoint couples over an untrusted network, like the Internet [2]. Furthermore, the recent transition to remote work, digital banking, online education and cloud computing has resulted in a significant increase in VPN usage in Nigeria, since they are frequently implemented as an access control and mechanism to protect the network segments and services [3].

While VPNs are popular, they have a number of drawbacks and risks, such as DNS leaks, kill-

Keywords: Data encryption, information security, remote work, security posture, virtual private network (VPN).

Production and hosting by NAUSS

* Corresponding author: Ahmad Adisa Adebayo
Email: adebayoadisa2015@gmail.com
doi: 10.26735/NWUW3576

switch failures, poor encryption settings, and misunderstandings about anonymity [4]. Past research primarily concerns technical vulnerabilities and the target audience of the VPN use in western countries, little research has been conducted on the subject of VPN trust and security concerns among users in developing countries like Nigeria [5]. The largest technological and commercial hub in Nigeria, Lagos faces a particular situation that combines the awareness of cybersecurity with growing concerns about cybercrime, the instability of its Internet service providers, and the growing digital dependency.

In spite of these shortcomings, most VPN customers place significant trust in these technologies and transfer the trust already placed on their network provider to the VPN provider without fully understanding their shortcomings. Hence, this research in particular makes a contribution, as it compares technically informed trust perceptions with the experiential trust perceptions of non-technical users. Thus, the study aims to assess the trustworthiness of VPN among users based on the security, privacy, and usability. This study is based on the following objectives:

1) Highlight the factors influencing trust in VPN services among IT professionals and non-professionals.
2) Compare the trust perceptions of IT professionals and non-professional users regarding VPN services.
3) Recommend strategies to improve VPN trust and cybersecurity awareness in Lagos, Nigeria.

II. Literature Review

This section summarizes important concepts, theory, and empirical studies regarding adoption of VPN, building trust, security issues, and acceptance of technology. It builds on the Technology Acceptance Model (TAM) and shows the gaps in the literature, particularly the limited work on developing countries and the absence of comparative study between users/non-users of IT in the high-risk digital environment of Nigeria.

A. Review of Related Concepts

Virtual Private Networks (VPNs) are technologies for secure and private Internet access using tunnelling protocols and authentication systems. VPNs are increasingly used for remote connection, cyber security, anonymity, and circumventing network restrictions. In [6], states that the commercial VPN services have gained global popularity because of the growing apprehensions about online surveillance, cybercrime, and data privacy breaches. VPNs have become more widely used in Nigeria due to the nation's growing reliance on digital tools, a weak network connectivity, concerns about cybercrime, and the rise of remote work.

Trust is one of the most important factors when considering VPN services adoption and ongoing use. Trust is a user's faith in the ability of a VPN provider to securely process data, ensure privacy and safeguard the user against cyber threats. Many VPN users have the false notion that they are completely anonymous online when they use a VPN, which leads to false expectations of security, [7]. The willingness to use VPNs therefore relies on the technical knowledge of users, the reputation of their providers, and the perceived reliability of the VPN provider.

The Technology Acceptance Model (TAM) by Reference [8] serves as a helpful theoretical model to analyze the trust and adoption of VPN adoption behaviour. TAM is based on two constructs: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). PU is the extent to which the user thinks that the technology helps his/her performance or security, whilst PEOU is the extent to which the user thinks the technology is easy to use [9]. TAM has been extended to include trust and perceived risk as external variables that affect behaviour intention in the scope of cyber security research. Technical configuration and cryptographic mechanisms also contribute to the PU of VPN adoption, as users value highly secure systems as good protection against online threats. Provider reputation diminishes risk and builds trust which positively affects PU and PEOU. The way users are educated and the importance of cybersecurity awareness also influence their understanding of VPNs, privacy, and usability [10].

Although, VPNs are supposed to be secure, there are several vulnerabilities associated with them, such as DNS and IP leaks, kill-switch failures, misconfigurations, outdated protocols, and risks from the VPN provider [11], [12]. Additionally, Man-in-the-middle attacks, DNS hijacking, brute force attacks, and malicious VPN apps are among the other cyber threats that face VPN users [13]. These risks are compounded by the high rate of cybercrime in Nigeria and the ambiguous regulatory landscape in the country as outlined in the Nigeria Data Protection Act (NDPA) [14]. Thus, the rising numbers of threats in the cyber world, internet fraud better known as "Yahoo-Yahoo" and surveillance concerns have driven the growth of VPN usage in Nigeria. But the gap in digital literacy persists in affecting understanding of VPN functionality. These contextual understandings differ from the ones found in western studies on VPNs [15].

B. Review of Related Works

Trust in VPNs, perceived security and technology adoption in various digital contexts have been studied. In [16], the use of VPNs was explored and discovered that many users are not technically savvy but rely on their perception of privacy and freedom of the Internet. It also found that users tend to have a lack of understanding about the limitations and vulnerabilities of VPN technologies.

The authors in [6] performed a study of the commercial VPN landscape and highlighted some significant security issues such as traffic leakage, substandard encryption implementation, and missing provider transparency. Trust in VPN services is largely based on its accountability and technical reliability, according to their findings. Likewise, In [17], DNS leakage weaknesses were identified in commercial VPN solutions and noted that users' perceived security does not necessarily equate to their actual security.

The authors in [15] investigated the perceptions of users of VPNs and found that many users resort to using monetised review sites and promotional information to choose their VPN providers. This behavior leads to a high risk of misinformation, and impacts users' trust decisions. The study also revealed that the reputation of the provider has a significant influence on the intention to use, especially among non-technical users.

In [18], determined that perceived usefulness has a significant impact on the decisions of adopting cybersecurity technologies in relation to TAM. They found that people are more likely to trust and use technologies that they feel can help them keep their personal information safe and make online more safer. Another important determinant of behavioural intention was perceived ease of use which was found among non-technical users.

In Nigeria, cybersecurity awareness research suggests that digital literacy greatly affects online trust behaviour. Lagos's internet users are increasingly relying on VPN services, with cyber fraud, online restrictions, and an unstable internet infrastructure being primary reasons. Thus, in Nigeria, there is a dearth of empirical studies that have directly compared the trust perception of both IT and non-IT users of VPNs. This study hence fills an important gap in studies by examining the role of technical expertise in the formation of VPN trust among users in Lagos, Nigeria.

C. Theoretical Framework: Technology Acceptance Model (TAM)

The Technology Acceptance Model proposed by Reference [8] is a model that aims to explain technology acceptance by using two variables of perceived usefulness and perceived ease of use. In cyber security settings, TAM has been expanded to trust and perceived risk. This study has found that: Technical configuration and encryption affects perceived usefulness. Provider reputation has a positive effect on perceived risk, which in turn affects the perceived ease of use. User awareness has a positive effect on behaviour intention and informed adoption. Paid VPN services are linked to higher perceived usefulness and trustworthiness.

Moreover, TAM frames the effect of technical configuration on PU (security benefits), the effect of provider reliability and education on PEOU (reduced uncertainty), and the paid-free gap on perceived risk and behavioral intention. The level of expertise (professionals vs. non-professionals) is an important moderator. As shown in Fig. 1, TAM explains the relationships between the external

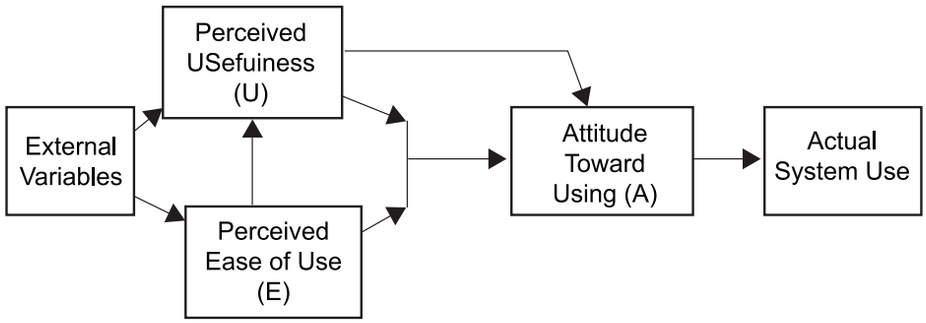

Fig.1 Technology acceptance model illustration [8].

variables, perceived usefulness, perceived ease of use, behavioural intention and actual system use, and gives the theoretical basis for understanding the trust perceptions of the users in this study.

III. Methodology

A. Design

This study employed a qualitative research design, specifically an exploratory descriptive research approach to understand in-depth the trust in Virtual Private Networks (VPNs) among IT professionals and non-professionals in Lagos, Nigeria. It is a suitable design as it enables the discussion of subjective experiences, perceptions and attitudes, which play a vital role in comprehending the complex factors affecting trust and risk awareness in using VPN. The qualitative design facilitated the collection of narrative data through semi-structured interviews, enabling the researcher to investigate deeper into participants' thoughts, attitudes, and behaviors regarding VPN usage in Nigeria.

B. Instrument

The instrument for this study was a research interview guide, developed as a primary data collection instrument given that it will allow the researcher to probe deeply, the experiences, perceptions, and concerns of professional and non-professional users of Virtual Private Networks (VPNs). Semi-structured interviews are suitable in conducting this qualitative research since it enables the researcher to ask open-ended questions and the flexibility to delve deeper into the answers of the participants to capture more natural data [19].

The interview guide was developed based on the objectives of the study and structured into three sections. In Section A, the demographic and background data regarding the participants i.e., age, gender, professional background, years of experience, and their patterns of typical use of VPNs (e.g., remote access, data protection, or secure communication) were collected. Section B concentrated on their trust and perception of privacy when using VPN with issues regarding data management, and transparency of the providers. Section C compiled their recommendations and suggestions on how they think VPN trust in users and professional environments can be improved.

C. Sampling

The population used in the study was 30 VPN users, which consist of Information Technology (IT) professionals as well as non-professionals who actively use Virtual Private Networks (VPNs) in their work or personal lives. These individuals include network administrators, cybersecurity analysts, system engineers, IT managers, software developers, among others, who engaged in the management or protection of digital infrastructure. The research targets IT professionals and non-professionals in both the government and private sectors who are employed in sectors like finance, healthcare, telecommunications, education, and technology companies. Purposive sampling approach was utilised to ensure that all the sampled participants have a significant experience and understanding of VPN usage. The purposive method that involves both non-professional users and IT professionals allows conducting a comparative analysis of VPN trust issues in

various user scenarios.The 30 sample used (10 IT professionals and 20 non-professionals) is sufficient since qualitative research focuses on depth rather than breadth. Research indicates that 30 interviews are adequate to achieve data saturation [20].

D. Data Collection

The interviews were done in a virtual environment either via phone (call) or internet (e.g., Zoom, Telegram, Microsoft Teams, WhatsApp call) and were conducted in accordance with the availability and convenience of the participants. Each interview lasted 20 to 30 minutes. The interviews were recorded on the tape with the consent of the participants and transcribed word-to-word to form the core of analysis. The interviews were arranged in a preferred time and form that was more participatory and also made them accessible to the participants. The flexibility comes in particularly handy among busy people and those with limited internet connectivity. Prior to taking part, all respondents received information about what the study was for, what they would have to do, and what their rights were as part of the research. A consent form was sent online to the participants, who read it and agreed to it before participating in the interview.

E. Analysis

This paper used thematic analysis method of analysis to interpret the collected interview data. The thematic analysis aided in determining the patterns and themes pertaining to the trust of VPN users, and suggestion to rectify it. Interview recordings were transcribed verbatim and the transcripts were coded manually into groups of themes e.g. trust in security features, privacy, and usability issues. This method is appropriate to the qualitative study since it allows the researcher to identify, analyse, and explain the trends or themes of the results and bring richness and full conceptions of the experiences, perceptions, and understandings of the subjects on the question of VPN trust and vulnerability [19].

IV. Results

This section presents the demographic description of interviewees and various codes that emerged after the transcribed responses were thoroughly analyzed using thematic analysis.

A. Demographic Profile of Respondents

A total of 30 participants which consist of 10 professionals and 20 non-professionals were interviewed and their data were analysed using thematic analysis. Participants were coded as respondent 1 – 30 with the professional users coded respondents 1 to 10 while the non-professional users coded respondents 11 -30. Most of the participants work in the private sector with 63.33% of the participants falling in this category. Nevertheless, 20 percent work in the government sector and 10 percent freelancer/self-employed and 6.67 percent students. In addition, most of the participants rated their knowledge about VPN as intermediate with 70% of the participants rating their knowledge as intermediate. Nevertheless, 26.67% of respondents think they are an expert and 3.33% respondents said that they are a beginner when it comes to VPN. 63.33% of respondents use it very often and 36.67% use it once a week or once a month. Great percentages of participants who use VPN have a high likelihood of giving rich insight by the participants with 60.00% of the participants using it unofficial and 20.00% using it official with, another 20.00% using it both official and unofficial. The outcome showed that 30.00% of the participants have been using VPN between 1-3 years and 43.33% of the participants have been using VPN between 4-6 years. 10.00% of the participants have used VPN between 7-9 years and 16.67% have used VPN more than 10 years. This experience year with VPN placed the participants in a position to provide valuable information regarding VPN security posture. The details are shown in Table I.

B. Analysis of Interview Responses

The thematic analysis revealed that four themes emerged with regards to the user trust in VPN: Technical Configuration and Encryption Protocols,

TABLE I
DEMOGRAPHIC PROFILE OF RESPONDENTS

Demographic variable	Categories	Frequency (%)
Employment/Profession	Private sector	19 (63.33%)
	Public sector	6 (20.00%)
	Freelancer/self-employed	3 (10.00%)
	Students	2 (6.67%)
Technical Knowledge	Beginner	1 (3.33%)
	Intermediate	21 (70.00%)
	Expert	8 (26.67%)
Frequency of Usage	Frequently	19 (63.33%)
	Occasionally	11 (36.67%)
Purpose of Usage	Unofficial	18 (60.00%)
	Official	6 (20.00%)
	Official and unofficial	6 (20.00%)
Duration of Usage	1-3 Years	9 (30.00%)
	4-6 Years	13 (43.33%)
	7-9 Years	3 (10.00%)
	10 Years or more	5 (16.67%)

Provider Reputation and Reliability, Paid vs Free Trust Gap and User Education and Awareness.

1) Technical Configuration and Encryption Protocols: The results show that IT professionals and non-professionals both realise that technical configuration and encryption protocols are key factors that inform trust in VPN services. Nevertheless, professionals show a more detailed and technical understanding of these aspects, often referencing specific protocols and configurations, whereas non-professionals focus more on general perceptions of encryption strength and its protective capabilities. Professional users (Respondents 1-10) emphasised the importance of configuration in maintaining VPN security in a consistent way. According to Respondent 1"most of the security issues that users experience on *VPN are by virtue of… configuration… authentication protocol and the encryption protocol that you want… your VPN to use." Respondent 5 pointed out the benefits of security by stating, "for IPsec, I will say that IPsec is very, very secure and it is very difficult for hackers to break the protocol*." This technical specificity reflects a higher degree of functional insight probably due to their professional exposure in implementation and administration of VPN systems. Encryption strength was another critical trust factor identified by professionals, as indicated by Respondent 4 saying "*VPNs are secure… it is encrypted communication through a tunnel… where you have slip ups, is when access is falling into the wrong ends*."

Non-professionals' (Respondents 11-30), in turn, acknowledged encryption but addressed it less technically, with many equating encryption with general online safety measure. An example is Respondent 19 saying, "*once your IP is hidden… they might not have access to you*," while Respondent 28 compare it to the privacy mode of web browsers stating that "*it's just like*

using incognito mode… it's going to put some shade on it." The non-professionals did not discuss which protocols to use and how to configure VPN connections such as IP masking and data protection, instead concentrating on observable VPN effects.

Both groups recognized that extra protection leads to increased trust. Professionals cited supplementary mechanisms such as firewalls or IP whitelisting (Respondent 7), but non-professionals references to safeguards were largely implicit, couched in terms of threats being imagined to be blocked. This discrepancy implies that the emphasis on technical settings and encryption is similar across the board, whereas knowledge levels and trust requirements vary greatly between professional and non-professional users.

2) Provider Reputation and Reliability: Perceptions of provider reputation and reliability of their security practices are key determinants of trust in VPN services by both IT professionals and non-professionals. Yet, professionals (Respondents 1 to 10) are likely to evaluate the reputation of providers from the lens of industry benchmark and technical credibility, whereas non-professionals (Respondents 11-30) incline to rely on personal experiences, recommendations, or brand familiarity. The credibility of established vendors and industry recognition were all regularly mentioned by the professionals as aspects of building trust. Respondent 7, as an example, said, "*for professional space, what they use is quite reliable… checkpoints… is one of the VPN that CBN use… which is obviously reliable*." Similarly, Respondent 9 also mentioned that reputable companies "*go extra mile… to improve the security of their product*," meaning that the perceived integrity of providers operational practices directly influence the trust of the users. Respondent 10 shared this point of view, stating that "*loopholes in every security system*," but they did trust some providers because the paid versions provided some benefits that fulfilled professional security requirements.

In comparison, non-professionals depended more on interpersonal trust and experience of use. Respondent 24, whose confidence is due to VPN "*given by the person… and… downloaded directly from the Play Store*," and Respondent 18 who felt cautious after having their VPN use detected multiple times on the websites many times indicating a drop in confidence as a result of personal negative experiences. Even where the VPN effectively performed properly, detection problems were also viewed to weaken reliability. Both groups recognized that no provider could promise total protection, but professionals were more likely to realise this as a reality about security, as Respondent 5 expressed: "*there are always loopholes in every security system*." Non-professionals, however, tended to explain it as a justification to restrict usage to lower-sensitivity applications.

In general, provider reputation and reliability are critical determinants of trust in both populations, though the basis for evaluating these qualities is divergent. Professionals underline objective factors of technical standards and industry popularity, and non-professionals highlight tangible user experiences and trusted recommendations. This distinction points out the need to differentiate trust-building initiatives to various user groups, to provide a balance between the technical credibility and user-facing assurances.

3) Free Versus Paid Trust Gap: A notable difference was found in VPN trust between paid and free services where both IT professionals and non-professionals tended to view paid VPNs as more secure and reliable. This trust gap was described, however, by professionals in the context of technical performance and contractual guarantees, and by non-professionals in the arena of perceived safety and a threat of data misuse. Paid services frequently evoked positive expectations among professionals due to greater levels of security and accountability. Respondent 2 "*for the ones that are paid for, they are secured… [for] free… they are not always that secure… your information and can actually be exposed to third party*." Likewise, Respondent 6 remarked, "*If you… pay to use VPN… the level of security is higher compared to… free VPN*." These opinions were rooted in the facts that paid providers generate enough interest in preserving high-quality encryption and preventing data breaches to secure

their reputation and customer base.

Non-professionals also understood the effectiveness of paid VPN but were more likely to pay attention to the aspect of trust and data privacy. Respondent 22 cautioned that free services "*have high chance of selling our information*," and Respondent 23 stated that providers of free versions were not likely to "*go the extra mile of adding additional layer of security… when it is free.*"This kind of rhetoric alludes to the fact that since no financial exchange is involved, then less of a responsibility is placed on the provider to secure user data. Nevertheless, this overall sentiment was not shared by all the non-professionals, with some of them showing signs of ambivalence due to having used free VPNs that performed satisfactorily in non-sensitive activities. Some would sacrifice security to gain convenience or price advantages, especially when VPNs were only applied to evade geo-restrictions.

Holistically, trust gap between paid and free VPNs is influenced by a combination of contractual, technical and experiential processes. Professionals are more likely to base their tendency to use paid options on objectively quantifiable security conditions and contractual claims, whereas non-professionals rely on perceived ethical behaviour and personal experience. This implies that marketing and security communication approaches must consider both the technical strength and the ethical guarantees of VPN providers to establish confidence among the variety of user groups.

4) User Education and Awareness: Sustained user education and awareness is necessary to build trust in the use of VPNs and reduce exposure to risks. Among IT professions and non-professions, participants also underlined the necessity to access credible information that is accurate and up-to-date, gathered through varying sources. IT professionals commonly outlined an active attitude toward life-long learning, communicating with original equipment manufacturers (OEMs), industry analysts, and formal training outlets. Respondent 1 emphasized, "*The way I learnt my own is from the VPN provider themselves… they have come up with the training on those OEM portal to the experts.*"This highlights the perceived importance of directed, controlled-learning. Respondent 2 likewise cited the use of authoritative market research: "*Gartner is a famous research companies [sic] that research cyber security solutions.*" Professional users also integrated in their learning, new online tools that have emerged. A mixture of formal and informal knowledge channels was reported by Respondent 3, who stated that "*I use AI chat, GPT precisely, and I use YouTube… to stay up to date*," Using networking websites like LinkedIn as well as attending webinars also emerged as a noteworthy strategy, which allows practitioners to gain access to both expert opinion and peer experience.

Less concerned with formal certifications, non-professional users, nevertheless, also emphasized awareness. Their sources of learning frequently focused on the availability of media and peer recommendations. Respondent 15 answered, "*From a friend, other users who have been expert on the VPN*," which implies trust in interpersonal information exchange. The others used publicly accessible materials, with Respondent 11 stating "*Generally, it's google… it takes us to forums, blogs, Stack Overflow…*" and Respondent 12 adding "I follow some pages on social media that talk about VPN."

Both groups highlighted the importance of active information distribution by VPN providers including specific information portals and awareness campaigns. Respondent 21 stated, "*A VPN company has a special page dedicated to information about all the features available," while Respondent 22 urged greater efforts: "If they put regulations in place… and… make the awareness the same way governments… do for pandemics.*" In general, professionals prefer to ground awareness strategies on disciplined, industry-based platforms, but non-professionals lean towards affordable, peer-driven ones. This difference implies that trust-building entails a combination of methods, which employs both technical skills and inclusive and accessible outreach.

C. Mapping of Results to Information System Theory

In order to validate the outcome of this study, the emerged themes for VPN users' trust among IT professionals and non-professionals are mapped or cross-tabulated against the external factors

TABLE II
SUMMARY OF MAPPING TABLE

S/N	Theme from the Research Analysis	Factors from Information System Theory/Model	Role of VPN Trust
1	Technical configuration & encryption	Perceived Usefulness	Determines belief in VPN effectiveness
2	Provider reputation & reliability	Perceived Ease of Use	Reduces cognitive burden and uncertainty
3	Paid vs Free trust gap	Perceived Usefulness / Behavioural intention	Signals security quality and accountability
4	User education & awareness	Perceived Usefulness / Perceived Ease of Use (External variable)	Shapes accurate trust and informed adoption

(reasons) that determine users' adoption of technology as established in information systems theory such as Technology Acceptance Model (TAM). This is aimed at verifying the outcome of the proposed interpretive method against the stated framework for investigating or predicting user acceptance or adoption of a technology like VPNs. Briefly, In technology Acceptance Model (TAM), it is postulated that technology acceptance by users depends on some external factors such as perceived usefulness or benefits, perceived ease of use, attitude towards use and the intention to use. These highlighted factors in the theory are cross tabulated against the factors that determine the security posture in VPNs as emerged from this study.

The mapping or cross tabulation in Table II shows that technical configuration & encryption is one of the reasons that determine the belief in VPN effectiveness and can be mapped to User perceived usefulness in TAM model. Also, Provider reputation & reliability is another factor that emerged as reason that reduces cognitive burden and uncertainty. This factor can be mapped to Perceived ease of use as found in the model. Similarly, Paid vs Free trust gap makes signals security quality and accountability. This can also be mapped to Perceived usefulness / Behavioural intention. Finally, User education & awareness shapes accurate trust and informed adoption. It can be mapped to Perceived usefulness / Perceived ease of use (External variable).

D. Discussion

Findings indicate four major determinants of VPN trust; technical configuration/encryption, provider reputation/reliability, and the paid–free trust gap and user education and awareness, which all parallel the trends observed in the literature, but indicate subtle differences existing in the opinions of IT professionals and non-professionals.

First, technical configuration and encryption protocols were appreciated by both groups, although professionals showed a much stronger understanding, mentioning particular protocols (e.g., IPsec) and additional security measures, such as IP whitelisting. This reflects literature results that trust is founded on encryption standards and configuration integrity [18], [6]. The findings also reveal that technical security features positively affected Perceived Usefulness (PU) from a TAM perspective, indicating that stronger encryption equated directly with improved cybersecurity and privacy protection to the professionals' perceived degree of usefulness [18]. VPN effectiveness evaluation, by contrast, was mostly done by non-professionals, who focused on externally visible results such as IP masking, access to the Internet, and the perceived anonymity. Non-technical users were not as knowledgeable about cybersecurity, which led to the increased impact of Perceived Ease of Use (PEOU) over technical assessment. This is why there is a trust gap between IT professionals and non-professionals. Objective security assessments were relied on by the professionals, and convenience, simplified user experiences were relied on by the non-professionals.

Second, the reputation and reliability of providers is another key determinant of trust among both groups, and previous literature emphasized brand credibility, transparency, and no-log policies [21], [22]. Industry benchmarks and technical performance analysis by professionals, along with interpersonal recommendations and personal experiences by non-professionals, an approach the literature cautions may be shaped by marketing and biased review platforms [22]. The perceived risk was lessened and the behavioural intention to use VPN services was increased when provider reputation was applied to the TAM, as it was considered an external variable. Those who used a reputable VPN service provider felt that their services were more reliable, protected data and more credible. The decrease in perceived risk led to an increase in both PU and PEOU because users thought that trusted providers would be safer and more convenient to trust when using the Internet.

Third, the findings verify widespread perception of higher security in paid VPNs: a pattern reflected in the existing literature, where free VPNs were associated with increased vulnerability risks, such as malware, DNS leakage, and weak encryption [23], [24]. Professionals in the study framed this preference in the context of contractual responsibility and measurable security advantages, which resonates with the principles Zero Trust of continuous verification of identity and tightly guarded access. Non-professionals contextualised the choice as ethical trust instead, as paid services will not sell data, which aligns with the noted in the literature that various users tend to mix commercial models with security assurances [24]. In the context of TAM, paid VPNs rose the PU for participants, as they believed that it provided more cybersecurity benefits and stable performance. Free VPNs, however, were associated with increased perceived risk owing to the apprehension of selling data, weak encryption and intrusive advertising. PEOU also was significant among non-professionals, as free VPNs were more readily available and more straightforward to use, though they were not as trusted.

Fourth, User Education and Awareness was a key factor in the formation of trust in VPNs and this concurs with the literature findings concluding that awareness is a primary factor determining trust and perception of vulnerability, and that a majority of users, particularly non-technical users, have misconceptions about VPN capability as a result of marketing and insufficient technical knowledge [7]. Therefore, when choosing a VPN, IT professionals used formal cybersecurity courses, OEM documentation, LinkedIn groups, webinars, and industry certifications for their research. Non-professionals relied heavily on social media information, blogs and peer influence and online tutorials. A TAM perspective showed that cybersecurity awareness led to increased PU and PEOU, that is, users' understanding of the functionality and limitations of VPNs, as well as their security implications. Educated users had higher behavioral intention due to their higher confidence in determining the effectiveness of VPN and their privacy claims.

Across themes, this study gives insightful analytical findings on the influence of technical expertise on VPN trust perception among internet users in Lagos, Nigeria. The study shows that VPN trust is not only based on the technological functionality, but also on the knowledge level, perceived value of security and the understanding of risk.TAM showed that the IT professionals have a stronger preference for Perceived Usefulness (PU) due to their focus on tangible attributes of VPN services like their level of security (encryption, DNS leak defense, protocol efficiency, etc.). Their trust decisions are, therefore, based on technical validation and assessment based on evidence. On the other hand, perceived ease of use (PEOU), provider popularity, convenience, and social influence are more important when considering the VPN services provided to non-professionals. This results in the conceptual trust gap which exists between technically knowledgeable users who are interested in objective security performance and non-technical users who are more concerned with usability and perceived simplicity.

E. Validity and Reliability

Credibility, dependability, and conformability [25] were used to improve the trustworthiness

of the findings. Member checking and peer debriefing were used to enhance credibility, and data triangulation between the professional and non-professional participant groups were used to enhance it. Reliability was facilitated by verbatim transcription, reflexive journaling, and an independent coder review of selected transcripts to achieve consistency in coding (inter-coder agreement). Also, reliability was assured through a process of audit trail throughout the thematic analysis process. These tactics reduced the biases that are often present in self-reported qualitative data and contributed to the contextual transferability.

V. Conclusion and Recommendations

This study aimed at assessing the levels of trust of VPN users among IT professionals and non-professionals in Lagos, Nigeria, revolving around some crucial variables that affect trust in professional work, and the general implication of the adoption of secure VPN. According to the findings of the qualitative research of the perception and attitude of 30 respondents on the trust associated with VPN, the research found out that there was a large gap between how the professionals and non-professionals perceived and reacted.

For trust factors, IT professionals put more emphasis on technical resiliency, encryption levels, and adherence of providers, whereas non-professionals focused on convenience, reputation, and assumed ethics of providers. Although contextual, the findings are consistent with a global trend of cybersecurity risks, further supporting the belief behind trust through balance of technical security, user competence, and transparent administration. To increase the trust of users in VPN, it is recommended that regulatory controls on VPN providers should be enhanced. Concerns regarding provider trustworthiness, jurisdictional risk, and possible government surveillance were sounded by both professionals and non-professionals. Regulators of cybersecurity at national levels must mandate VPN providers in Nigeria to divulge their logging policies, jurisdictional compliance, and security certifications. This would make things more transparent and allow informed decision making. The earlier research emphasised that providers' transparency increases with regulatory interventions aimed at enhancing user trust and minimising the chances of information leakage [26], [27].

The data used in this study was self-reported, and it was based on the claims of the respondents with regards to their experiences, practices, and perceptions, which constitute a limitation for this study. Self-reported data are susceptible to biases like social desirability bias in which subjects portray themselves in a better (more desirable) light and recall bias where specific subjective experiences can be inaccurately remembered or selectively revealed [28]. This could have affected the validity and comprehensiveness of data collected, especially when it comes to delicate issues like security leaks or inefficient usage habits.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] C. Leberknight, J. Tsai, and Y. Wang, "VPNs and user privacy: A comprehensive analysis," *Privacy and Security Journal, 8(4), 200–215*, 2021.

[2] W. Alasmary, F. Alhaidari, and M. Alshaikh, "Security implications of large-scale VPN deployments in enterprise environments," IEEE Access, 10, 114567–114580. https://doi.org/10.1109/ACCESS, 2022.

[3] A. Rosic, D. Novak, and M. Petrovic, "Enhancing VPN protocols for improved cybersecurity," *Journal of Network Security*, 12(1), 33–47, 2021.

[4] X. Liu, Y. Li, and J. Yu, "DNS hijacking in VPN environments: Detection and prevention approaches," IEEE Transactions on Dependable and Secure Computing, 19(2), 905–920, 2022.

[5] S. M, U. Haq, "Analysis of VPN vulnerabilities and insider threats in remote-work infrastructure," *International Journal of Research in Interdisciplinary Studies*, 3(2), 112–128, 2025.

[6] M. T. Khan, J. DeBlasio, and G. M. Voelker, "An empirical analysis of the commercial VPN ecosystem," IEEE Security & Privacy, 20(2), 38–46, 2022.

[7] S. Ramamurthy and R. Bhargavi, "User misconceptions about VPN privacy: An empirical analysis of browser fingerprinting and tracking vulnerabilities," *Journal of Computer Security*, 31(3), 375–392, 2023.

[8] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, 13(3), 319–340, 1989.

[9] R. P. Bagozzi, "The legacy of the technology acceptance model and a proposal for a paradigm shift," *Journal of the Association for Information Systems*, 8(4), 244–254, 2007.

[10] Y. Lee, K. A. Kozar, and K. R. Larsen, "The technology acceptance model: Past, present, and future," Communications of the Association for Information Systems, 12(1), 752–780, 2022.

[11] J. Ren, D. Lindskog, and L. Cheng, "Security weaknesses in VPN protocols: A comprehensive review," IEEE Communications Surveys & Tutorials, 23(1), 342–375, 2021.

[12] J. Baek, S. Lee, and J. Park, "VPN client security assessment: Analysis of configuration vulnerabilities," Security and Communication Networks, Article 2478564, 2023.

[13] K. Qollakaj, "A study on the VPN security landscape post Covid-19," Array, 27, Article 100437. https://doi.org/10.1016/j.array.2025.100437, 2025.

[14] Nigeria Data Protection Act, 2023, "Federal Republic of Nigeria," https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf, 2023.

[15] S. Ramesh, T. Vyas, and R. Ensafi, "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers" arXiv. https://arxiv.org/abs/2208.03505, 2023.

[16] A. Dutkowska-Żuk, M. Tahaei, K. Renaud, and R. Dey, "How and why people use virtual private networks," In 31st USENIX Security Symposium. USENIX Association. https://www.usenix.org/system/files/sec22-dutkowska-zuk.pdf, 2022.

[17] M. Ikram, N. Vallina-Rodriguez, and G. Tyson, "Identifying DNS and traffic leakage vulnerabilities in commercial VPN services," IEEE Transactions on Dependable and Secure Computing, 19(5), 3073–3088, 2022.

[18] S. Aggarwal, V. Kumar, and K. Sunil, "Consumer behaviour patterns in VPN adoption decisions," *Journal of Information Security and Applications*, 74, Article 103387, 2023.

[19] J. W. Creswell and C. N. Poth, "Qualitative inquiry & research design: Choosing among five approaches (4th ed.)," SAGE, 2018.

[20] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? An experiment with data saturation and variability," Field Methods, 18(1), 59–82. https://doi.org/10.1177/1525822X05279903, 2006.

[21] M. J. Awan, A. Yasin, and S, Ahmed, "Evaluating user comprehension of VPN provider no-logs claims," *Journal of Cybersecurity*, 9(1), Article tyad010, 2023.

[22] C. Zhang, Z. Cai, W. Chen. X, Luo, and J. Yin, "Flow burst: Exploitation of a VPN flow control vulnerability," In 29th USENIX Security Symposium (pp. 1–16), 2021.

[23] S. Nanda and R. C. Panigrahi, "Malware prevalence in free VPN applications: A security analysis," IEEE Access, 11, 53817–53834, 2023.

[24] A. Malik, M. A Shah, and Z. Malik, "Analysis of IPv6 traffic leakage in free VPN services," *Journal of Network and Computer Applications*, 213, Article 103569, 2023.

[25] Y. S. Lincoln and E. G. Guba, "Naturalistic inquiry," SAGE, 1985.

[26] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *International Journal of Information and Education Technology*, 10(5), 378–382, 2021.

[27] Organisation for Economic Co-operation and Development, "Embedding values and attitudes in curriculum," OECD Publishing, 2021.

[28] P. M. Podsakoff, S. B. MacKenzie, and N. P. Podsakoff, "Sources of method bias in social science research and recommendations on how to control it," Annual Review of Psychology, 63, 539–569. https://doi.org/10.1146/annurev-psych-120710-100452, 2012.