

Quantum computing impact of cybersecurity identity verification measures on WhatsApp resilient infrastructure

JosephNg Poh Soon^{1,2}, Nair Preeta², Kumar Praveen², Kok Peng Yew², Phan Koo Yuen³

¹Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University, Kuala Lumpur, Malaysia

²Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University, Kuala Lumpur, Malaysia

³Department of Computer Science, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Kampar, Malaysia

Article Info

Article history:

Received Feb 19, 2024

Revised Jun 22, 2024

Accepted Jul 3, 2024

Keywords:

Brand trust

Cybersecurity

Identity verification

Resilient infrastructure

Transaction efficiency

User perceptions

WhatsApp

ABSTRACT

This study investigates the impact and implications of implementing cybersecurity identity verification on the popular instant messaging platform, WhatsApp. Specifically, it focuses on the effects of such a measure on resilient infrastructure, user perceptions of the platform's branding and trustworthiness, and the cost-effectiveness of this approach in preventing scams, phishing, fraud, and cybercrime. Empirical data collected from a diverse group of WhatsApp users highlight that the introduction of identity verification could potentially enhance transaction efficiency, foster trust, and boost user satisfaction, particularly regarding the platform's security. However, the cost and complexity of implementation pose significant challenges. Despite these hurdles, most users perceive the potential benefits to outweigh the associated costs, pointing to a broad acceptance of such security measures. The study provides practical and theoretical contributions, offering valuable insights for managers and decision-makers at WhatsApp, as well as contributing to academic discussions on digital platform management and security. The research also underscores the societal implications of such a measure, suggesting an increase in trust in digital communication platforms and supporting safer financial transactions on social media. The integration of identity verification on WhatsApp being a responsive institution emerges as a valuable but complex endeavor, demanding careful planning to ensure maximum value creation for all stakeholders.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

JosephNg Poh Soon

Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University

Kuala Lumpur 56000, Malaysia

Email: joseph.ng@ucsiuniversity.edu.my

1. INTRODUCTION

In an era characterized by digital interconnectedness, instant messaging platforms such as WhatsApp play an increasingly pivotal role in facilitating communication for over two billion users globally as of the year 2023 in an increasing upward trend [1]. This ubiquitous utilization prompts a pressing necessity for robust identity verification measures to ensure secure and trustworthy exchanges. Although WhatsApp has made notable strides toward ensuring message encryption and privacy [1], the challenge of authentic identity verification lingers. However, with the introduction of these sophisticated identity verification technologies come potential privacy and ethical concerns that are impossible to disregard [2]. This research will therefore scrutinize these concerns, suggesting effective strategies that could mitigate these risks while

simultaneously preserving user trust and platform integrity. Lastly, achieving widespread adoption and implementation of these measures hinges on user acceptance [2]. This research will thus investigate user perceptions and attitudes toward identity verification in WhatsApp and devise strategies aimed at enhancing user acceptance and overall system adoption. In conclusion, this research embarks on a comprehensive exploration to construct a balanced framework that not only addresses technological effectiveness and privacy challenges but also considers user perceptions and acceptance, promoting a secure and trustworthy messaging environment [3].

WhatsApp, serving as a vital communication conduit for over two billion users worldwide [3], has become a target of sophisticated cybercrimes, escalating the need for robust identity verification systems. Despite the platform's reliance on phone number verification and end-to-end encryption, concerns persist about its ability to effectively deter impersonation and protect user identities. Between 2019 and 2020, there was a notable surge in the frequency of data breaches in the United States, which escalated from 1,108 instances to 1,291, marking an increase of 8%, according to a study by the Identity Theft Resource Center (ITRC). This escalation had severe implications for more than 155.8 million individuals who became victims of these breaches in 2020. Consequently, messaging platforms, including WhatsApp, have emerged as prominent conduits for such illicit activities, thereby underscoring the urgency for robust identity verification mechanisms [4]. Implementing advanced technological solutions, like passport identification artificial intelligence (AI) technology and facial recognition, could bolster WhatsApp's identity verification capabilities. However, a study by Privacy International (2022) highlights that 65% of users express concerns about data privacy and security when these technologies are mentioned. Therefore, the challenge of preserving user trust while enhancing security becomes more intricate and demands careful examination and action. Additionally, limited research into user perceptions and acceptance of advanced identity verification systems in messaging platforms presents a substantial knowledge gap. As per a report by the Center for Technology and Society (2023), understanding user attitudes is essential to achieving a 70% adoption rate, considered the baseline for effective implementation of these security measures. This study seeks to address this multifaceted problem by exploring effective technological solutions, scrutinizing potential privacy and ethical implications, and investigating user attitudes toward identity verification on WhatsApp. The aim is to provide a balanced, user-centric approach that enhances platform security and cultivates user trust, contributing to safer digital communication environments. The following is the research hypotheses as show in Figure 1.

- H1: users who have undergone identity verification on WhatsApp will experience improved efficiency in their transactions compared to users who have not undergone verification.
- H2: the implementation of identity verification on WhatsApp positively influences user perceptions of the platform's branding and trustworthiness.
- H3: the cost of implementing identity verification on WhatsApp is significantly outweighed by the reduction in scams, phishing, and fraud incidents.

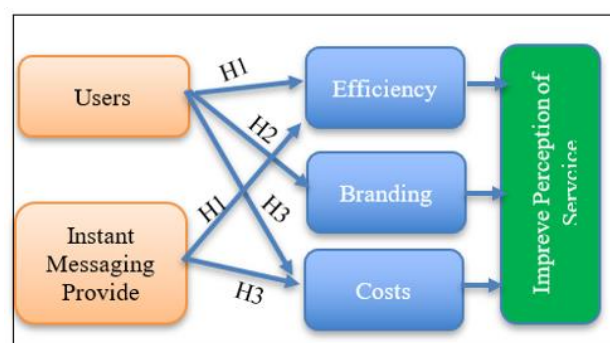


Figure 1. Research framework

2. LITERATURE REVIEW

2.1. Current operation process and technology environment

One of the most substantial shifts in the landscape of mobile and social media has been the transition from traditional texting to mobile app-based social messaging. Mobile messaging applications now rank among the most downloaded and frequently used apps globally [5]. The messaging apps that are regarded as the best and most secure include Facebook, WhatsApp, Telegram, Signal, WeChat, Skype, and Viber [6]. For

most users, Facebook and WhatsApp have become synonymous with mobile messaging. Excluding China, where WeChat holds the majority share, over 2.5 billion individuals employ these two Meta platforms for mobile messaging, accounting for 90% of the mobile messaging market share in numerous regions [7]. Tables 1 and 2 provide a summary of the security and privacy features of the messaging apps.

Table 1. Security features apps

Messaging app	End to end-to-end encryption	Encryption in transit	Private key not accessible by sp	Delete message from the server	Self destruct message	Open source	Password lock	Verification SMS/email	Two-step verification
Facebook	✓	✓			✓				
WhatsApp	✓		✓				✓	✓	
Telegram	✓	✓	✓		✓	✓	✓		
Signal	✓		✓	✓	✓		✓		
WeChat									
Skype	✓	✓							
Viber	✓		✓	✓	✓		✓		

Table 2. Reliability statistic, Cronbach alpha's score

Construct	Number of items	Cronbach alpha's score
Improved efficiency	4	0.83
Positive branding perception	4	0.79
Cost-effective reduction of scams	4	0.80

2.2. Social media integration

Social media integration (SMI) is an innovative method for verifying user identities on platforms like WhatsApp by leveraging their existing social media accounts, such as Facebook or LinkedIn [8]. This approach offers a seamless and efficient way to validate user identities through cross-referencing information from their social media profiles. In SMI, users are prompted to connect their social media accounts to their WhatsApp profiles. Firstly, it streamlines the verification process by utilizing users' existing social media accounts, eliminating the need for additional documentation or complex procedures. Secondly, it enhances the user experience by leveraging familiar platforms, reducing the friction associated with traditional identity verification methods. From a branding perspective, implementing SMI highlights a commitment to innovative and user-friendly security measures. However, SMI also faces certain limitations and challenges. Firstly, its reliability depends on the accuracy and authenticity of users' social media accounts [8]. False information or fake profiles can undermine the effectiveness of this method. Secondly, privacy concerns may arise as users may be reluctant to share their social media information due to potential misuse or unauthorized access to their data [9]. Platforms must address these concerns and implement robust privacy measures to maintain user trust.

2.3. Hybrid approach and future considerations for identity verification

While the current technology options offer improved identity verification capabilities, there is a need for a hybrid approach that combines the strengths of existing methods while integrating newer technologies. This hybrid approach can provide a more comprehensive and robust identity verification system. By leveraging the advantages of multiple technologies, such as biometrics, artificial intelligence, machine learning, and blockchain, platforms like WhatsApp can strengthen their identity verification processes and enhance user trust. In the past, identity verification on platforms like WhatsApp relied on manual methods, mobile verification, and user-provided information [10]. However, these approaches were prone to human error, manipulation, and fraud, lacking the necessary reliability and robustness. To address these limitations, advanced methods have emerged, including document submission, biometric verification, SMI, video verification, and trusted third-party verification.

3. RESEARCH METHOD

The selected research design for this study aimed to explore the impact of implementing identity verification on WhatsApp by examining users' perceptions of efficiency, branding, and cost associated with the implementation. Positivism is a philosophical school that asserts that genuine knowledge is derived from empirical evidence and logical reasoning. It rejects other forms of knowledge acquisition, such as intuition or religious faith, considering them either meaningless or unreliable [11], [12]. In this study, positivism will be

employed in the quantitative aspect, specifically using questionnaires, to examine the relationship between the implementation of identity verification on WhatsApp and the perspective in improved efficiency, positive branding perception, and cost-effective reduction of scams. Interpretivism, on the other hand, refers to a sociological research method where actions or events are analyzed based on the cultural beliefs, norms, and values of the society in which they occur [13]–[15]. It corresponds to the qualitative aspect of this study, which involves utilizing interview questions to gain a deeper understanding of participants' perspectives and experiences. This approach involved employing both quantitative and qualitative methods to collect data, thereby facilitating a comprehensive understanding of the research topic [16]–[18]. In this study, a single survey conducted through Google Forms was used, with distinct sections dedicated to quantitative and qualitative data collection. The target population for this study comprised individuals who actively use WhatsApp and may have encountered instances of scams, phishing, or fraud. The research aimed to investigate their perceptions regarding the implementation of identity verification. To ensure the validity and reliability of the survey, it underwent a validation process. A higher reliability indicates a stronger correlation between the survey results. Cronbach's alpha is a statistical test used to estimate the internal consistency or reliability of a composite score. The purpose of this test was to evaluate the reliability of the quantitative measures in the survey as shown in Table 2.

By looking at the collected data sampling result, Cronbach's alpha score will be tested with the strength of association on which alpha coefficient range would be reliable when the value is ($\alpha > 0.70$). Based on the table, the first construct of the survey, "Improved efficiency" achieved a Cronbach's alpha score of ($\alpha > 0.83$), indicating good reliability in gathering information on participants' perceived efficiency toward the implementation of identity verification on WhatsApp. The second construct, "Positive branding perception" also exhibited good reliability with a Cronbach's alpha score of ($\alpha > 0.79$). Similarly, the final construct, "Cost-effective reduction of scams" demonstrated good reliability with a Cronbach's alpha score of ($\alpha > 0.80$) in capturing participants' opinions on the perceived cost of the implementation.

4. RESULTS AND DISCUSSION

Table 3 shows the first hypothesis (H1) posits that users who have undergone identity verification on WhatsApp will experience improved efficiency in their interactions and transactions compared to users who have not undergone verification. The statistical analysis provided some support for this hypothesis. The four predictor variables used in the model (age, gender, years of experience in using WhatsApp, and education level) accounted for 39.6% of the variation in efficiency, while the adjusted R-squared value of 0.251 suggests that these variables explain approximately 25.1% of the variation in the actual population. Importantly, the p-value was 0.006, indicating a statistically significant relationship between identity verification and increased efficiency. In contrast, the second hypothesis (H2) suggested that users who have undergone identity verification on WhatsApp will perceive the platform's branding more positively and have higher levels of trust compared to users who have not undergone verification. However, the statistical analysis did not provide support for this hypothesis. The model's four predictor variables only accounted for 17.6% of the variation in the perception of branding and trust, and the p-value was 0.564, suggesting no statistically significant relationship between identity verification and users' perception of the platform's branding and trust. Lastly, the third hypothesis (H3) proposed that implementing identity verification on WhatsApp will prove cost-effective in reducing instances of scams, phishing, and fraud. However, the regression analysis did not support this hypothesis either. The four predictor variables accounted for only 26.2% of the variation in instances of scams, phishing, and fraud. The adjusted R-squared value suggested these variables explained approximately 8.4% of the variation in the actual population, and the p-value was 0.165, indicating no statistically significant relationship between identity verification and a reduction in scams, phishing, and fraud. Thus, the evidence does not suggest that identity verification implementation on WhatsApp effectively reduces these fraudulent activities.

Table 3. Results of the survey

Hypothesis	R	R ²	Adjusted R ²	RMSE	F	p-value	Conclusion
H1: improved efficiency	0.629	0.396	0.251	0.603	2.734	0.006	Significant, users with verification experience improved efficiency
H2: positive branding perception	0.419	0.176	-0.022	0.679	0.888	0.564	Not significant, no evidence of positive perception with verification
H3: cost-effective reduction of scams	0.511	0.262	0.084	0.749	1.475	0.165	Not significant, no considerable evidence that verification reduces scams cost-effectively

4.1. Quantitative data results

In Figure 2, the survey responses related to the potential implementation of identity verification on WhatsApp are presented. The x-axis represents the Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), and the y-axis indicates the number of respondents. Regarding the statement "The implementation of identity verification in WhatsApp would streamline my interactions and transactions on the platform," most respondents agreed. To be precise, 20.6% (y=13) strongly agree, 46% (y=29) agree, 25.4% (y=16) remain neutral, 6.3% (y=4) disagree, and 1.6% (y=1) strongly disagree. For the statement "I believe the addition of identity verification would make WhatsApp safer for online transactions," a sizeable portion of respondents agreed. Around 36.5% (y=23) strongly agree, and 30% (y=30) agree. Neutral responses comprised 8% (y=4) of the participants, while 6.35% (y=4) disagree, and 1.6% (y=1) strongly disagree. When asked "With the potential introduction of identity verification in WhatsApp, I would be more inclined to use the app for business or financial transactions 36.5% (y=23) strongly agree, and 30% (y=30) agree. Neutral responses comprised 8% (y=4) of the participants, while 6.35% (y=4) disagree, and 1.6% (y=1) strongly disagree. Lastly, for the statement "I feel identity verification could reduce fraudulent activity, thereby enhancing the efficiency of transactions on WhatsApp," most of the respondents concurred. About 40% (y=25) strongly agree, 47.6% (y=30) agree, 6.3% (y=4) remain neutral, 3.2% (y=2) disagree, and 3.1% (y=2) strongly disagree.

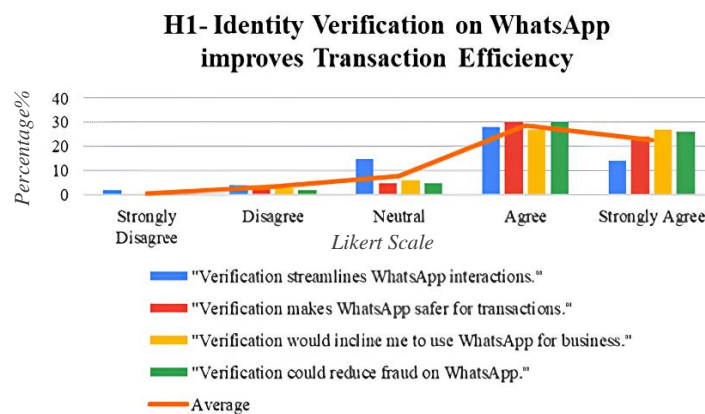


Figure 2. Chart hypothesis 1

In Figure 3, the responses to the survey about the impact of potential identity verification on WhatsApp are presented. The x-axis represents a Likert scale from 1 (strongly disagree) to 5 (strongly agree), while the y-axis represents the number of respondents. Addressing the statement "Implementing identity verification on WhatsApp will enhance the platform's reputation and trustworthiness," most respondents concurred. Specifically, 41.2% (y=26) strongly agree, 30% (y=30) agree, 8% (y=5) are neutral, and none disagree. On the statement "I believe identity verification would strengthen WhatsApp's brand as a secure and reliable platform for communication," most respondents agree or strongly agree, at 22% (y=22) and 47.6% (y=30) respectively. About 9.5% (y=6) are neutral, 6.35% (y=4) disagree, and 1.6% (y=1) strongly disagree. When asked "Given the implementation of identity verification on a different instant messaging platform, would you feel safer and thus, be more inclined to use that platform over WhatsApp," responses varied more. Around 19% (y=12) strongly agree, 35% (y=22) agree, 36.5% (y=23) are neutral, 8% (y=5) disagree, and 1.6% (y=1) strongly disagree. Finally, regarding the statement "The implementation of identity verification on WhatsApp would likely result in a decrease in my concern about scams, phishing, and fraud," most of the respondents agree or strongly agree, with 33.3% (y=20), and 41.7% (y=25) respectively. Meanwhile, 15% (y=9) of respondents remain neutral, 8.3% (y=5) disagree, and 1.7% (y=1) strongly disagree.

In Figure 4, the respondents' opinions regarding the benefits of implementing identity verification on WhatsApp and whether the benefits outweigh the associated costs are observed. The x-axis represents the Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree), while the y-axis indicates the number of respondents. Starting with the statement "Verification is cost-effective for preventing fraud on WhatsApp," most respondents agree with this statement. Specifically, 31.7% (y=20) strongly agree, 50.8% (y=32) agree, 14.3% (y=9) remain neutral, and only 1.6% (y=1) disagree or strongly disagree. Moving on to the statement "Costs of verification are justified by increased security," a considerable number of neutral responses account

for 28.6% (y=18) of respondents. However, the majority still agree with the statement, with 28.6% (y=18) strongly agreeing and 36.5% (y=23) agreeing. A small percentage, 4.8% (y=3), disagrees, and 1.6% (y=1) strongly disagrees. Regarding the statement "Could verification give WhatsApp a competitive advantage?" there is a majority agreement among the respondents. Approximately 27% (y=17) strongly agree, and 31.7% (y=20) agree with this statement. Additionally, 33.3% (y=21) remain neutral, while 6.3% (y=4) disagree and 1.6% (y=1) strongly disagree. When considering the statement "Would bear costs for verification to reduce risk on WhatsApp," the responses are more evenly distributed. Around 19% (y=12) strongly agree, 23.8% (y=15) agree, 25.4% (y=16) remain neutral, 15.9% (y=10) disagree, and 15.9% (y=10) strongly disagree.

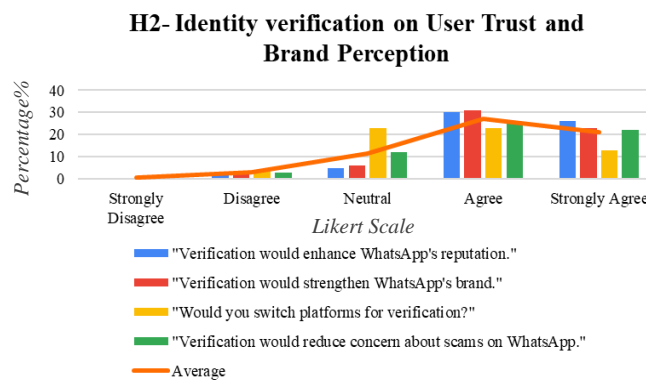


Figure 3. Chart hypothesis 2

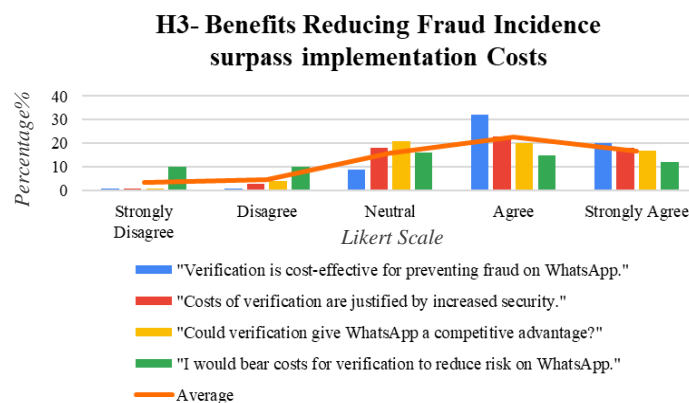


Figure 4. Chart hypothesis 3

From Figure 5, 48% of the respondents preferred to increase security and trust to improve the verification of their identity. This will help to enhance the potential adoption of WhatsApp in the future when compared to other social media applications. In potential reservations or concerns you might have about the implementation of identity verification on WhatsApp, particularly about branding and trust, the most prevalent response, held by 36% of the respondents, was that they had no reservations or concerns about the implementation of identity verification. These respondents were at ease with the notion, and some even suggested that such a feature should be implemented immediately. However, the survey revealed significant concerns regarding privacy and potential data leaks. Around 33% of the respondents voiced concerns about their data being mishandled or leaked. This indicates a substantial level of mistrust and apprehension about how WhatsApp, and its parent company Meta, handle user data. Similarly, 15% of respondents were worried about the potential misuse of their personal information as shown in Figure 6. These individuals expressed concerns about their data being used for purposes other than identity verification, such as targeted advertising or even identity theft. 12% of respondents were concerned about the complexity of the verification process. They worried that additional steps to verify their identity could introduce unnecessary hassle and complicate the user experience. There were a few unique concerns as well: one respondent was worried about identity theft by hackers, and another expressed concern about potential costs associated with the new feature.

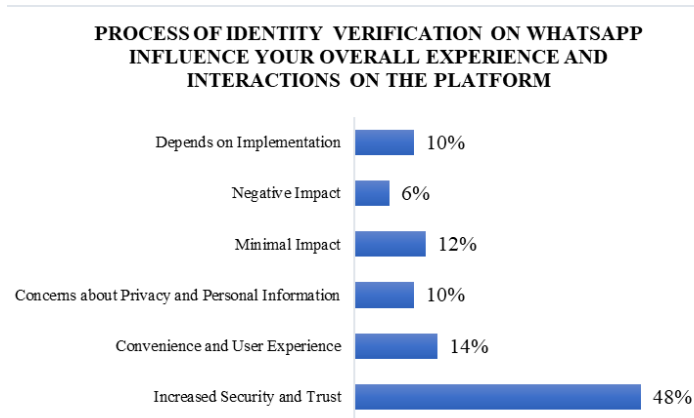


Figure 5. H1 interview results

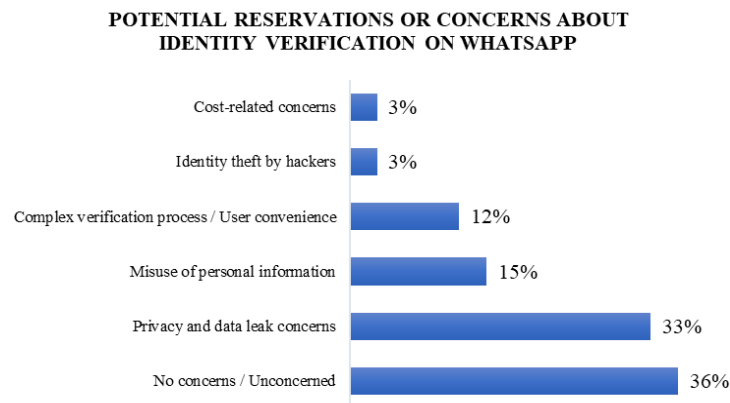


Figure 6. H2 interview results

For the costs associated with implementing ID verification, the data shows an even split between those who stated the cost would not affect their decision to use WhatsApp (34% of respondents) and those who said it could deter their usage (32% of respondents) as shown in Figure 7. This highlights a significant potential impact of introducing a cost associated with implementing an identity verification system in WhatsApp. The respondents who were unconcerned about the cost believed that the security benefits outweighed any potential financial expense. However, those deterred by the cost raised concerns about the perceived value and fairness of having to pay for a feature that they believe should be inherent to the platform's security. A smaller portion (11%) were undecided and said their decision would depend on the level of cost, indicating that there is a potential price threshold for these users. Around 18% of the responses were unclear or did not provide a clear yes or no answer 5% of the respondents believed that the cost of such a feature should be borne by the provider, demonstrating an expectation that security measures should be a part of the service provided and not an additional cost to users.

This research provides several practical contributions, primarily in enhancing the user experience on the WhatsApp platform. By demonstrating the positive impact of identity verification on transaction efficiency, the research shows the potential to boost user satisfaction, particularly for those engaging in online transactions on the platform. The sense of enhanced security from identity verification could encourage more diverse uses of the platform, such as conducting business transactions [19]–[21]. The insights provided by this study can be particularly beneficial to managers and decision-makers at WhatsApp. The findings can help inform the strategic decision to implement identity verification, demonstrating its potential value in terms of user satisfaction and transaction efficiency. It adds a new dimension to our understanding of how users perceive brand trust about security features, especially in the context of widely used communication platforms [22]–[25] like WhatsApp. Moreover, the research provides insights into the cost-benefit trade-offs involved in implementing security measures, enriching theoretical discussions in the field of digital platform management and security.

COST ASSOCIATED WITH IMPLEMENTING AN IDENTITY VERIFICATION SYSTEM IN WHATSAPP COULD POTENTIALLY AFFECT YOUR DECISION TO USE THE APPLICATION

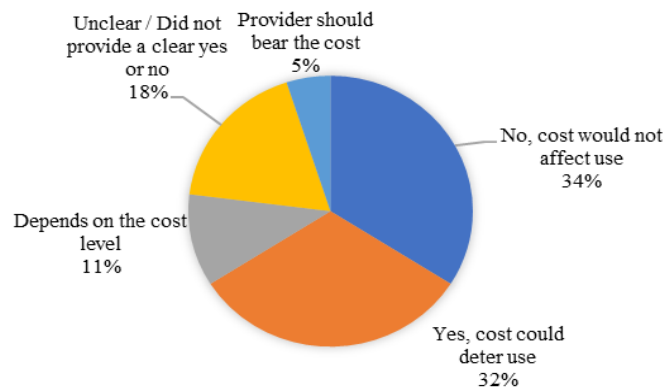


Figure 7. H3 interview results

5. CONCLUSION

This research set out to explore the implications of introducing identity verification on WhatsApp, with a particular emphasis on transaction efficiency, user perceptions of trust, and branding, as well as the cost-effectiveness of this measure in mitigating scams, phishing, and fraud. Based on the findings, it is evident that the proposed measure is generally favored by users, as it promises to enhance transaction efficiency and significantly improve the platform's security. This sense of security can enhance user satisfaction and foster a more positive perception of the brand. However, it is critical to acknowledge the challenges associated with this implementation, primarily the cost and potential complexity. The managerial implications of this research suggest that any decision to implement identity verification should be strategic, balancing the costs with the potential for reducing fraud incidence and improving user experience. This process must be made as user-friendly as possible to ensure the platform maintains its reputation for ease of use and accessibility. From a theoretical perspective, this research contributes to the growing body of knowledge regarding the role of security measures in digital communication platforms. It adds empirical evidence supporting the positive impact of such measures on transaction efficiency and user trust in a brand. Societal implications of the study are particularly salient in the current digital age, where trust in digital communication platforms is pivotal. Implementing identity verification can potentially lead to safer financial transactions on social media platforms and increase overall digital literacy by encouraging users to be more aware of security measures. The conclusion derived from this research suggests that the implementation of identity verification on WhatsApp could be a valuable step forward. Future research could delve deeper into privacy considerations associated with the implementation of identity verification, identifying strategies that can meet user needs without infringing on their privacy.





REFERENCES

- [1] L. Ceci, "Number of monthly active WhatsApp users worldwide from April 2013 to March 2020," Statista. [Online]. Available: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>
- [2] M. Karmanov, M. Putyato, and A. Makaryan, "Whatsapp messenger user data security analysis on android," in *VII International Conference "Safety Problems of Civil Engineering Critical Infrastructures" (SPCECI2021)*, 2023, p. 070014. doi: 10.1063/5.0137318.
- [3] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?," *Computer Fraud & Security*, vol. 2020, no. 9, pp. 15–19, Jan. 2020. doi: 10.1016/S1361-3723(20)30098-1.
- [4] N. Anand and I. Brass, "Responsible innovation for digital identity systems," *Data and Policy*, vol. 3, no. 1, 2021, doi: 10.1017/dap.2021.35.
- [5] S. Dechand, A. Naiakshina, A. Danilova, and M. Smith, "In encryption we don't trust: the effect of end-to-end encryption to the masses on user perception," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, Jun. 2019, pp. 401–415. doi: 10.1109/EuroSP.2019.00037.
- [6] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A deeper look into cybersecurity issues in the wake of covid-19: a survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8176–8206, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.003.
- [7] J. Botha, C. Van 't Wout, and L. Leenen, "A comparison of chat applications in terms of security and privacy," *European Conference on Information Warfare and Security, ECCWS*, vol. 2019-July, pp. 55–62, 2019.





- [8] J. A. Hall, "What we do in the shadows: the consumption of mobile messaging by social media mobile apps in the twilight of the social networking era," *Mobile Media & Communication*, vol. 11, no. 1, pp. 66–73, Jan. 2023, doi: 10.1177/20501579221133610.
- [9] Y. S. Park, L. Konge, and A. R. Artino, "The positivism paradigm of research," *Academic Medicine*, vol. 95, no. 5, pp. 690–694, May 2020, doi: 10.1097/ACM.0000000000003093.
- [10] H. H. Alharahsheh and A. Pius, "A review of key paradigms: positivism vs interpretivism," *Global Academic Journal of Humanities and Social Sciences*, vol. 2, no. 3, pp. 39–43, 2020, doi: 10.36348/gajhss.2020.v02i03.001.
- [11] K. Subaramaniam, R. Kolandaisamy, A. Bin Jalil, and I. Kolandaisamy, "Cyberbullying challenges on society: a review," *Journal of Positive School Psychology*, vol. 6, no. 2, pp. 2174–2184, 2022.
- [12] A. Firdaus, G. S. AlDharhani, Z. Ismail, and M. F. Ab Razak, "The summer heat of cryptojacking season: detecting cryptojacking using heatmap and fuzzy," in *2022 International Conference on Cyber Resilience (ICCR)*, IEEE, Oct. 2022, pp. 1–5. doi: 10.1109/ICCR56254.2022.9995891.
- [13] P. S. JosephNg, "Hotel room access control: an NFC approach ecotourism framework," *Journal of Science and Technology Policy Management*, vol. 15, no. 3, pp. 530–551, Apr. 2024, doi: 10.1108/JSTPM-10-2021-0153.
- [14] M. Huang and F. K. Chong, "Empowering travelers with airfare comparison, flight tracking, and real-time weather forecasts on android," in *2023 IEEE 11th Conference on Systems, Process & Control (ICSPC)*, IEEE, Dec. 2023, pp. 7–12. doi: 10.1109/ICSPC59664.2023.10420178.
- [15] G. S. Al-Dharhani, Z. A. Othman, and A. A. Bakar, "A graph-based ant colony optimization for association rule mining," *Arabian Journal for Science and Engineering*, vol. 39, no. 6, pp. 4651–4665, Jun. 2014, doi: 10.1007/s13369-014-1096-5.
- [16] P. S. JosephNg, "EaaS optimization: available yet hidden information technology infrastructure inside medium size enterprise," *Technological Forecasting and Social Change*, vol. 132, pp. 165–173, Jul. 2018, doi: 10.1016/j.techfore.2018.01.030.
- [17] T. Nandy, R. Md Noor, R. Kolandaisamy, M. Y. I. Idris, and S. Bhattacharyya, "A review of security attacks and intrusion detection in the vehicular networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, p. 101945, Feb. 2024, doi: 10.1016/j.jksuci.2024.101945.
- [18] T. Nandy *et al.*, "A secure, privacy-preserving, and lightweight authentication scheme for vanets," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20998–21011, Sep. 2021, doi: 10.1109/JSEN.2021.3097172.
- [19] P. Hayashi, G. Abib, and N. Hoppen, "Validity in qualitative research: a processual approach," *Qualitative Report*, vol. 24, no. 1, pp. 98–112, Jan. 2019, doi: 10.46743/2160-3715/2019.3443.
- [20] A. F. Hayes and J. J. Couffts, "Use omega rather than Cronbach's alpha for estimating reliability. but...", *Communication Methods and Measures*, vol. 14, no. 1, pp. 1–24, Jan. 2020, doi: 10.1080/19312458.2020.1718629.
- [21] J. Barbera, N. Naibert, R. Komperda, and T. C. Pentecost, "Clarity on Cronbach's alpha use," *Journal of Chemical Education*, vol. 98, no. 2, pp. 257–258, Feb. 2021, doi: 10.1021/acs.jchemed.0c00183.
- [22] S. J. Stratton, "Population research: convenience sampling strategies," *Prehospital and Disaster Medicine*, vol. 36, no. 4, pp. 373–374, Aug. 2021, doi: 10.1017/S1049023X21000649.
- [23] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy, "The online survey as a qualitative research tool," *International Journal of Social Research Methodology*, vol. 24, no. 6, pp. 641–654, Nov. 2021, doi: 10.1080/13645579.2020.1805550.
- [24] H. Wang and J. Zhang, "Blockchain based data integrity verification for large-scale IoT data," *IEEE Access*, vol. 7, pp. 164996–165006, 2019, doi: 10.1109/ACCESS.2019.2952635.
- [25] N. K. Lung, C. P. Lin, and D. A. Dewi, "Designing a research model for depression tendency detection using facial expression recognition," *Journal of Engineering Science and Technology*, vol. 19, no. 2, pp. 163–172, 2024.

BIOGRAPHIES OF AUTHORS







Prof. Ts. Dr. JosephNg Poh Soon     is Professor in Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University, Malaysia. Graduated with a PhDIT., Master in Information Technology (Aus), Master in Business Administration (Aus), and Associate Chartered Secretary (UK) with various instructor qualifications, professional certifications, and industry memberships. Listed numerous times as the World's Top 2% scientist in artificial intelligence and image processing by Stanford University, USA, and with his blended technocrat mix of both business senses and technical skills, has held many multinational corporation senior management positions, global posting and leads numerous 24x7 global mission-critical systems. He can be contacted at email: joseph.ng@ucsiuniversity.edu.my.







Nair Preeta     currently serves as a Senior Project Manager with DHL. She also holds the position of Vice President at Project Management Institute (PMI) Malaysia. With a wealth of experience, she has previously worked as a Project Engineer at Philip Morris and Mondelez, held roles in Weir Minerals both in Malaysia and the UK, and served as a Senior Project Manager at UEM Edgenta. Preeta's academic credentials include a Bachelor's in Industrial Chemistry, a Master's in Engineering Management, and a Master's in Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University, Malaysia. Additionally, she holds numerous certifications in project management, Lean Six Sigma, and various AI-related fields and low-code development platforms certificates. She can be contacted at email: i23024063@student.newinti.edu.my.







Kumar Praveen     currently working as a Software development manager at AMS OSRAM. He has 12 years of experience in Software Development specifically SAP ERP area. He completed his Bachelor's from Andhra University, India, and a Master's in Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University, Malaysia. On a personal side, he loves to explore the outdoors, camping, and road trips together with his family. He can be contacted at email: kumarchitturi@gmail.com.



Kok Peng Yew     graduated with a Bachelor of Information Technology (Honours) in Software Systems Development from TARUMT and is currently in the final semester of a Master in Department of Network and Security, Faculty of Data Science and Information Technology, INTI International University, Malaysia. With over two years of experience in visual inspections and artificial intelligence, he works in the manufacturing industry as an MLOps CoE. In this role, he leads and delivers AI solutions that integrate with various vendors to enhance production floors and has recently taken on project management responsibilities to oversee AI projects related to visual inspection AI solutions. He can be contacted at email: kokpeng5149@gmail.com.



Asst Prof. Ts. Dr. Phan Koo Yuen     graduated with a Ph.D. in Business Information Technology (Malaysia) and an M.Sc. in Information Studies (Singapore). He is currently working at Department of Computer Science, Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia as a computer science assistant professor. His research interests focus on the domains of information systems, information technology, business intelligence success, and firm performance. He can be contacted at email: phanky@utar.edu.my.