PREDICTING DATA LEAK RISK FROM SMARTPHONE DEPENDENCY, DIGITAL MEMORY AND USAGE PATTERNS

ALI, A.[1*] – NUJI, M. N. N.[1] – ONG, M. H. A.[2] – SALLEH, M. A. M.[3]

[1] *Faculty of Communication and Media Studies, Universiti Teknologi MARA (UiTM), Selangor, Malaysia.*

[2] *Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) Johor Branch, Johor, Makaysia.*

[3] *Faculty of Social Sciences and Humanities, Universiti Kebangsaan Malaysia, Selangor, Malaysia.*

**Corresponding author*
e-mail: anuar0688[at]uitm.edu.my

(Received 18th June 2025; revised 20th August 2025; accepted 28th August 2025)

Abstract. Smartphone is no longer limited to communication purposes but has evolved into a digital tool for managing work, learning, and daily social activities. This influence has implications for smartphone dependency and the formation of digital memory. However, heavy dependency, reliance on digital memory, and unsafe usage habits increase the risk of data leaks. Despite rising concerns over data privacy, many users especially young adults continue to underestimate how their smartphone dependence, digital memory practices, and usage pattern contribute to potential data leakages. Therefore, this study examines the relationship between smartphone dependency, digital memory, usage patterns and data leak risk among young adults in Malaysia. Using Partial Least Squares Structural Equation Modelling (PLS-SEM) on 353 valid responses, the findings reveal significant positive relationships between smartphone dependency ($\beta = 0.449$), digital memory ($\beta = 0.245$), and usage patterns ($\beta = 0.235$) with data leak risks, explaining 78.5% of the variance. These findings indicate that excessive smartphone dependency, increasing reliance on digital memory, and risky usage behaviors significantly contribute to users' digital vulnerability. This highlights the urgent need for digital literacy to reduce the risk of personal data leaks aimed at building a more informed and digitally responsible society.
Keywords: *smartphone dependency, digital memory, usage pattern, data leak, structural equation modelling*

Introduction

After going through several eras, the world today is facing rapid progress due to the existence of various information and digital communication technologies. The transition from the industrial age to the information technology age not only provides opportunities for active user engagement with machines but also cultivates the concept of a networked society (Castells, 2023). Meanwhile, the process of transitioning from the information technology era to the post-digital era has witnessed society to the adaption use of technology in daily life (Berry, 2024). In Malaysia, the use of communication technology such as smartphones are very common among every group of society to the extent that almost one hundred percent of Malaysians own smartphones (Chellapan et al., 2024). This issue of technology adaptation is in line with McLuhan (1975) early prediction that humans will always need technology to manage their daily lives. It turns out that, in the context of smartphones, their use is very important as a mobile communication tool that helps bring users' geographical positions closer to continue to actively connect with each other (Goggin, 2021). The transition of modern

age also witnessed the development of smartphones in 2020, which were accompanied by 5G cellular network services. This network also made smartphones smarter in providing experiences to individual users in the form of augmented reality (AR) and virtual reality (VR). This intelligence is also able to imitate the capabilities of the human brain and human behavioral patterns through artificial intelligence (AI) technology (Goggin, 2025). The implications of this phenomenon have caused smartphones to undergo a transformation process from mere communication tools to communication tools capable of digitizing data, information and human memory (Niu et al., 2022). This digitization process has caused human memory to be channeled from the human body to smartphones. Through the concept of digital memory, Reading (2009) conceptualised that smartphones are used as a form of digital diary by users to record and manage every activity of daily life. Anderson Zorn (2021) supports this statement by stating that features such as storage space capacity, cameras and high-resolution screens are factors that make smartphones the main digital diary for individual users, especially youth.

In addition, Internet connectivity also encourages the process of digitizing data, information and memory to occur faster. Internet connectivity has provided smartphones with the opportunity to stay always connected to cloud storage technology. This advantage has made the process of transferring, accessing and editing digital data and information possible at any time (Li et al., 2021). This process of digitizing data and information also does not only occur between smartphones and cloud storage. In fact, the Internet connectivity that occurs all the time also encourages the sharing of various digital content uploaded on social media such as Facebook, Instagram, Twitter and Pinterest. However, most existing mobile applications and digital communication technology platforms do not explain the guidelines on the data sharing policy uploaded by each individual user. Flew and Gillett (2021) emphasizes that the policy on the privacy risks of data sharing in cyberspace outlined by technology providers such as Facebook, Instagram and Google should be used as a guide by all technology providers. The sincerity through this service policy includes the right of users to know how their data is managed and where the data is located. This service policy is important in outlining the rights of users and technology providers regarding any matter involving the management and control of individual user data. Today's reality shows that the guidelines and service policies provided by a few technology providers are less clear in terms of the management and use of individual user data (Gawer and Srnicek, 2021). Similarly, Saritepeci et al. (2024) emphasizes that this situation occurs due to the attitude of a few individual users who underestimate the importance of the service policy provided by communication technology providers. Users only care about the services offered and are careless about the importance of the service policy. This happens because most individual users do not realize that the data and digital information they share has its own value.

This phenomenon contributes to online security issues such as cybercrime, leaks and theft of user data occur worldwide. In Malaysia, Berita Harian in 2021 reported that cases of theft of personal data in digital form were increasingly prevalent from 2017 to 2020. Attempts to trade telecommunications data through the Lowyat.net portal forum in 2017 proved that the digital data had valuable value to the point of being traded for commercial purposes. Despite the security features through the Public Cellular Service Blocking (PCBS) launched by MCMC in early 2014, a total of 46.2 million data sets were leaked in 2019 with the number of data leaks exceeding the population of

Malaysia. In particular, the PCBS initiative aims to block any services from a lost or stolen smartphone even if the Subscriber Identity Module (SIM) card is changed to a new owner. Although digital security has gained prominence in academic and public discourse, there is limited empirical focus on how behavioral factors such as smartphone dependency, digital memory practices, and usage patterns intersect to predict data leak risk. More importantly, users often fail to perceive these behavioral elements as interconnected contributors to digital vulnerability. Despite the growing awareness of data privacy, the everyday behaviors that increase exposure are frequently underestimated or ignored. This disconnect between awareness and behavior forms a critical gap in understanding modern digital risk. Therefore, this study adopts a structural equation modelling (SEM) approach to examine the predictive relationships between smartphone dependency, digital memory, and usage patterns in relation to the risk of data leaks. By empirically analyzing how these variables interact, the study aims to provide a comprehensive framework for understanding behavioral contributions to digital vulnerability. Findings from this research can form digital literacy campaigns, smartphone usage guidelines, and cybersecurity interventions, ultimately encouraging users to adopt safer digital habits and reduce their exposure to data-related threats.

Literature review

Smartphone dependency

Dependence on the use of smartphones occurs when its function has developed into a tool for digitizing data, information and memory of individual users, especially among youth. Smartphone dependence in this context is capable of having a lasting negative impact on the ability of individual users in terms of memory and mental strength (Linden et al., 2021). Similarly, previous study found that the function of smartphone as a digital memory tool is capable of reducing the short-term memory capacity of individual users, especially youth. In this regard, the phenomenon of smartphone dependence needs to be examined in depth to understand the purpose of its use and subsequently be able to unravel how data digitization occurs. To explore this issue, exploration needs to begin by understanding the dimensional differences between the terms of smartphone dependence and smartphone addiction. This is due to the overlapping definitions between these two concepts, which has led to confusion in views on this phenomenon. Most past studies involve analysis of smartphone dependence, which is closely related to the fields of communication and media. Meanwhile, studies that involve exploring smartphone addiction usually have a relationship with the fields of psychology and health. Kim (2020) refers to smartphone addiction as the active use of a user's smartphone to meet the needs of daily life. Guided by the Media System Dependency Theory by Ball-Rokeach (2008) the needs of daily life refer as goals that individual users want to achieve. These goals include the goal of understanding a situation, the goal of establishing communication relationships with other individuals, and the goal of satisfying the desire for entertainment (Ball-Rokeach, 2008). Looking at the importance of this issue in society, several researchers around the world have studied various goals of smartphone addiction. Instruments such as the Persian Version Test of Mobile Phone Dependency (TMD) have also been successfully created to measure the level of dependence of individual users on this communication tool (Vezzoli et al., 2023).

Digital memory and cognitive offloading

The transition of the times transformed the development of smartphones in 2020, which were accompanied by 5G cellular network services. This network also made smartphones smarter by being able to provide experiences to individual users in the form of augmented reality (AR) and virtual reality (VR). This intelligence is also able to imitate the capabilities of the human brain and human behavioral patterns through artificial intelligence (AI) technology (Tehlan et al., 2021). Specifically, the role of humans in remembering things is argued to have been taken over by smartphones. The transfer of human burden to this technology is so significant that smartphones are said to be able to replace part of the functions of the human brain. This is due to the ability of smartphones to process and store information quickly at any one time. The discussion on the transformation of smartphones in the previous description clearly proves that communication technology has a very important relationship with society. Technology and humans as entities that cannot be separated as two separate entities. This is because technology and humans actively interact. This thinking is in line with Irwin (2021) argument on the definition of technology through the concept of 'technical being'. This concept means technology as a being that does not have an end in itself and will only be active as an instrument that is moved by humans for a purpose. Vaterlaus et al. (2021) stated that smartphones are not just passive instruments, its ability to take over human intelligence through the digitization of data and memory. Smartphones are able to function like the human brain in terms of remembering, storing and managing information (Reading, 2009). In the context of digital memory, smartphones are used as a tool for digitizing data, information and memories such as personal photos, personal videos, family photos, educational materials and job information (Reading, 2009). In fact, a few individual users of the iPhone smartphone brand are also able to record information related to their health when this brand company began introducing health application services that have been installed since the iOS8 operating system was launched (Van Zandwijk and Boztas, 2021). This application can collect information such as nutrition, blood type and heart rate monitoring. This user data, information and memory are recorded through the camera function, sophisticated databases and algorithms integrated into smartphone technology. Indirectly, the process of digitizing memory occurs using smartphones as digital memory storage devices in the 21st century (Calinescu, 2024). This situation supports the suggestion by Reading (2009) about the ability of smartphones to be used not only to record events and memories, but also to share these recordings with other users. This sharing is often done all the time and at any time through social networking platforms such as Facebook, Twitter and Instagram which are accessed using smartphones. Spath et al. (2023) argue that Internet connectivity has caused this process of digitization, documentation and sharing of data to occur anywhere with its use at any time. Internet connectivity with smartphones has made it the most important wireless technology that allows the world's society to be fully connected (Spath et al., 2023).

Smartphone usage patterns and risky behaviors

Smartphone usage patterns which include how often, where, and for what purposes these devices are used for, have a significant impact on user vulnerability. Usage habits often shape the likelihood of security missteps. Lotfy et al. (2021) highlighted that frequent users are more likely to connect to public Wi-Fi networks, leave devices

unlocked, or use convenience features such as autofill for passwords and unencrypted storage. This perspective is also in line with Reading (2009) argument on the ability of smartphones to be used anytime and anywhere. Looking at the features offered by smartphone technology providers, this technology is not limited to communication purposes alone. This technology has undergone further transformation when its sophistication that combines the roles of laptops, social media and the Internet is able to support the formation of global relationships to occur anytime and anywhere. For example, the sophistication of smartphone communication technology today allows youth to connect through various online social activities. This continuous use includes activities of updating social media accounts, finding new contacts and expanding networks through various social networks. Next, the role of smartphones in supporting mobile computing functions has also attracted attention. Its ability to provide real-time information such as time, weather forecast, latest news and directions has led young people to continue to rely on its use (Kehtarnavaz et al., 2022). This advantage also provides opportunities for individual users, especially young people, to access the digital information space quickly. The contradiction was seen in the 19th century, when emphasized that society at that time experienced a lack of information due to the limitations of existing media in information dissemination activities. However, with the help of communication technologies such as smartphones, various digital data and information can be shared easily and quickly around the world (Miller et al., 2021). At the same time, the sophistication of smartphone operating systems also allows individual users to continue to access, edit and store digital content easily. Google purchased an operating system called Android in 2005 to support web browsing and information search activities via smartphones (Goel and Singal, 2021). This success was continued by Apple when it successfully introduced mobile technologies such as the iPod and iPad in 2007 which fully supported the use of the iOS operating system for the purpose of accessing information. This success has caused individual users, who are also represented by the youth group, to continue to rely on smartphones for information search activities. Previous study also emphasized that the existence of search engines such as Google that are able to function via smartphones has encouraged activities to access news, magazines and search for various other information online (Leith, 2021).

The risk of data leaks

This phenomenon of smartphone dependency and digital memory contribute to online security issues such as cybercrime, leaks and theft of user data occur worldwide. Data leak risks emerge not only from external cyberattacks but also from internal behavioral vulnerabilities (Zhang et al., 2023). Many users are unaware of how their actions contribute to metadata collection and profiling, especially by commercial apps that monetize user data. Even when no direct data leak occurs, the aggregation of behavioral patterns and personal information across multiple platforms can create vulnerabilities in the broader digital ecosystem (Greshake et al., 2023). The sense of control that users feel over their data is often illusory, masked by complex settings and the opaque nature of data brokerage systems. Importantly, many data leaks are not caused by malicious intent but by complacency or misinformation (Lee, 2024). Users may assume that default privacy settings are sufficient, or that biometric locks offer full protection. This gap between perceived and actual security practices reveals the need for more targeted digital literacy efforts, especially among heavy smartphone users. For example, the hacking incident of Miami-based technology firm Kaseya has witnessed a

large-scale theft of customer data. A report released by Utusan Malaysia in 2021 stated that this hacking group also demanded a payment of RM291 million to restore the captured data. Skatova et al. (2023) argue on the importance of individual users' digital data and information is indeed valuable and needs to be protected as well. However, Birch et al. (2021) emphasized that the definition of digital data and information initially seemed simple, but this definition has become increasingly complicated as today's digital communication world is experiencing an increase in the types of digital data and information, forming a concept classified as big data. Shukla et al. (2022) shows the growth of online business activities globally with a positive increase in market size every year. In addition, bill payment systems are also introduced through online banking activities to help users manage their daily lives (Chauhan et al., 2022). Smartphone users also have registered accounts such as Shopee, Lazada, and several other fixed accounts to subscribe to goods they want to buy online (Koswara, 2025). However, challenges that can be seen include the level of security and the level of user satisfaction with online financial services. According Ariffin et al. (2021), security issues often occur through the sharing of financial information belonging to individual users during online buying and selling transactions between users and business operators. A report by Berita Harian in 2015 stated that most Maybank users in Malaysia also expressed dissatisfaction with the issue of Maybank2u service disruptions that often occur due to system maintenance activities.

Materials and Methods

A combination of quantitative analysis and cross-sectional research methodologies were used, since both methodologies can be considered as sufficient methods to investigate and measure the proposed research hypothesis (Creswell and Creswell, 2017). The data were collected using the structured and close-ended questionnaire, which is consists of 24 items and each question used a 5-likert scale scaling ranging from 1 as Strongly Disagree to 5 as Strongly Agree. A total of 450 responses were collected from young adults using convenience sampling in the Klang Valley. Out of these, 353 completed the questionnaire in full, yielding a response rate of 78.4%.Structural Equation Modelling analysis was used in this research by using a Partial Least Square (i.e. PLS-SEM) due to the nature of this research can be considered as an exploratory study since the researcher intend to explore the effect of selected independent variables toward dependent variable (Hair et al., 2019). Besides that, this method is suitable for this study since it can testing the convergent and discriminant validities of the indicators measuring the targeted variables (Hair et al., 2019), hence it can ensure the validities of the model. In addition, since PLS-SEM estimation technique used the bootstrapping methodology for testing the hypothesis, the results of this analysis can be considered sufficient enough because this method make a free assumption of the data distribution (Hair et al., 2017). *Figure 1* shows the proposed theoretical framework for this study based on the previous explained literature review. There consists four variables which is three variables (i.e. Dependency, Memory, and Pattern Usage) served as the independent variables, whereas Data Leak can be described as the dependent variable.

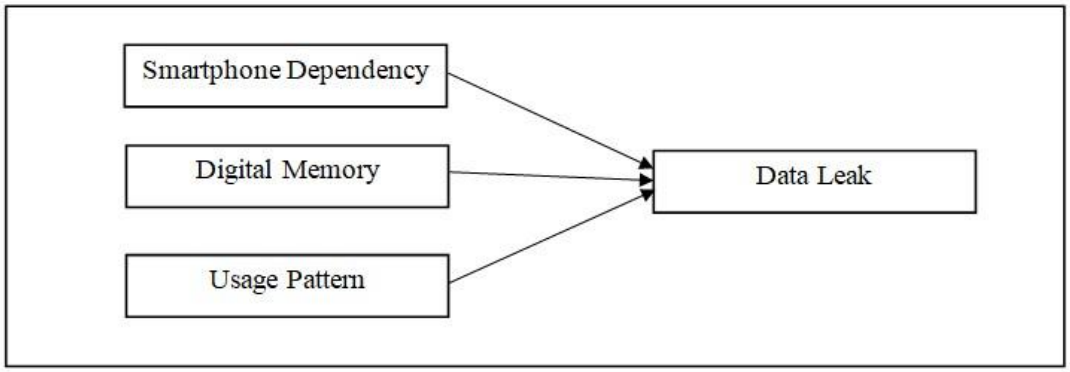

Figure 1. *Theoretical framework.*

Results and Discussion

Measurement model

Table 1 indicated that, all indicators for measuring targeted variables meet the minimum requirement of .70 factor loading value and were significant load to their own variable for at least 95% confidence interval (Hair Jr et al., 2017). Besides that, all indicators do not suffers from the extremely non-normal distribution as well as extreme outliers since the Skewness (Range: -0.541 to 0.342) and Kurtosis (Range: -0.487 to 0.367) statistics within the ± 1.00. On the other hand, the Average Variance Explain (i.e. AVE) for each variable was above .50, as well as both reliability assessments (i.e. Cronbachs Alpha and Composite Reliability) were above .70, hence if confirms that all indicators for measuring the targeted variable have meet a good unidimensionality and convergent validity assessments. As for discriminant validity of the model, *Table 2* indicated that the model meets the requirement of discriminant validity since each latent variable produce less than .90 of the HTMT ratio value (Henseler et al., 2015). Therefore, it can barely conclude that, the indicators that were used to measured targeted construct were totally used for the respectively construct.

Table 1*. Convergent validity for measurement model.*

Indicator	Loading	AVE	γ	α
Dependency		.676	.926	.904
DEP1	.854*			
DEP2	.844*			
DEP3	.807*			
DEP4	.776*			
DEP5	.831*			
DEP6	.818*			
Memory		.668	.923	.899
MEM1	.731*			
MEM2	.820*			
MEM3	.858*			
MEM4	.887*			
MEM5	.809*			
MEM6	.788*			
Pattern Usage		.660	.921	.896
PAT1	.750*			
PAT2	.834*			

PAT3	.833*			
PAT4	.861*			
PAT5	.833*			
PAT6	.758*			
Data Leak		.660	.921	.896
DAT1	.801*			
DAT2	.857*			
DAT3	.808*			
DAT4	.836*			
DAT5	.787*			
DAT6	.812*			

*Note: AVE=Average Variance Explained; γ=Composite Reliability; α=Cronbach's Alpha; *p<.05.*

***Table 2**. HTMT discriminant analysis for measurement model.*

Category	Dependency	Memory	Pattern Usage	Data Leak
Dependency				
Memory	.850			
Pattern Usage	.848	.838		
Data Leak	.846	.818	.828	

Structural model

The analysis indicated that, about 78.5% (R2 = .785) of the variance explained were able explained by Dependency, Memory, and Pattern Usage independent variables toward Data Leak. Besides that, the effect size (i.e. f2) as well as predictive relevance (i.e. q2) for each path coefficient can be considered from medium to small effect (Hair et al., 2019). *Table 3* also indicated that, Dependency (β = 0.449, t = 5.526, 95% BCa CI: (0.301, 0.614)), Memory (β = 0.245, t = 2.800, 95% BCa CI: (0.071, 0.411)), as well as Pattern Usage (β = 0.235, t = 3.078, 95% BCa CI: (0.067, 0.378)) give a positive significant effect toward the Data Leak. Hence, it is indicated that, if the average level of Dependency. Memory, and Pattern Usage increase simultaneously, the probability that Data Leak is likely to increase. *Figure 2* and *Figure 3* shows the analysis of PLS-SEM.

***Table 3**. Structural model assessment.*

Path	β	t-statistic	95% BCa Bootstrap	f^2	q^2
DEP → DAT	0.449	5.526*	(0.301, 0.614)	.195	.157
MEM → DAT	0.245	2.800*	(0.071, 0.411)	.108	.087
PAT → DAT	0.235	3.078*	(0.067, 0.378)	.085	.073

*Note: DEP=Dependency; MEM=Memory; PAT=Pattern Usage; DAT=Data Leak; β=Standardized Beta Coefficient; f^2=Effect Size; q^2=Predictive Relevance; [a]The bootstrap samples was 5000 samples; *p <.05.*

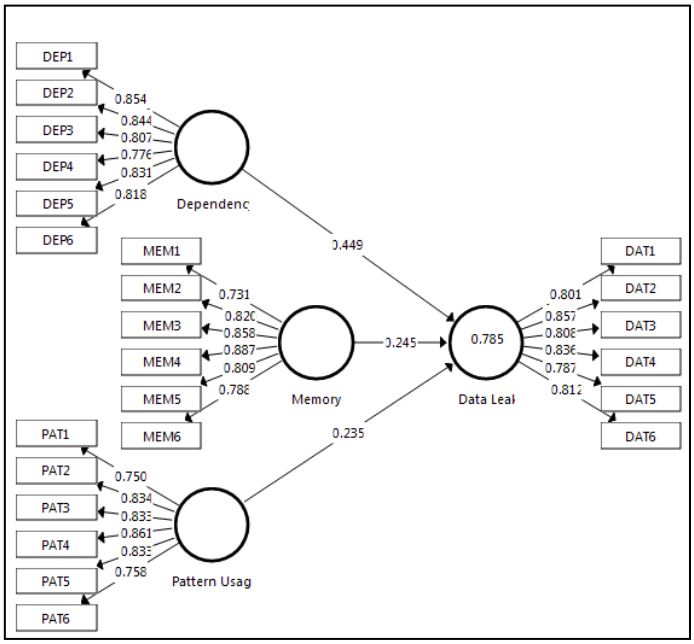

Figure 2. *Loading assessment.*

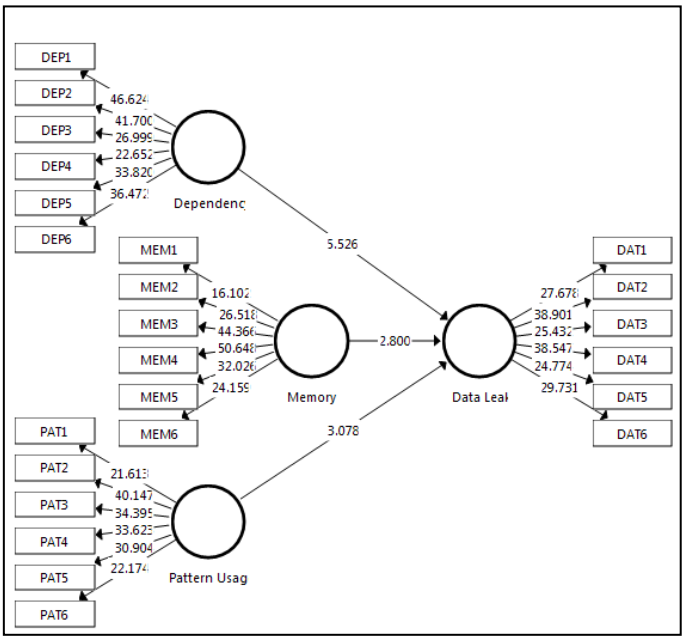

Figure 3. *Bootstrapping assessment.*

Overview of the structural model

The structural model in this study reveals a strong predictive capability, with an R^2 value of 0.785. This finding indicates that smartphone dependency, digital memory reliance, and specific usage patterns collectively account for a substantial proportion of the variance in data leak vulnerability. This level of exploratory highlights that user behavior is a dominant factor in digital exposure which possibly surpassing the importance of traditional cybersecurity measures like encryption, firewalls, and antivirus software. This redirection of focus from purely technological safeguards to behavioral dimensions of smartphone usage offers a significant research argument

which the digital security must be reframed as a human-centered issue rather than merely a technical one. This aligns with recent literature that critiques the overemphasis on hardware and software defenses without adequately considering how everyday user behaviors introduce risks (Kim, 2020). The implication here is that digital literacy and behavioral interventions could be more effective in reducing vulnerability than simply improving security protocols. For instance, campaigns emphasizing secure behavior patterns which like regularly updating apps, using secure passwords, or reducing unnecessary permissions. This situation could significantly reduce leak risks when widely adopted.

Smartphone dependency as a primary contributor

Among the model's variables, smartphone dependency exhibits the strongest influence on data leak vulnerability ($\beta = 0.449$). This supports the research argument that behavioral overdependence on smartphones diminishes users' cognitive control and critical engagement with digital security. Such dependency often leads to compulsive phone checking, reduced attention span, and habitual interaction with apps without thorough security scrutiny. Li et al. (2021) proved that smartphone dependence has both positive and negative implications among youth. According to them, the dependence that benefits youth is for learning purposes. While the negative implications include excessive Internet dependence and social networking. Anderson Zorn (2021) argued that the function of smartphones as a digitalization tool is related to the phenomenon of dependence among youth. This dependence exists when smartphones support various types of digital communication such as social interactive technology, online gaming applications, social applications and others.

The role of digital memory in cognitive offloading

Harkin and Kuss (2021) argued that smartphones are a communication tool that represents the self of an individual user. Their criticism refers to the situation that smartphones reflect a user. This personality can be translated through digital identities created by using smartphones. The identity construction is through digitization of user data and information stored in the smartphone's memory chip or card (Reading, 2009). This digital data and information can be used as evidence to detect the identity of a user by digital forensics practitioners. Meanwhile, Miller et al. (2021) also agreed that personal personality is formed through digital communication activities that are repeatedly carried out through smartphones. The repetition of these communication activities can translate a user's personality, interests, communication skills and social style. These findings prove that smartphone usage patterns can translate a user's personality, which includes human attitudes and personalities.

Data risk embedded in usage patterns

Usage patterns, while slightly less impactful ($\beta=0.235$), remain a meaningful predictor of data leak risk. This includes behavioral routines such as frequent multitasking, excessive app downloads, blind acceptance of terms and conditions, and engaging with unknown links or third-party services. These everyday behaviors, while seemingly harmless, incrementally increase the surface area for digital vulnerabilities. Youth also do not care about the security aspects of data and digital information, especially when using communication channels such as smartphones and social media.

This refers to their excitement in using the services offered for the purpose of entertainment, socialization and continuous online communication. However, according to Adnan et al. (2025), they do not practice cybersecurity, especially in terms of understanding the policies and guidelines set by technology providers as well as matters related to cyber law. Despite the existence of various related laws such as the Computer Crime Act 1997, the Electronic Commerce Act 2006, the Personal Data Protection Act 2010, the Consumer Protection Act 1999 and the Communications and Multimedia Act 1998, awareness of the importance of digital content management is still at a low level. Users do not feel that these laws are important as protection against online data and privacy threats (Adnan et al., 2025). They also stated that the knowledge factor is closely related to awareness of digital data management among users, especially youth. Therefore, it is proven that important knowledge about the importance of digital assets is needed to create high awareness among youth.

Conclusion

The simultaneous presence of high dependency, strong digital memory reliance, and poor usage patterns creates a compound risk environment, not just an additive one. This combination forms a behavioral ecosystem in which one factor reinforces the others. For example, dependency increases usage frequency, which encourages memory offloading, further increasing exposure. Such interactions suggest that a single behavioral intervention may not suffice. Comprehensive strategies that address the interplay between multiple habits are required to effectively reduce leak risks. The continuous dependence on smartphone usage has caused the users to produce various digital content. This digital content includes data, information and memory that has valuable value. Apart from digital content, various digital platforms are also registered including social media platforms, blogs, financial platforms and buying and selling platforms. Most individual users, especially the youth, are not aware of the importance of the data, information, memory and digital platforms that have been formed as very valuable assets. Indeed, this study extends the application of behavioral cognitive frameworks in cybersecurity by empirically proving that non-technical human factors, like digital memory habits and dependency, can predict security risks. It challenges the dominant technology-centered discourse by showing that user psychology is not just a background concern but a central risk domain. This study provides general awareness to users, especially the youth, about relationships between smartphone dependency, digital memory, and usage patterns in relation to the risk of data leaks Communication technologies such as smartphones not only challenge the active involvement of users, but their sophistication also leads to questions about the management of digital data and memory.

Acknowledgement

This study was self-funded. The authors wish to express their gratitude to Universiti Teknologi MARA (UiTM) for institutional support, and to all participants who generously contributed their time to complete the survey.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Adnan, M., Syed, M.H., Anjum, A., Rehman, S. (2025): A framework for privacy-preserving in IoV using federated learning with differential privacy. – IEEE Access 13: 1-12.
[2] Anderson Zorn, A.K. (2021): Portable archives: Using mobile technology for archival education and outreach in a campus community. – Archival Issues 41(1): 23-35.
[3] Ariffin, S.K., Abd Rahman, M.F.R., Muhammad, A.M., Zhang, Q. (2021): Understanding the consumer's intention to use the e-wallet services. – Spanish Journal of Marketing-ESIC 25(3): 446-461.
[4] Ball-Rokeach, S.J. (2008): Media system dependency theory. – The International Encyclopedia of Communication 4p.
[5] Berry, D.M. (2024): Post-digital humanities: Computation and cultural critique in the arts and humanities. – ArXiv Preprint 3p.
[6] Birch, K., Cochrane, D.T., Ward, C. (2021): Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. – Big Data & Society 8(1): 1-14.
[7] Calinescu, A. (2024): The impact of digital technologies on memory and memory studies. – Journal of Contemporary Philosophical and Anthropological Studies 2(1): 45-56.
[8] Castells, M. (2023): The network society revisited. – American Behavioral Scientist 67(7): 940-946.
[9] Chauhan, S., Akhtar, A., Gupta, A. (2022): Customer experience in digital banking: A review and future research directions. – International Journal of Quality and Service Sciences 14(2): 311-348.
[10] Chellapan, T., Daud, N.M., Narayanasamy, S. (2024): Smartphone use patterns and the impact on eye convergence among Malaysian teenagers. – International Journal of Ophthalmology 17(11): 2093-2100.
[11] Creswell, J.W., Creswell, J.D. (2017): Research design: Qualitative, quantitative, and mixed methods approaches. – Sage Publications, Thousand Oaks 438p.
[12] Flew, T., Gillett, R. (2021): Platform policy: Evaluating different responses to the challenges of platform power. – Journal of Digital Media & Policy 12(2): 231-246.
[13] Gawer, A., Srnicek, N. (2021): Online platforms: Economic and societal effects. – European Parliament Research Service Study 25p.
[14] Goel, M., Singal, G. (2021): Android OS case study. – ArXiv Preprint 21p.
[15] Goggin, G. (2025): Mobile AI: Communication and mobility after the smartphone. – Communication and Change 1(1): 5-15.
[16] Goggin, G. (2021): Apps: From mobile phones to digital lives. – Wiley, Hoboken 154p.
[17] Greshake, K., Abdelnabi, S., Mishra, S., Endres, C., Holz, T., Fritz, M. (2023): Compromising real-world LLM-integrated apps with indirect prompt injection. – Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security 12p.
[18] Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M. (2019): When to use and how to report the results of PLS-SEM. – European Business Review 31(1): 2-24.
[19] Hair, J.F., Matthews, L.M., Matthews, R.L., Sarstedt, M. (2017): PLS-SEM or CB-SEM: Updated guidelines on which method to use. – International Journal of Multivariate Data Analysis 1(2): 107-123.
[20] Harkin, L.J., Kuss, D. (2021): "My smartphone is an extension of myself": A qualitative exploration. – Psychology of Popular Media 10(1): 28-38.

[21] Henseler, J., Ringle, C.M., Sarstedt, M. (2015): A new criterion for assessing discriminant validity in variance-based SEM. – Journal of the Academy of Marketing Science 43(1): 115-135.
[22] Irwin, R. (2021): Heidegger and Stiegler on failure and technology. – In Bernard Stiegler and the Philosophy of Education, Routledge, London 14p.
[23] Kehtarnavaz, N., Parris, S., Sehgal, A. (2022): Smartphone-based real-time digital signal processing. – Springer Nature, Cham 155p.
[24] Kim, Y.C. (2020): Media system dependency theory. – The International Encyclopedia of Media Psychology 3: 1-17.
[25] Koswara, A. (2025): E-commerce rivalry in Southeast Asia: Google Trends analysis of TikTok Shop, Shopee and Lazada. – Mingzhi International Journal of Business 1(1): 23-34.
[26] Lee, M. (2024): Hacks, leaks, and revelations: The art of analyzing hacked and leaked data. – No Starch Press, San Francisco 544p.
[27] Leith, D.J. (2021): Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google. – Proceedings of International Conference on Security and Privacy in Communication Systems 10p.
[28] Li, X., Fu, S., Fu, Q., Zhong, B. (2021): Youths' habitual use of smartphones alters sleep quality and memory: Insights from a national sample of Chinese students. – International Journal of Environmental Research and Public Health 18(5): 12p.
[29] Linden, T., Nawaz, S., Mitchell, M. (2021): Adults' perspectives on smartphone usage and dependency in Australia. – Computers in Human Behavior Reports 3: 9p.
[30] Lotfy, A.Y., Zaki, A.M., Abd-El-Hafeez, T., Mahmoud, T.M. (2021): Privacy issues of public Wi-Fi networks. – Proceedings of the International Conference on Artificial Intelligence and Computer Vision 12p.
[31] McLuhan, M. (1975): McLuhan's laws of the media. – Technology and Culture 16(1): 74-78.
[32] Miller, D., Abed Rabho, L., Awondo, P., De Vries, M., Duque, M., Garvey, P., Haapio-Kirk, L., Hawkins, C., Otaegui, A., Walton, S. (2021): The global smartphone: Beyond a youth technology. – UCL Press, London 105p.
[33] Niu, G.F., Shi, X.H., Zhang, Z.L., Yang, W.C., Jin, S.Y., Sun, X.J. (2022): Can smartphone presence affect cognitive function? Fear of missing out as moderator. – Computers in Human Behavior 136: 6p.
[34] Reading, A. (2009): Memobilia: The mobile phone and the emergence of wearable memories. – In Save As… Digital Memories, Springer, London 15p.
[35] Saritepeci, M., Yildiz Durak, H., Özüdoğru, G., Atman Uslu, N. (2024): Digital literacy and security awareness in online privacy concerns: Gender differences. – Online Information Review 48(5): 983-1001.
[36] Shukla, M., Jain, V., Misra, R. (2022): Factors influencing smartphone-based online shopping: Evidence from young women shoppers. – Asia Pacific Journal of Marketing and Logistics 34(5): 1060-1077.
[37] Skatova, A., McDonald, R., Ma, S., Maple, C. (2023): Unpacking privacy: Valuation of personal data protection. – PLOS ONE 18(5): 21p.
[38] Spath, D., Gausemeier, J., Dumitrescu, R., Winter, J., Steglich, S., Drewel, M. (2023): Digitalisation of society. – In Handbook of Engineering Systems Design, Springer, Cham 27p.
[39] Tehlan, R., Sharma, B.K., Walia, M., Dhillon, D., Saini, D.K. (2021): Assessment of authenticity of face recognition by AI techniques in smartphones. – In Handbook of AI in Engineering Applications, Springer, Cham 12p.
[40] Van Zandwijk, J.P., Boztas, A. (2021): The phone reveals your motion: Digital traces of walking, driving and other movements on iPhones. – Forensic Science International: Digital Investigation 37: 10p.

[41] Vaterlaus, J.M., Aylward, A., Tarabochia, D., Martin, J.D. (2021): "A smartphone made my life easier": Age of adolescent smartphone acquisition and well-being. – Computers in Human Behavior 114: 10p.
[42] Vezzoli, M., Colombo, A., Marano, A., Zoccatelli, G., Zogmaister, C. (2023): Test for mobile phone dependence: Psychometric properties and confirmatory factor analysis. – Current Psychology 42(1): 714-725.
[43] Zhang, Y., Yang, Y., Lin, Z. (2023): Don't leak your keys: Exploiting AppSecret leaks in mini-programs. – Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security 12p.