**Proceeding**
**Jogjakarta Communication Conference**
Volume 4, No 1, pp. 534-546
ISSN 2988-5523

# Does Digital Inclusion Guarantee Digital Safety? Gendered Cyber Vulnerabilities among Urban Women Farmer Groups

Lian Agustina Setiyaningsih [1*], Irma Mufita Yulistiowati [1], Muhammad Hanif Fahmi [2], Firmando Sion Prayoga [1]

[1] Department of Communication Science, Universitas Merdeka Malang, 65146, Indonesia
[2] Faculty Department of Information System, Universitas Islam Raden Rahmat Malang, 65163, Indonesia

[*]Corresponding author's email: lian.agustina@unmer.ac.id

**Keywords**
Digital inclusion; Digital safety; Gender; Delegated control; Urban women farmer group

ABSTRACT

The expansion of the platform-based economy in the digital era has driven increased digital inclusion for women's groups, including urban women farmer communities. However, increased digital access and participation are not always accompanied by strengthened digital security. This study aims to analyze how urban women farmer groups construct and negotiate digital security literacy within platform economy practices, and to identify the gap between digital inclusion and account security sovereignty. This study fills a theoretical gap in the digital inclusion and digital literacy literature, which tends to emphasize individual access and skills without considering the distribution of security control based on social and gender relations. The study used a qualitative case study approach with one women's farmer group in Malang City, Indonesia, involving eight informants (six members and two marketplace administrators). Data were collected through in-depth interviews, focus group discussions, and observations of digital communication practices. The results indicate that although the group's digital engagement is high, centralized marketplace account management and password-sharing practices within the domestic sphere create a sense of delegated control. Digital security is understood as a matter of interpersonal trust, rather than systematic procedures, thus giving rise to relational vulnerabilities. The conclusion is that digital inclusion does not automatically guarantee digital security; Security sovereignty depends on the distribution of control within domestic and collective structures, so security literacy needs to be understood as a relational social practice.

## 1. Introduction

The expansion of digital platforms in the era of artificial intelligence (AI) has fundamentally transformed patterns of economic participation, communication practices, and community organization. In various developing countries, digital inclusion is promoted as a path to empowerment, economic mobility, and social connectivity. Governments, development agencies, and technology companies often position digital access as a solution to inequality, particularly for women and vulnerable groups. However, despite the growing access to platforms like WhatsApp, Instagram, and online marketplaces, attention to digital security has lagged (Palupi, 2019; Setiyaningsih et al., 2021). From a Communication Arts perspective, a crucial question arises: Does increased participation in the platform-based economy automatically guarantee digital security and autonomy?

In Indonesia, digital transformation has penetrated the informal economy, including urban women farmers. These groups are increasingly utilizing digital media to market products, manage orders, and build relationships with consumers (Fahmi et al., 2021; Olivier & Heinecken, 2017). Social media platforms and marketplaces serve not only as a means of economic transactions but also as a communication infrastructure that fosters trust, visibility, and collective reputation (Shankar et al., 2022). However, this digital adoption is often not accompanied by adequate cybersecurity training or a systematic digital protection framework. As a result, digital inclusion in the community economy can coexist with forms of vulnerability that are not always (Setiyaningsih & Fahmi, 2025).

Studies on digital inclusion have focused heavily on aspects of access, skills, and technology use (Bagchi-Sen et al., 2010; Silver, 1994). Digital literacy frameworks generally focus on an individual's ability to access, evaluate, and produce information in online environments (Gilster & Glister, 1997; Kateryna et al., 2020; Lin & Wang, 2020). Recent developments have begun to incorporate the dimension of digital security literacy, which encompasses the ability to maintain privacy, manage account authentication, and recognize cyber risks (Smit et al., 2025). However, much of this literature assumes individual users. It fails to consider collective or relational patterns of platform engagement, particularly in the informal economy, where account ownership and management can be shared or delegated.

Similarly, Tickner (2004) feminist studies on cybersecurity demonstrate that digital risks are not gender-neutral. Women are more vulnerable to online harassment, digital surveillance, financial fraud, and various forms of control based on domestic and social relationships (Teixeira, 2023; Van Dijk, 2006). Gender-based digital vulnerabilities emerge not only in online public spaces but also in relational practices such as password sharing (Saadi et al., 2024), partner-managed accounts (Dziewa & Glowacz, 2022), and account centralization by group administrators (Siahaan, 2022). In this context, cyber risks are not only technical but also embedded in the communication structures and power relations surrounding platform use.

While the literature on digital inclusion and gender-based digital risks is growing, few studies examine how digital security literacy is shaped in informal (Setiyaningsih, & Jatmikowati, 2019), platform-based community economies (Upadhyay et al., 2022). Urban women's farming groups represent a relatively underexplored context in digital communication studies. Most research focuses more on the digitalization of large-scale agriculture or formal MSMEs in marketplace ecosystems (Warschauer, 2007). Few studies have examined how practices of digital control delegation, such as sharing passwords with partners or centralizing marketplace accounts by group admins-influence cybersecurity capacity in women-based collective economies (Cheng & Bilal, 2025; Nath & Athinuwat, 2021; Yurembam et al., 2025).

This gap points to a broader theoretical tension: digital inclusion is often celebrated as a form of empowerment, but digital participation can actually generate new layers of relational (Carcelén-García et al., 2023) and structural vulnerabilities (Helsper & Smahel, 2020). When digital engagement is mediated by domestic authorities or collective management, access does not necessarily translate into autonomy or security. In platform-based communication systems, control over accounts often means control over visibility, financial transactions, and reputational capital. Therefore, the key issue is not simply whether women have engaged in digital spaces, but rather under what conditions and to what extent they possess digital security sovereignty.

Against this backdrop, this study aims to analyze how urban women farmers construct and negotiate digital security literacy within platform-based economic practices mediated by gender relations. Specifically, this study examines the types of structural and relational digital risks that emerge in their engagement with platforms. Platform, how gender shapes exposure to and perceptions of digital threats, how domestic and collective control arrangements function as informal cybersecurity mechanisms, and where the gap between digital inclusion and digital security capacity lies.

To address this gap, this study aims to explore how digital security practices shape urban women farmers' engagement with digital platforms. Specifically, it identifies the forms of digital security risks that emerge in the use of platforms by urban women farmers and analyzes how gender relations influence exposure to and perceptions of digital threats. It also examines how domestic and collective control arrangements, such as account access sharing, authentication management, and informal trust

mechanisms, function as contextually evolving forms of cybersecurity practices within platform-based economic activities. This analysis seeks to uncover the gap between expanding digital inclusion and the community platform economy's digital security capacity.

This research contributes to communication arts studies in three aspects. First, it expands the discourse on digital literacy by positioning cybersecurity as a relational and collective practice, rather than simply an individual competency. Second, it integrates a gendered cybersecurity perspective into the study of platform economies, highlighting the delegation of digital authority as a source of vulnerability. Third, it presents an empirical analysis of digital security negotiations within women's community economies in the Global South, while also questioning the assumption that digital access automatically guarantees safe and autonomous participation.

To empirically examine these dynamics, this research adopts a qualitative case study approach focusing on digital governance practices within a group of urban women farmers who actively use digital platforms for economic activities. This approach was chosen because it allows for an in-depth analysis of how digital security practices are shaped through the interaction between the group's organizational structure, gender relations, and the platform infrastructure used in daily activities. By positioning account management practices as the unit of analysis, this research examines digital security risks not only as a technical issue but also as a social phenomenon shaped by the distribution of authority, authentication arrangements, and informal control mechanisms within the group. This approach allows for identifying gaps between expanding digital inclusion and digital security capacity within platform-based economic practices. The following section describes the research design, research locations and participants, data collection procedures, and the analytical strategies used to understand digital governance configurations and their implications for digital security vulnerabilities.

## 2. Method

This research uses a case study design to deeply understand digital security literacy practices among a group of urban women farmers, using a qualitative approach. This approach was chosen because the research focuses on the construction of meaning, communication practices, and relational dynamics that shape digital security within the context of a platform-based economy. The case study allows for a contextual analysis of password-sharing practices, delegation of account control, and informal security mechanisms that emerge in domestic and collective interactions.

The research was conducted among a group of urban women farmers who actively utilize social media and online marketplaces for economic activities. The research was conducted in Malang City, East Java Province, Indonesia. The unique characteristics of this group of women in the city are their urban residence and the cultivation of vegetables and fruit for daily consumption. Informants were selected purposively based on the following criteria: (1) active group members, (2) involved in managing or using digital accounts for product marketing, and (3) experienced in sharing account access or managing platforms collectively. Participants included both regular members and group marketplace administrators, enabling analysis of digital control relations at both the domestic and collective levels.

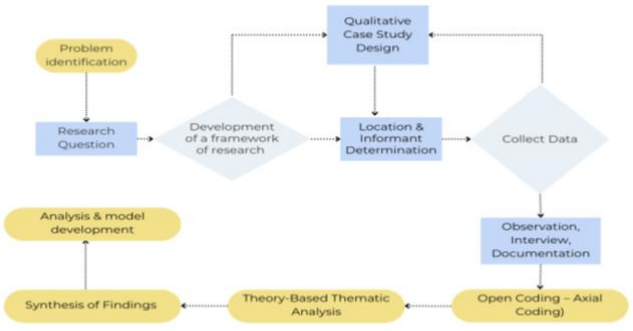


**Figure 2** Research Flow [1]

(Developed by the author, 2026)

Data were collected through in-depth semi-structured interviews with eight informants, consisting of six regular members and two marketplace administrators of an urban women farmers' group. The in-depth interviews were used to explore personal experiences with digital platform use, password sharing practices, perceptions of cybersecurity risks, and the dynamics of account control in both the domestic and collective spheres. Six regular members were interviewed to understand usage practices and reliance on account management. In contrast, two marketplace administrators were interviewed to explore mechanisms for account centralization, digital decision-making, and responsibilities for managing online transactions. In addition to individual interviews, focus group discussions (FGDs) were conducted to identify collective patterns in marketplace management, forms of digital communication coordination, and risk-mitigation mechanisms that have developed informally among members (Shabina et al., 2024). To maintain confidentiality, informants were coded M1–M6 (members) and A1–A2 (admins) in all quotes and analyses.

Furthermore, researchers conducted limited observations of the group's digital communication practices, including patterns of account access distribution, platform administration tasks, and online interactions with consumers. These observations aimed to observe how digital control structures operate in everyday practice directly. Documentation in the form of screenshots (with participant consent) and field notes was used to strengthen the analysis of account control delegation structures, internal communication patterns, and potential digital security vulnerabilities emerging in the platform-based economy.

Data were analyzed using a thematic analysis approach. The analysis process involved transcription, open coding, categorization, and the extraction of key themes (Mey, 2022; Njie & Asimiran, 2014). Initial coding focused on identifying types of digital risks (e.g., password control, centralization of marketplace accounts), forms of power relations in account management, and informal mitigation practices that developed within the group.

Next, these themes were analyzed interpretively, linking them to a digital security literacy framework and a gender perspective on platform communication. The analysis not only identified security practices but also examined how these practices were negotiated within domestic and collective relational structures, as well as the gaps between digital access and digital security capacity. To ensure data validity, this study employed triangulation of sources and methods, comparing findings from individual interviews, focus group discussions (FGDs), and observations. Furthermore, member checking was conducted by confirming interview summaries with several participants to ensure accurate interpretations. Transparency in the coding process and recording of researcher reflections was also maintained to minimize interpretive bias.

## 3. Result and Discussion

The following research findings are presented and discussed within the conceptual framework outlined above. The analysis focuses on how digital account governance practices are shaped within the economic activities of urban women farmer groups utilizing digital platforms. Using a theory-informed thematic analysis approach, interview and observation data are analyzed to identify recurring patterns of practice in managing account access, authentication, and digital coordination within the group. The findings are then organized into four main themes that represent the evolving configuration of digital governance in everyday practice: the distribution of digital account authority within the group, the mediation of authentication in the domestic sphere, the role of informal trust as a governance mechanism that replaces formal security protocols, and the conditions under which digital inclusion actually creates security vulnerabilities. Each theme is presented not only as an empirical description but also critically analyzed by linking it to the Social Practice Theory framework and the concept of micro digital governance to explain how the interaction between technology, organizational structure, and social relations shapes digital security practices in the context of a platform-based economy.

### 3.1. Presenting the Results

#### General Findings of Digital Phenomena in Urban Women Farmers' Groups

Women's farmer groups in Malang City demonstrate a high level of digital engagement in supporting their economic activities. WhatsApp is used for customer coordination and communication, Instagram serves as a promotional showcase for products, and an Instagram-based marketplace account is collectively managed to sell crops. Several members acknowledged that digital platforms expand market reach and increase sales. One member stated, *"Now buyers are not just neighbors, but some come from out of town too because they see posts on Instagram"* (Informant M3). Digitalization has thus become an integral part of the group's communication and economic distribution practices.

Table 1. Digital Practices and Security Governance in Urban Women Farmers' Groups [2]

| Digital Practice | Evidence | Pattern | Implication |
|---|---|---|---|
| **Platform use (WhatsApp, Instagram)** | "Buyers now come from outside the area" (M3) | Active digital engagement | Expands market reach |
| **Marketplace account management** | "Admin handles chats and transfers" (M1) | Centralized account control | Unequal digital authority |
| **Role division in digital tasks** | Members send products; admin manages platform | Delegated digital roles | Efficiency prioritized |
| **Password sharing** | "My husband keeps the passwords" (M5) | Domestic mediation of access | Gendered security control |
| **Account security access** | Limited to admins/household | Restricted authentication | Security shaped by relationships |

Source: Developed by the author (2026)

However, this intense engagement is not accompanied by equal distribution of control over the account and its security system. Two admins centrally manage the marketplace account, while other members handle digital administrative tasks themselves, as stated: *"The sales account is actually handled by the admin. We just send the goods, and then they handle the chat and transfers"* (Informant M1). In the domestic sphere, the practice of sharing passwords with husbands also occurs, citing trust or technical limitations, as expressed by the phrase, *"My husband usually keeps the passwords. I am afraid I will press the wrong key if I manage them myself"* (Informant M5). This situation indicates that despite the group's active digital engagement, control over account access and security is not evenly distributed. The findings suggest that digital security literacy does not exist as an individual competency but is shaped by the structures of domestic and collective relationships.

This pattern indicates that digital participation within the group primarily occurs at the level of economic activity rather than digital governance. While members actively contribute to production, promotion, and order fulfillment, control over platform infrastructure and security settings remains concentrated among a limited number of actors. Such arrangements create a layered structure of participation in which many members are digitally engaged but lack direct authority over account access or security management. As a result, the benefits of digital inclusion, such as expanded market access coexist with unequal control over the technological systems that enable these activities. This configuration suggests that digital engagement in community-based platform economies is shaped not only by technological adoption but also by organizational roles and relational dynamics that influence how digital authority and security responsibilities are distributed within the group.

#### Structural Risks in the Platform Economy

The management of the women's farmer group's marketplace account is centralized among two admins, who have full control over login access, product uploads, customer communication, and transaction confirmation. This model creates a single point of control within the group's digital

economy structure. Other members do not have direct access to the account or technical information related to digital security, including password settings and authentication. One member stated, *"We do not know the sales account password. It is all held by the admin, so if anything happens, we ask him"* (Informant M2). This statement indicates that control over the digital communication infrastructure is not evenly distributed, but rather concentrated in the hands of certain individuals.

This centralization also poses the potential risk of leaks or misuse, both intentional and unintentional. Reliance on one or two account managers means that all transaction activity and the group's digital reputation depend on the capacity and integrity of the admin. One admin admitted, *"If there is a problem with the account or if you forget the password, all sales can stop because other members cannot access it"* (Informant A1). This statement demonstrates that the sustainability of the group's digital economy is highly dependent on the stability and control of certain individuals, creating systemic vulnerabilities in the event of access disruptions or internal conflict.

Table 2. Structural Risks in the Platform-Based Management of Marketplace Accounts [3]

| Structural Condition | Evidence (Interview) | Observed Risk | Implication |
|---|---|---|---|
| **Centralized account control** | "We do not know the sales account password" (M2) | Limited member access | Unequal digital authority |
| **Dependence on two admins** | "If there is a problem with the account, sales can stop" (A1) | Single point of control | Operational disruption risk |
| **Restricted security knowledge** | Members unaware of password settings or authentication | Low shared security capacity | Structural dependency |
| **Limited transaction transparency** | "We just trust the admin… we do not always see chats and transfers" (M4) | Informal monitoring | Reduced accountability |
| **Trust-based governance** | Reliance on personal trust instead of procedures | Weak formal security protocol | Institutional vulnerability |

Source: Developed by the author (2026)

Furthermore, the centralized model also raises issues of transparency in transaction management and account security. Some members stated that they do not always know the details of customer communication processes or account security mechanisms. One informant stated, *"We just trust the admin, but we do not always see chats and transfers directly"* (Informant M4). Collective trust becomes the primary mechanism that replaces formal security procedures. However, this situation demonstrates structural dependency in platform management. Account centralization creates structural dependency that limits members' digital autonomy.

**Domestic Relations and Delegation of Account Control**

In addition to centralization at the collective level, the practice of delegating account control also occurs in the domestic sphere through password sharing with husbands. Several members admitted that account management, including password storage and authentication settings, was delegated to their partners due to trust, limited technical knowledge, and the division of household chores. One informant stated, *"My husband usually keeps the passwords because he understands phones better, and I am afraid of making mistakes if I set them myself"* (Informant M5). This statement demonstrates that digital security literacy is influenced not only by technical skills but also by the construction of gender roles within the household. This delegation is often viewed as a form of cooperation or efficiency, but it also reflects a dependence on technological authority associated with men in the domestic context.

This practice of sharing access also impacts control. The verification code (OTP) and financial access associated with marketplace accounts or digital accounts are often overlooked. In some cases, transaction notifications or authentication codes are sent to the husband's device, leaving women without direct control over the transaction confirmation process. One member revealed, *"If an OTP arrives, it usually goes to my husband's phone because his number is registered. So I wait for him to log in"* (Informant A2). This situation demonstrates that access to digital security systems is not

entirely in the hands of female users, but rather mediated by domestic relationships that impact their financial and digital autonomy. This practice of sharing access places digital security within domestic power relations, rather than within individual control.

Table 3. Domestic Mediation of Digital Account Control [4]

| Domestic Practice | Evidence (Interview) | Observed Pattern | Implication |
|---|---|---|---|
| **Password storage by husband** | "My husband usually keeps the passwords…" (M5) | Delegated account management | Gendered technological authority |
| **Limited technical confidence** | Women rely on husbands for settings | Perceived skill gap | Reduced digital autonomy |
| **OTP sent to husband's phone** | "I wait for him to log in" (A2) | Authentication mediated by spouse | Indirect control over transactions |
| **Shared account access in household** | Partners assist in login and verification | Domestic cooperation | Security embedded in family relations |
| **Trust-based delegation** | Passwords shared due to trust | Informal access governance | Dependency in digital security |

Source: Developed by the author (2026)

These findings indicate that digital account governance in urban women farmers' groups extends beyond organizational arrangements and is deeply embedded in household dynamics. The delegation of passwords and authentication processes to husbands reflects how digital control is negotiated through everyday domestic relationships rather than solely through technical competence. As a result, women's engagement with digital platforms occurs within a layered structure of authority in which familial roles mediate access to technology, financial verification, and security management. While such arrangements are often perceived as practical solutions to technical limitations or workload distribution, they simultaneously reshape the boundaries of digital autonomy. In this context, digital security becomes relationally governed rather than individually controlled, illustrating how platform participation in community-based economies intersects with gendered power relations that influence access, authority, and security within digital infrastructures.

**Risk Perception and Security Awareness**

Although the practice of delegating account control and marketplace centralization indicates potential structural vulnerabilities, most members do not explicitly view these conditions as digital security risks. Risks are more often understood as external threats, such as hacking or fraud by external parties, rather than as consequences of shared internal controls. One informant stated, *"I am afraid of hacking or fraud, but if my husband holds the password, he is safe, he is at home"* (Informant M5). This statement demonstrates that a sense of security is built on interpersonal trust, rather than on an understanding of digital security systems. Therefore, security is perceived more as a matter of social relationships than as a technical, procedure-based risk management.

Furthermore, awareness of advanced security features such as two-factor authentication (2FA), device-based login management, and phishing detection is relatively low. Some members admitted they had never considered additional security settings as long as their accounts remained usable without interruption. One participant stated, *"As long as there are no problems, we never think about using additional security or anything else. The important thing is being able to sell"* (Informant M2). The digital literacy orientation, which emphasizes economic functions over system protection, suggests that risk is often understood as an external technical issue rather than a consequence of relational control structures.

Table 4. Domestic Mediation of Digital Account Control [5]

| Risk Perception | Evidence (Interview) | Observed Pattern | Implication |
|---|---|---|---|
| **Risk viewed as external threat** | "I am afraid of hacking or fraud…" (M5) | Security linked to outside attacks | Internal governance risks overlooked |
| **Trust in household members** | "If my husband holds the password, he is safe" (M5) | Security based on interpersonal trust | Security framed as relational safety |
| **Low awareness of security features** | Limited knowledge of 2FA and device login settings | Minimal use of advanced protection | Weak technical security practices |
| **Economic priority in platform use** | "The important thing is being able to sell" (M2) | Focus on economic function | Security treated as secondary concern |
| **Passive security awareness** | Security considered only after problems occur | Reactive security mindset | Potential vulnerability accumulation |

Source: Developed by the author (2026)

Taken together, these findings reveal a mismatch between the structure of digital account governance and the way group members perceive risks. While centralized account management and the delegation of authentication processes can create systemic vulnerabilities, these arrangements are rarely viewed as internal security risks. Instead, security is largely framed in terms of interpersonal trust and the absence of visible technical disruptions. This perception reflects a pragmatic orientation toward digital platforms, in which maintaining continuous sales activity is prioritized over implementing preventive security measures. Consequently, digital security awareness primarily develops in response to external threats rather than as a proactive understanding of platform governance and access controls. This pattern suggests that within community-based platform economies, perceptions of safety are shaped less by technical knowledge of cybersecurity practices and more by relational confidence in familiar actors, thereby reinforcing the normalization of governance structures that may inadvertently sustain underlying digital vulnerabilities.

**Informal Security Mechanisms and the Literacy Gap**

In the absence of formal security procedures, women's farmer groups rely on collective trust mechanisms as their primary protection against digital risks. Account security is not managed through a multi-layered verification system or authorization-based access sharing, but rather through social relationships, which are considered sufficient to guarantee stability. One member stated, *"We just trust the admin, because we have been working together for a long time and there have never been any problems"* (Informant M4) interpersonal trust substitutes for structured digital security protocols. In practice, informal social controls such as peer oversight and reputation within the group-serve as primary safeguards. However, they are not explicitly designed to protect against more complex cyber risks.

However, there was no formal digital security training, written guidelines on password management, or standard procedures in the event of an access breach. Most members admitted to having never received specific cybersecurity training. One informant said, *"We have received training on online marketing, but we were never taught about account security or security settings"* (Informant A1). This gap indicates that the developed digital literacy is more focused on increasing sales and visibility than on protecting systems and data. Thus, the security mechanisms in place are reactive and trust-based, rather than preventative and procedure-based. Digital inclusion is taking place without a systematic foundation in digital security.

Table 5. Informal Security Mechanisms and Digital Literacy Gap [6]

| Security Practice | Evidence (Interview) | Observed Pattern | Implication |
|---|---|---|---|
| **Trust-based account protection** | "We just trust the admin…" (M4) | Security built on interpersonal trust | Informal governance replaces protocols |
| **Peer monitoring within group** | Members rely on reputation and long-term cooperation | Social oversight as safeguard | Limited protection against cyber risks |
| **Absence of formal procedures** | No written password rules or breach protocol | Informal security management | Weak institutional security structure |
| **Lack of cybersecurity training** | "We were never taught about account security" (A1) | Literacy focused on marketing skills | Security knowledge gap |
| **Economic-oriented digital literacy** | Training emphasizes online sales and promotion | Platform use prioritized over protection | Preventive security practices absent |

Source: Developed by the author (2026)

These findings highlight that digital security practices within the women's farmer groups are shaped more by social cohesion and long-standing interpersonal relationships than by formal cybersecurity frameworks. While trust and peer monitoring provide a sense of stability in daily operations, they function primarily as informal governance mechanisms rather than as structured safeguards against digital threats. The absence of standardized procedures, documented security guidelines, and targeted cybersecurity training indicates that digital capacity building in these communities has largely prioritized economic participation over system protection. As a result, digital literacy develops functionally, supporting marketing, communication, and sales without a parallel understanding of risk management and platform security. This imbalance suggests that digital inclusion initiatives, when focused predominantly on economic empowerment, may inadvertently overlook the institutional and technical foundations required to ensure secure, resilient digital participation within community-based platform economies.

### 3.2. Create a Discussion

Digital inclusion in women's community economies is not synonymous with digital security sovereignty. Although women's farming groups in Malang City have actively used various platforms to expand markets and increase product visibility, this participation does not automatically confer autonomy in managing account security. Involvement in the platform-based economy occurs within a structure of delegated and relational control, both through centralized marketplace management and the practice of password sharing within the domestic sphere. In this context, control over accounts, including login access, authentication settings, and transaction confirmation, becomes a key determinant of digital sovereignty. When this control is not in users' hands, digital participation can create new forms of vulnerability. Thus, digital inclusion without equal distribution of control does not guarantee security but can instead reproduce dependency and vulnerability within surrounding social-relational structures.

This finding challenges the dominant assumption in digital inclusion literature, which measures empowerment based on access and use, without considering the distribution of security control. Classic studies on digital inclusion emphasize the importance of access to technology, user skills, and participation in digital spaces as key indicators of social and economic integration (Van Dijk, 2006; Warschauer, 2007). Similarly, digital literacy frameworks generally focus on individual competencies in accessing, understanding, and producing digital content (Abell & Biswas, 2023). However, this approach tends to position users as autonomous actors in control of their own devices and accounts. The results of this study indicate that, in the context of women's community economies, digital literacy is not entirely individual, but rather relationally shaped through the distribution of delegated account control within domestic and collective structures. Thus, there is a blind spot in mainstream literature that has not adequately integrated the dimensions of security,

authority, and power relations into measures of digital inclusion. Access and skills are insufficient to ensure security when control over digital security systems is not in users' hands.

The findings regarding password sharing and OTP control within households demonstrate that digital security cannot be understood as a purely technical issue, but rather as part of the structure of gender-based power relations. From a feminist cybersecurity perspective, digital risks are not neutral but are shaped by the distribution of authority and control within social relations (Tickner, 2004). The practice of sharing account access with one's husband is not simply a pragmatic habit or a form of domestic cooperation. However, it reflects how technological authority is often associated with men within the household structure. When control over passwords and two-factor authentication rests with the male partner, women's digital security is mediated by patriarchal relations that determine who has the right to control access. Thus, digital security is embedded in domestic structures that produce dependency and limit the autonomy of female users. This finding extends studies of gender and technology, which emphasize that technology is not neutral but rather reproduces or negotiates existing power relations.

This article proposes the concept of "Relational Cyber Vulnerability" to explain that digital security vulnerabilities in women's community economies stem not primarily from limited access or low technical skills, but from the delegated distribution of control within domestic and collective social relations. This concept emphasizes that risk arises when authority over accounts including password management, authentication, and transactions does not reside directly with the user but is mediated by the relational structures that shape everyday digital communication practices. Thus, digital security needs to be understood as a matter of distributed authority, not simply individual competence. The implications of these findings suggest that digital literacy initiatives focused on improving online access and marketing tend to neglect the relational dimension of security. Training programs that fail to integrate gender-based security considerations risk expanding participation without strengthening digital sovereignty.

Furthermore, community marketplace management requires more structured transparency and access-sharing mechanisms to prevent account centralization from creating systemic dependency. By viewing digital security as a distributed social practice, digital empowerment approaches can shift from a centralized approach. There is a shift from increased participation to more equitable and sustainable control.

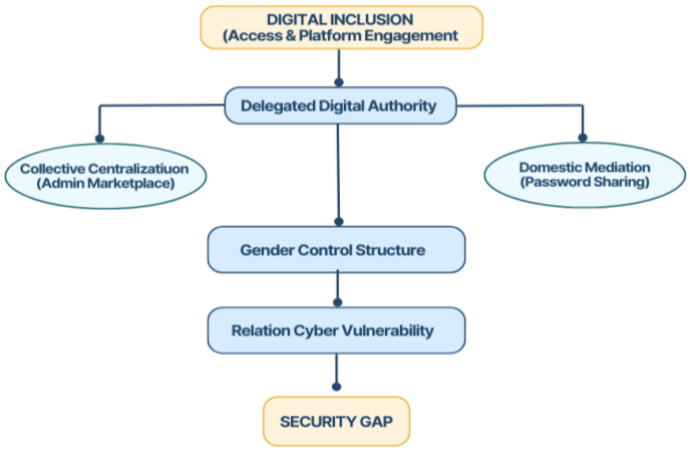


**Figure 2** Relational Cyber Vulnerability Framework and the Emergence of a Security Gap [7]

(Developed by the author, 2026)

Based on the overall findings and analysis, this article synthesizes a relational model that explains the dynamics of digital security in women's community economies. This process begins with digital inclusion, namely, active use of platforms for economic activities. However, this inclusion occurs under conditions of delegated control, where account management and security systems are not entirely in the hands of individuals, but rather centralized by collective administrators or mediated by partners in the domestic sphere. This delegation then operates through gendered mediation,

namely the distribution of technological authority influenced by gender-based power relations. This combination of centralization and gender mediation results in relational vulnerability, in which security risks arise not from a lack of access but from unequal control structures. The accumulation of these conditions ultimately creates a security gap, namely the gap between high levels of digital participation and limited digital security capacity. Thus, the question is no longer whether women are digitally included, but rather the extent to which they have sovereignty over digital security within the relational structures that shape platform communication practices.

## 4. Conclusion

This research shows that the successful integration of digital platforms into women's community economies does not automatically translate into enhanced digital security and autonomy. In the context of urban women farmers, the practice of centralizing accounts and delegating domestic control creates a security pattern that is relational and trust-based rather than procedural. These findings emphasize the importance of viewing digital security as part of the social structure that shapes platform communication practices, rather than simply a matter of individual technical skills. Therefore, digital empowerment efforts at the community level need to consider the distribution of control, gender dynamics, and collective governance to ensure that digital participation goes hand in hand with sustainable protection.

## 5. Acknowledgement

The authors extend their gratitude to the Urban Women Farmers Group in Malang, especially Cemara Hijau Farm and Green Residence Farm, for their generous participation and collaborative engagement in this study. The insights shared by the participants were essential to the development of the research findings and conceptual framework. This research was supported by funding from the Department of Communication Studies, Universitas Merdeka Malang, whose institutional assistance is gratefully acknowledged.

## 6. References

Abell, A., & Biswas, D. (2023). Digital Engagement on Social Media: How Food Image Content Influences Social Media and Influencer Marketing Outcomes. *Journal of Interactive Marketing*, *58*(1), 1–15. https://doi.org/10.1177/10949968221128556

Bagchi-Sen, S., Rao, H. R., &, Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional*, *12*(1), 24–31.

Carcelén-García, S., Narros-González, M. J., & Galmes-Cerezo, M. (2023). Digital vulnerability in young people: gender, age and online participation patterns. *International Journal of Adolescence and Youth*, *28*(1), 2287115.

Cheng, Y. W., & Bilal, A. (2025). Regulatory data privacy concerns in proliferating IoT era of telecommunication data monetisation: a systematic literature review. *Computing*, *107*(9), 190.

Dziewa, A., & Glowacz, F. (2022). Getting out from intimate partner violence: Dynamics and processes. A qualitative analysis of female and male victims' narratives. *Journal of Family Violence*, *37*(4), 643–656.

Fahmi, M. H., Widayati, S., & Setiyaningsih, L. A. (2021). Phenomenology Study of Rural Women Identity, Information Communication Technology and Human Security. *1ST INTERNATIONAL CONFERENCE IN SOCIAL SCIENCE (ICONISS) 2020*, 1–8.

Gilster, P., & Glister, P. (1997). *Digital literacy*. Wiley Computer Pub.

Helsper, E. J., & Smahel, D. (2020). Excessive internet use by young Europeans: psychological vulnerability and digital literacy? *Information, Communication & Society*, *23*(9), 1255–1273.

Kateryna, A., Oleksandr, R., Mariia, T., Iryna, S., Evgen, K., & Anastasiia, L. (2020). Digital Literacy Development Trends in the Professional Environment. *International Journal of*

*Learning, Teaching and Educational Research*, *19*(7), 55–79. https://doi.org/10.26803/ijlter.19.7.4

Lin, X., & Wang, X. (2020). Examining gender differences in people's information-sharing decisions on social networking sites. *International Journal of Information Management*, *50*, 45–56. https://doi.org/10.1016/j.ijinfomgt.2019.05.004

Mey, G. (2022). Qualitative methodology. In *International handbook of psychology learning and teaching* (pp. 453–478). Springer.

Nath, T. D., & Athinuwat, D. (2021). Key factors of women empowerment in organic farming. *GeoJournal*, *86*(6), 2501–2520. https://doi.org/10.1007/s10708-020-10211-6

Njie, B., & Asimiran, S. (2014). Case study as a choice in qualitative methodology. *Journal of Research & Method in Education*, *4*(3), 35–40.

Olivier, D. W., & Heinecken, L. (2017). Beyond food security: women's experiences of urban agriculture in Cape Town. *Agriculture and Human Values*, *34*(3), 743–755. https://doi.org/10.1007/s10460-017-9773-0

Palupi, Palupi. (2019). Selective Self-Presentation Through Video-Mediated Communication:A Study of Hyperpersonal Communication. *MediaTor*, *12*(1), 102-112.

Saadi, Z. M., Sadiq, A. T., Akif, O. Z., & Farhan, A. K. (2024). A survey: security vulnerabilities and protective strategies for graphical passwords. *Electronics*, *13*(15), 3042.

Setiyaningsih, L. A., & Jatmikowati, S. H. (2019). Media Baru Dalam Komodifikasi Waktu Luang Ibu Rumah Tangga. *ETTISAL: Journal of Communication*, *4*(1), 23–32.

Setiyaningsih, L. A., & Fahmi, M. H. (2025). Mengkaji Ulang Literasi Digital dan Adopsi Media Digital oleh Kelompok Wanita Tani Perkotaan di Negara ASEAN. *Prosiding Seminar Nasional Ilmu Ilmu Sosial (SNIIS)*, *4*, 1165–1184.

Setiyaningsih, L. A., Fahmi, M. H., & Molyo, P. D. (2021). Selective Exposure Media Sosial Pada Ibu dan Perilaku Anti Sosial Anak. *Jurnal Komunikasi Nusantara*, *3*(1), 1–11. https://doi.org/10.33366/jkn.v3i1.65

Shankar, V., Grewal, D., Sunder, S., Fossen, B., Peters, K., & Agarwal, A. (2022). Digital marketing communication in global marketplaces: A review of extant research, future directions, and potential approaches. *International Journal of Research in Marketing*, *39*(2), 541–565. https://doi.org/10.1016/j.ijresmar.2021.09.005

Siahaan, A. L. S. (2022). Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi. . *Majalah Hukum Nasional*, *52*(2), 209–223.

Silver, H. (1994). Social exclusion and social solidarity: Three paradigms. *Int'l Lab. Rev.*, *133*, 531.

Smit, A., Swart, J., & Broersma, M. (2025). Bypassing digital literacy: Marginalized citizens' tactics for participation and inclusion in digital societies. *New Media & Society*, *27*(6), 3127–3145. https://doi.org/10.1177/14614448231220383

Teixeira, T. C. (2023). Gendering Cyberwarfare: Towards a Feminist Approach to the Development of International Humanitarian Law Applicable to Cyber Operations. . *CEBRI-Revista: Brazilian Journal of International Affairs*, *7*, 58–80.

Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review*, *16*(1), 43–48.

Upadhyay, P., Kumar, A., Dwivedi, Y. K., & Adlakha, A. (2022). Continual usage intention of platform-based governance services: A study from an emerging economy. *Government Information Quarterly*, *39*(1), 101651. https://doi.org/10.1016/j.giq.2021.101651

Van Dijk, J. A. G. M. (2006). Digital divide research, achievements and shortcomings. *Poetics*, *34*(4–5), 221–235.

Warschauer, M. (2007). The paradoxical future of digital learning. *Learning Inquiry*, *1*(1), 41–49.

Yurembam, G. S., Pramanik, M., Yengkhom, R. D., Hemochandra, L., Chakma, B., Jhajharia, D., & Patle, G. T. (2025). Integration of Digital Innovation in Urban Farming: A Review towards Advancing Sustainable Food Security in South and Southeast Asian Cities. *Journal of Agricultural Engineering (India)*, *62*(2), 494–517. https://doi.org/10.52151/jae2025622.1937