International Journal Software Engineering and Computer Science (IJSECS)
6 (3), 2026, 1262-1270
Published Online December 2026 in IJSECS (http://www.journal.lembagakita.com/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v6i3.8166.

RESEARCH ARTICLE Open Access

User Perceptions and Security Requirements for Digital Inheritance Management Systems: Evidence from a Survey Study

Kinyuy Marie-Noel Ngala [1*], **JohnPaul A.C. Hampo** [2], **Blessed Nkurumah Kpudzeka** [3], **Fomukom Mark Nsah Tanyi** [4]

[1*,2,3,4] Catholic University of Cameroon, Bamenda, North West Region, Cameroon.

Article History:

Received: July 24, 2026.
Revised: July 25, 2026.
Accepted: November 21, 2026.
Available online: November 30, 2026.
Published: December 1, 2026.

***Corresponding Author:**
ngalamarienoel5@gmail.com

Abstract: Digital legacy systems are frequently designed around assumptions about what users want and trust, yet these assumptions are rarely tested directly against user data. This paper reports a small-scale, exploratory survey (n = 39) conducted to inform the design of a digital will management system by examining awareness of digital-asset succession, trust in the secure storage of testamentary documents, and the perceived importance of specific security and access-control features. Respondents were recruited through a convenience sample distributed via an online form and were predominantly young adults (38 of 39 respondents aged 18–24). Results showed a pronounced gap between perceived importance and preparedness: 30 of 39 respondents (76.9%) rated their digital assets as important or very important, yet only 12.8% reported having ever made a plan for them, and 59.0% did not know what happens to their online accounts after death or prolonged inactivity. Trust in a secure system to store a digital will was mixed (16 yes, 16 maybe, 7 no), while support for requiring multiple trusted people to approve emergency access was comparatively strong (56.4%). Encryption of documents (84.6%) and strong password protection (74.4%) were the most requested features, whereas automatic access after inactivity was more contested (16 yes, 17 no, 6 maybe) than multi-party approval. We discuss these findings against prior digital-legacy and privacy-paradox literature and derive concrete design implications, while remaining explicit that a convenience sample of 39 young respondents from a single institutional context cannot be generalized to the broader population and that all findings should be read as exploratory.

Keywords: Digital Inheritance; User Perceptions; Security Awareness; Trust; Multi-Party Authorization.

© The Author(s) 2026, corrected publication 2026. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution, and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third-party material in this article are included in the article's Creative Commons license unless stated otherwise in a credit line to the material. Suppose the material is not included in the article's Creative Commons license, and your intended use is prohibited by statutory regulation or exceeds the permitted use. In that case, you must obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

1. Introduction

Digital will and digital-inheritance management systems are typically designed around assumptions about what prospective users want, trust, and are willing to adopt: that users value encryption, that they want multiple trusted contacts involved in emergency access, or that automatic release after inactivity is acceptable. These assumptions matter because a system's security model is only as effective as its adoption; a highly secure digital will manager that users do not trust or understand will not be used, and its protective value is never realized in practice. Yet system-design literature in this area, including much of the digital-inheritance research reviewed in Section 2, tends to justify design choices by reference to other systems or to general security principles rather than to direct evidence of user perceptions.

This paper addresses that gap by reporting the results of a small, exploratory survey conducted to inform the design of LegacyVault, a companion digital will management system developed by the authors (Hampo *et al.*, 2026b). The survey examined four broad constructs: 1) current digital-asset habits and awareness of what happens to online accounts after death or prolonged inactivity; 2) trust in a secure system to store sensitive testamentary documents; 3) attitudes toward specific access-control mechanisms, in particular multi-party approval and inactivity-triggered automatic access; and 4) demand for specific security features (encryption, password protection, activity monitoring, and audit logging). We report the resulting data honestly and completely, including where the findings are inconclusive or contradict a designer's intuition, and we remain explicit throughout about the survey's methodological limitations, which are described in full in Section 3.2 and revisited in Section 4.3.

The contributions of this paper are threefold: 1) empirical, if exploratory, evidence of a gap between the perceived importance of digital assets and actual succession-planning behavior among a sample of young adult digital-platform users; 2) descriptive evidence on the relative acceptability of multi-party authorization versus automatic inactivity-triggered access, two mechanisms that are often treated as interchangeable in the digital-inheritance literature but that our respondents evaluated quite differently; and 3) a transparent, small-n case study in reporting survey evidence for a systems-design paper without overstating what a convenience sample of 39 respondents can support.

2. Related Work

2.1 Awareness and planning for digital assets after death

Öhman and Watson (2019) document the scale of unmanaged digital remains on major platforms and argue that most users have given little thought to what happens to their accounts after death. Bellamy *et al.* (2018) similarly find that digital legacy is an under-planned area of personal data management compared with the planning norms that exist for physical assets and wills, while Harbinja (2017) attributes part of this gap to the unclear legal status of digital assets, which leaves users uncertain about what, if anything, they can formally plan for. Accordingly, our survey's awareness items (Section 4.1) were designed to test whether this reported gap between perceived importance and actual planning behavior would appear in a small, local sample, independent of the specific legal context discussed in prior literature. Notably, most existing studies draw on platform-level data (such as account counts and policy analyses) or qualitative and legal arguments rather than direct survey measurements of ordinary users' stated awareness and planning behavior side by side. Measuring both constructs within the same instrument, as this survey does, allows the gap between them to be quantified directly for a given sample rather than inferred indirectly from separate strands of evidence, thereby offering a modest methodological contribution independent of the small sample size used here.

2.2 The privacy/security intention–behavior gap

A related and more general phenomenon in the privacy literature is the privacy paradox, wherein users frequently report strong concern about privacy and security while nonetheless failing to take corresponding protective action (Barth & de Jong, 2017). If a similar pattern holds for digital-legacy planning specifically, respondents who rate their digital assets as important would nonetheless be expected to report low rates of actual planning, yielding a specific, falsifiable prediction that Section 4.1 examines directly against our empirical data rather than assuming it holds.

2.3 Trust in digital-inheritance systems

Gibson and Kumar (2023) and Zahir (2025) discuss the fragmented and inconsistent nature of existing platform-specific inheritance tools, arguing that this fragmentation undermines user trust in any single mechanism. Meanwhile, Cetin (2024) and Autili *et al.* (2026) report from reviews of related systems literature that transparency and auditability are associated with higher user trust in systems handling sensitive legal

Copyright © 2026 IJSECS

information. None of this literature, however, provides direct survey evidence of trust levels among prospective users of a purpose-built digital will system, which is the gap our trust items (Section 4.1) address at an exploratory scale. Furthermore, the distinction between trust in a general digital platform (e.g., an e-mail or cloud-storage provider) and trust in a system specifically entrusted with a will or comparable legal document remains underexamined. A user might trust a cloud provider with everyday files while remaining more cautious about a document with legal and emotional significance because the costs of a security failure differ substantially—a lost holiday photograph and a compromised will do not carry the same consequence. Our instrument's trust item was therefore worded to target this specific, higher-stakes context rather than digital security in general, which is why its results are analyzed alongside the more general perceived-account-security item in Section 4.1 and discussed in Section 4.2.

2.4 Multi-party authorization and automatic access

Multi-party or threshold-based access control allows assigned users to collectively authorize valid digital access without any single user holding the complete key (Berwin, 2026). Prior work on digital-legacy system design (Hampo *et al.*, 2026a, 2026b) argues on security-engineering grounds that requiring agreement from more than one trusted party before releasing emergency access reduces the risk of single-party compromise or coercion compared with a single-contact or fully automatic release. Similarly, Zhao *et al.* (2026) note that traditional key-authentication schemes rely on bilinear pairings, which limits their generalizability due to substantial computational and communication overhead; they address this limitation by combining blockchain-based key-agreement protocols, attribute-based signatures, and linear secret-sharing key authentication. In addition, Paul and Sinha (2025) combined attribute-based encryption with a functional stream cipher to mitigate data leakage in cloud storage environments.

However, whether prospective users perceive these two inheritance-release mechanisms—multi-party approval versus automatic inactivity-triggered release—as similarly acceptable, or view them quite differently, is an empirical question that this survey was designed to probe (Section 4.1) rather than a question that the security-engineering literature alone can answer. Taken together, the reviewed literature motivates four empirical research questions: (RQ1) Is there a gap between the perceived importance of digital assets and actual succession-planning behavior in our sample? (RQ2) How much do respondents trust a secure system to store a digital will? (RQ3) Do respondents evaluate multi-party approval and automatic inactivity-triggered access similarly or differently? (RQ4) Which specific security features do respondents rate as important for a digital will management system? Sections 4.1 and 4.2 examine each question in turn using the survey data described in Section 3.

2.5 Comparison with Previous Studies

Previous studies on Gojek and Grab have predominantly followed two separate research streams. The first stream focuses on usability and user experience evaluation through empirical instruments such as the User Experience Questionnaire (Khuntari, 2022) and the System Usability Scale (Damanik *et al.*, 2025). Although these investigations effectively map user perceptions and identify operational interface strengths, their analytical conclusions are confined to descriptive score comparisons and percentile rankings without establishing strategic decision priorities. The second stream applies game theory to examine competitive platform interactions, evaluating dimensions such as marketing attributes (Nurhasanah *et al.*, 2023), promotional mixes (Christanto *et al.*, 2023), pricing mechanisms, and fleet operations (Cai *et al.*, 2024; Wang *et al.*, 2024; Wang & Li, 2024). However, these game-theoretic models rarely consider human-computer interaction parameters as direct competitive strategies. This study differs from previous research by integrating Nielsen's usability dimensions directly into a game-theoretic payoff framework. Rather than evaluating interface quality in isolation or limiting game models to operational and marketing variables, this study positions Gojek and Grab as competing decision-makers whose strategic alternatives are defined by learnability, efficiency, memorability, errors, and satisfaction. Transforming empirical user evaluations into relative payoff values analyzed through maximin, minimax, and saddle point principles allows this study to determine the specific usability attributes that offer the strongest competitive advantage for each platform, thereby bridging interface evaluation and strategic decision-making.

3. Methodology

3.1 Instrument and recruitment

A 16-item structured questionnaire was developed and distributed as an online form (https://docs.google.com/forms/d/1zyjZPV30EiNJS7D7OtYFH6vywg9R8ouKzTS5Jh_a-oY). The instrument comprised four sections: demographic and digital-platform-usage items (items 1–3); awareness and planning items concerning digital assets after death or prolonged inactivity (items 4–6); trust and security-perception

Copyright © 2026 IJSECS

items, including two multiple-select items on trusted security methods and desired system features (items 7–11); and access-control and system-adoption items, including two closed-ended items on multi-party approval and automatic inactivity-triggered access alongside two open-ended items on user concerns and suggestions (items 12–16). Respondents were recruited through a convenience sample—that is, the form link was shared through the researchers' personal and academic networks—rather than through random or stratified sampling of a defined population. Item wording used plain, non-technical language throughout (for example, "Would you trust a secure online system to store your digital will or important documents?" rather than a technical term such as "custodial risk"), on the reasoning that a survey aimed at gauging ordinary users' perceptions rather than specialists' technical judgments should not require security-domain literacy to be answered meaningfully. Two items (items 8 and 11) allowed multiple selections because trust in security methods and demand for system features were not expected to be mutually exclusive choices. The instrument was not formally piloted with a separate sample prior to distribution, which we note as a methodological limitation in Section 4.3.

3.2 Respondents and limitations of the sample

Thirty-nine complete responses were collected. Respondents were overwhelmingly young adults: 38 of 39 (97.4%) reported being aged 18–24, and 1 (2.6%) reported being aged 25–34, with no respondents recorded in other age brackets. All 39 respondents reported using digital platforms such as Google, Facebook, e-mail, or cloud storage. Consequently, this sample is best characterized as a convenience sample of young, digitally active individuals drawn substantially from a single academic and social network. It should not be treated as representative of the general population, of older adults (who arguably have more immediate reason to plan digital succession), or of non-users of digital platforms. All findings in Sections 4.1 and 4.2 should be read with this sampling limitation in mind; we return to it, together with other study limitations, in Section 4.3.

3.3 Data analysis approach

Closed-ended items were analyzed using simple descriptive statistics (frequencies and percentages), whereas multiple-select items were analyzed by counting each selected option independently so that percentages for these items do not sum to 100%. Two descriptive cross-tabulations were computed to examine RQ1 and RQ3 (reported in Section 4.1); given the small sample size and the resulting sparse cell counts, no inferential statistical tests (e.g., chi-square tests) were applied, and no claim of statistical significance is made anywhere in this paper. The two open-ended items (concerns and suggestions) were reviewed manually and grouped into recurring descriptive themes. This process represents a simple qualitative categorization intended to characterize the range of responses rather than a formally validated content-analysis procedure with independent inter-coder reliability statistics, and it is reported as such in Section 4.1.

4. Results and Discussion

4.1 Results

4.1.1 Awareness and planning (RQ1)

Table 1 reports respondents' self-rated importance of their digital assets alongside their reported online document-storage frequency and awareness of what happens to accounts after death or prolonged inactivity.

Table 1. Digital-asset usage, perceived importance, and awareness/planning (n = 39)

Item	Response	n	%
How often do you store important documents online?	Often	13	33.3%
	Sometimes	10	25.6%
	Rarely	8	20.5%
	Always	7	17.9%
	Never	1	2.6%
How important do you think your digital assets are?	Very important	20	51.3%
	Important	10	25.6%
	Neutral	9	23.1%
Aware of what happens to accounts after death/long inactivity?	No	23	59.0%
	Not sure	9	23.1%
	Yes	7	17.9%
Have you ever considered planning your digital assets after death?	Never thought about it	19	48.7%
	No	15	38.5%
	Yes	5	12.8%

Copyright © 2026 IJSECS

Combining the importance and planning items directly addresses RQ1. Among the 20 respondents who rated their digital assets as "very important," 8 (40.0%) had never thought about planning for them and only 3 (15.0%) had actually made a plan; similarly, among the 10 respondents who rated them as "important," only 1 (10.0%) had made a plan. Across the full sample, 30 of 39 respondents (76.9%) rated their digital assets as important or very important, whereas only 5 of 39 (12.8%) reported having made an actual plan, representing a roughly six-to-one gap between stated importance and reported planning behavior. This pattern is consistent with the privacy/security intention–behavior gap discussed in Section 2.2 (Barth & de Jong, 2017) and with the general under-planning of digital legacy reported by Öhman and Watson (2019) and Bellamy *et al.* (2013, 2018), although our data speak specifically to this young, convenience-sampled group.

4.1.2 Trust in secure storage and perceived account security (RQ2)

To examine RQ2, respondents were asked to evaluate the perceived security of their existing online accounts, their trust in a dedicated online system for storing a digital will, and their willingness to adopt a system such as LegacyVault, as summarized in Table 2.

Table 2. Perceived account security, trust in a secure digital-will system, and stated adoption intent (n = 39)

Item	Response	n	%
How secure do you think your online accounts are?	Secure	20	51.3%
	Neutral	16	41.0%
	Not secure	2	5.1%
	Very secure	1	2.6%
Would you trust a secure online system to store your digital will?	Yes	16	41.0%
	Maybe	16	41.0%
	No	7	17.9%
Would you use a system like LegacyVault?	Maybe	21	53.8%
	Yes	15	38.5%
	No	3	7.7%

As shown in Table 2, trust in a secure system to store a digital will was evenly split between "yes" and "maybe" (16 respondents, or 41.0%, each), with a minority (7, or 17.9%) answering "no." Stated willingness to actually use a system like LegacyVault followed a similar pattern, with a plurality (21, or 53.8%) selecting "maybe" rather than a firm "yes" (15, or 38.5%) or "no" (3, or 7.7%). These results indicate conditional rather than firm trust: most respondents are not opposed to the concept, yet a majority are not fully convinced either. This finding aligns with the fragmentation and inconsistency concerns raised by Gibson and Kumar (2023) and Zahir (2025), and it suggests that transparency and demonstrable auditability—which are associated with higher user trust (Cetin, 2024; Autili *et al.*, 2026)—may serve as important design priorities for converting "maybe" responses into firm adoption.

4.1.3 Access-control preferences: multi-party approval versus automatic access (RQ3)

Table 3 presents respondents' attitudes toward two distinct emergency access-control mechanisms: requiring multiple trusted contacts to approve access versus granting automatic access after prolonged account inactivity.

Table 3. Attitudes toward multi-party approval versus automatic inactivity-triggered access (n = 39)

Item	Response	n	%
Should a digital will system require multiple trusted people to approve access?	Yes	22	56.4%
	No	10	25.6%
	Not sure	7	17.9%
Should access be automatically granted to trusted contacts after long inactivity?	No	17	43.6%
	Yes	16	41.0%
	Maybe	6	15.4%

The comparison in Table 3 reveals the clearest contrast in the dataset relevant to system design. A clear majority (22 of 39, or 56.4%) supported requiring multiple trusted people to approve access, compared with only 10 (25.6%) opposed. By contrast, fully automatic access after inactivity—with no additional human approval step—was the plurality-rejected option (17 of 39, or 43.6%, answering "no" versus 16, or 41.0%, answering "yes"), reflecting a near-even split that leans slightly against automatic release. In other words, respondents in this sample were considerably more comfortable with a human, multi-party check on emergency access than with a purely automatic, inactivity-only trigger. This distinction is often collapsed in platform-level "legacy contact" designs (Section 2.4), yet our respondents evaluated the two mechanisms

Copyright © 2026 IJSECS

quite differently. Furthermore, a simple descriptive cross-tabulation of trust in a secure system (Table 2) against support for multi-party approval showed that preference for multi-party approval remained fairly consistent across trust levels (supported by 10 of 16 "yes-trust" respondents, 10 of 16 "maybe-trust" respondents, and 2 of 7 "no-trust" respondents). Given the small cell counts, we do not treat this distribution as a formally tested statistical association, but it is consistent with multi-party approval being valued somewhat independently of overall baseline trust in the system.

4.1.4 Feature and security-method preferences, and open-ended themes (RQ4)

Table 4 reports the results for the two multiple-select items examining trusted security methods and desired system features; because respondents could select more than one option, percentages are calculated against all 39 respondents and do not sum to 100%.

Table 4. Trusted security methods and desired system features, multiple selection permitted (n = 39; feature item n = 38 respondents, 1 left blank)

Item	Option	n	%
Security methods trusted most	Biometric authentication (fingerprint/face ID)	25	64.1%
	Two-factor authentication (OTP)	20	51.3%
	Passwords only	18	46.2%
	Security questions	5	12.8%
Important features in a digital will system	Encryption of documents	33	84.6%
	Strong password protection	29	74.4%
	Emergency access after inactivity	17	43.6%
	Activity monitoring (behavior tracking)	16	41.0%
	Audit logs (tracking system activities)	13	33.3%
	Trusted contacts system	13	33.3%

Encryption of documents (84.6%) and strong password protection (74.4%) were the two most frequently selected features, ranking well ahead of emergency access after inactivity (43.6%), activity monitoring (41.0%), audit logs (33.3%), and a trusted-contacts system (33.3%). This ordering indicates that, from the respondents' perspective, foundational data-protection mechanisms are valued more highly than the specialized inheritance-specific mechanisms (inactivity-triggered access and trusted contacts) that constitute the primary technical novelty of systems such as LegacyVault—an important, if humbling, design signal discussed further in Section 4.2. Regarding trusted authentication methods more broadly, biometric authentication was the most trusted single method (64.1%), ahead of two-factor authentication (51.3%) and passwords alone (46.2%). The two open-ended items (concerns about storing sensitive documents online and suggestions for improving digital security and inheritance systems) were manually reviewed and grouped into descriptive themes. Because a single response could reference more than one theme, and because one response (Respondent 1) restated the survey question rather than answering it and was therefore excluded from the thematic counts, the following percentages are illustrative rather than exhaustive. Concern about unauthorized access, hacking, or credential theft was the most prevalent theme, appearing in 18 of the 38 substantive concern responses (47.4%); privacy-related concerns (e.g., unauthorized individuals viewing personal documents) appeared in 4 responses (10.5%); explicit data-loss or data-breach concerns appeared in 4 responses (10.5%); legal or regulatory-compliance concerns appeared in 2 responses (5.3%); and 4 respondents (10.5%) explicitly stated that they had no concerns. Suggestions were more varied and less thematically concentrated, but recurring points included implementing stronger multi-factor and biometric authentication, sending periodic notification or confirmation prompts before an emergency trigger fires, limiting the number of trusted contacts, and integrating the system with formal legal recognition of digital wills. This final point echoes the legal-status gap identified by Harbinja (2017), emerging here from an end-user perspective rather than a legal-scholarship one.

4.2 Discussion

With respect to RQ1, which asked whether a gap exists between the perceived importance of digital assets and actual planning behavior, our data reveal a pronounced discrepancy: approximately three-quarters of respondents rated their digital assets as important or very important, yet fewer than one in eight had ever made a succession plan, a pattern that held even among those who rated their assets as "very important." This finding corroborates the general privacy and security intention–behavior gap documented outside the digital-legacy context (Barth & de Jong, 2017) as well as prior claims of widespread under-planning specifically for digital assets (Öhman & Watson, 2019; Bellamy *et al.*, 2018). For system designers, the practical implication is that a digital will management system cannot assume its target users arrive already motivated to plan; rather, user onboarding and communication strategies must actively close the awareness gap (for example,

Copyright © 2026 IJSECS

by directly informing users about what currently happens to unmanaged online accounts) instead of assuming that stated asset importance will translate into system adoption on its own.

Similarly, the results for RQ2—an even split between "yes" and "maybe" on system trust and a plurality of "maybe" responses on adoption intent—indicate that while most respondents in this sample are not opposed to the concept of a secure digital will system, they are not yet fully convinced of its trustworthiness. Combined with the qualitative finding that unauthorized access and hacking constituted by far the most frequently cited concern (Section 4.1.4), this pattern suggests that visible, explainable security controls—not merely the backend implementation of security, but a user's ability to observe and understand how protection works—may serve as the decisive lever for converting conditional trust into active adoption. This interpretation aligns with prior literature demonstrating that system transparency and auditability foster user trust when handling sensitive legal information (Cetin, 2024; Autili *et al.*, 2026).

Regarding access control and feature prioritization, RQ3's clearest finding is the asymmetry between support for multi-party approval (56.4% yes) and support for fully automatic inactivity-triggered access (41.0% yes versus 43.6% no, leaning against). Rather than treating multi-party approval and automatic release as interchangeable inactivity-handling mechanisms, as much of the platform-level "legacy contact" literature implicitly does (Section 2.4), designers should configure multi-party human approval as the more broadly acceptable default and offer automatic release as a secondary or opt-in mechanism, at least for user populations resembling our sample. Complementing this result, RQ4 provides a humbling signal for designers of inheritance-specific systems: respondents prioritized foundational protections (document encryption and password strength) well above the specialized inheritance mechanisms (inactivity triggers, trusted contacts, and audit logs) that represent the core technical novelty of systems such as LegacyVault. This ordering does not imply that inheritance-specific mechanisms are unneeded—indeed, the multi-party approval results in Table 3 demonstrate clear demand for structured emergency authorization—but it indicates that a digital will system's value proposition should lead with foundational security guarantees and frame inheritance-specific features as an extension of trusted, general-purpose document protection. Table 5 summarizes how the empirical findings in Section 4.1 address each of the four research questions posed in Section 2 and outlines their corresponding design implications.

Table 5. Summary of survey findings against the four research questions and their associated design implications

Research question	Key finding (n = 39)	Design implication
RQ1: Gap between perceived importance and planning behavior?	Yes — 76.9% rated digital assets important/very important; only 12.8% had made a plan	Onboarding should actively close the awareness gap rather than assume motivated users
RQ2: How much do respondents trust a secure digital-will system?	Conditional — 41.0% yes, 41.0% maybe, 17.9% no; adoption intent similarly split (53.8% maybe)	Visible, explainable security controls may convert conditional trust into firm trust
RQ3: Multi-party approval vs. automatic inactivity access?	Multi-party approval clearly preferred (56.4% yes) over automatic access (41.0% yes, 43.6% no)	Default to multi-party human approval; treat automatic release as secondary/opt-in
RQ4: Which security features are prioritized?	Encryption (84.6%) and password protection (74.4%) rank well above inheritance-specific features (33.3%–43.6%)	Lead product messaging with foundational security; frame inheritance features as an extension

4.3 Limitations

The findings reported above represent useful early design signals, and we have sought to interpret them proportionally rather than either dismissing them due to their small scale or overstating their generalizability. Nevertheless, seven methodological limitations should be read alongside every finding in Sections 4.1 and 4.2 rather than treated as a closing caveat. Specifically, 1) the study relies on a convenience sample rather than a probability sample: because respondents were recruited through the researchers' personal and academic networks rather than through random or stratified sampling, the sample cannot be assumed to represent any defined population, and self-selection bias (e.g., digitally engaged individuals being more willing to complete a security-related survey) cannot be ruled out; 2) the sample exhibits a severe age skew, with 38 of 39 respondents (97.4%) aged 18–24, meaning that the results describe the perceptions of a young, digitally active cohort and should not be extrapolated to older adults, who may hold different digital-asset profiles and attitudes toward succession planning; 3) due to the small sample size (n = 39), subgroup and cross-tabulated results (such as Section 4.1.1's importance-by-planning breakdown and Section 4.1.3's trust-by-multi-party-support breakdown) rest on small cell counts and are therefore reported strictly descriptively without inferential statistical testing; and 4) all items rely on self-report measures of perceptions and stated intentions (e.g.,

Copyright © 2026 IJSECS

"would you use") rather than observed behavior, and stated adoption intent is well documented in the technology-acceptance literature to over-predict actual usage. Furthermore, with respect to context and measurement, 5) recruitment occurred within a single institutional and social context: although the questionnaire did not record institutional affiliation directly, sharing the survey via personal and academic networks makes it likely that most respondents share a common environment, which may inflate response homogeneity beyond what the age distribution alone indicates; 6) the open-ended thematic groupings in Section 4.1.4 were derived through informal thematic coding via a single author's manual review rather than a multi-coder protocol with formal inter-rater reliability metrics, and thus represent an illustrative characterization of response content rather than a validated qualitative content analysis; and 7) no test–retest reliability or construct-validity assessment was conducted, as the instrument was purpose-built for this exploratory study and was not formally piloted or validated against an established psychometric scale, meaning that item-level measurement error cannot be excluded.

5. Conclusion and Recommendations

This paper reported a small-scale, exploratory survey (n = 39) examining user awareness, trust, and access-control preferences relevant to the design of digital-inheritance management systems. Despite its limited scale and skew toward young, digitally active respondents, the survey surfaced three findings with direct design relevance: 1) a substantial gap between the perceived importance of digital assets and actual succession-planning behavior; 2) conditional, rather than firm, trust in secure digital-will systems that appears closely linked to concerns about unauthorized access; and 3) a clear preference for multi-party human approval over fully automatic inactivity-triggered access, alongside a feature-priority ordering that places foundational encryption and password protection ahead of specialized inheritance mechanisms. These findings should be read strictly as descriptive evidence from a small, convenience-sampled group rather than as population-level claims; even so, they suggest concrete, testable design priorities—namely, leading with visible, foundational security guarantees, defaulting to multi-party rather than automatic emergency access, and actively addressing the awareness gap during user onboarding—that a future, larger-scale, and more representative study could confirm, refine, or overturn. We view the present study as an initial, honestly scoped data point toward that broader effort, and we encourage replication with larger and more demographically diverse samples, ideally including older adults, who arguably hold the most immediate stake in digital-inheritance planning.

More generally, we contend that systems-design papers in this domain benefit from reporting user-perception evidence with the same methodological transparency normally reserved for security or performance evaluations: stating sample size and recruitment procedures plainly, distinguishing descriptive observations from inferential claims, and explicitly flagging where findings may not generalize, rather than presenting convenience-sample survey results with the confidence of a controlled experiment. We hope that this paper's candid treatment of its methodological limitations proves at least as useful to future digital-legacy research as the specific empirical percentages reported in Section 4.

References

Autili, M., Corsi, R., De Sanctis, M., Inverardi, P., & Pelliccione, P. (2026). Ethics label for digital systems to promote transparency and user awareness. *Journal of Systems and Software*, *235*, 112752. https://doi.org/10.1016/j.jss.2025.112752

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bellamy, C., Arnold, M., Gibbs, M., & Nansen, B. (2018). Death, data, and digital legacy: Exploring the management of digital remains. *Information, Communication & Society*, *21*(3), 1–16. https://doi.org/10.1080/1369118X.2017.1348533

Bellamy, C., Arnold, M., Gibbs, M., Nansen, B., & Kohn, T. (2013). *Death and the Internet: Consumer issues for planning and managing digital legacies*. Australian Communications Consumer Action Network. https://www.craigbellamy.net/images/death.pdf

Copyright © 2026 IJSECS

Berwin, D. (2026, June 20). *Threshold signatures explained: How distributed key management works*. Silence Laboratories. https://silencelaboratories.com/blog/threshold-signatures-explained

Cetin, M. B. (2024). *Evaluating the effects of digital privacy regulations on user trust* [Master's thesis, Vrije Universiteit Amsterdam]. arXiv. https://arxiv.org/pdf/2409.02614

Gibson, D., & Kumar, R. (2023). Fragmented identity systems and challenges in cross-platform digital access management. *Journal of Information Security and Applications*, *68*, 103115. https://doi.org/10.1016/j.jisa.2022.103115

Hampo, J. A. C., Ngala, K. M., Tanyi, F. M. N., & Kpudzeka, B. N. (2026a). A behavioral risk-aware access control framework for secure digital legacy systems. *World Journal of Advanced Research and Reviews*, *31*(1), 868–882. https://doi.org/10.30574/wjarr.2026.31.1.1903

Hampo, J. A. C., Ngala, K. M., Tanyi, F. M. N., & Kpudzeka, B. N. (2026b). LegacyVault: A secure web-based digital will management system with multi-party verification and behavioral monitoring. *International Journal of Engineering and Computer Science*, *15*(7), 28820–28825. https://doi.org/10.18535/ijecs.v15i07.5619

Harbinja, E. (2017). *Legal aspects of the transmission of digital assets on death* [Doctoral dissertation, University of Strathclyde]. Strathclyde Theses Archive (STAX). https://stax.strath.ac.uk/concern/theses/k3569438f

Öhman, C., & Watson, D. (2019). Are the dead taking over Facebook? A big data approach to digital death. *Big Data & Society*, *6*(1), 1–13. https://doi.org/10.1177/2053951719842540

Paul, P., & Sinha, K. (2025). Multiparty authorization for secure data storage in cloud environments using improved attribute-based encryption. *Journal of Systems Engineering and Electronics*, *35*(4). https://doi.org/10.48550/arXiv.2512.23216

Zahir, R. M. (2025). *Cloud storage security: Risks and solutions*. Preprints. https://doi.org/10.20944/preprints202511.1778.v1

Zhao, X., Tan, W., Ye, Y., Ding, H., He, Z., & Zhu, M. (2026). Multi-party key authentication and agreement protocol for attribute access structures in industrial IoT. In *Proceedings of the 2026 5th International Conference on Cryptography, Network Security and Communication Technology (CNSCT '26)* (pp. 222–227). Association for Computing Machinery. https://doi.org/10.1145/3802927.3802961

Copyright © 2026 IJSECS