Buletin Ilmiah Sarjana Teknik Elektro
Vol. 7, No. 4, December 2025, pp. 955-979
ISSN: 2685-9572, DOI: 10.12928/biste.v7i4.14589

Cybersecurity and Privacy Governance in IoT-Enabled Social Work: A Systematic Review and Risk Framework

Yih-Chang Chen [1,3], Chia-Ching Lin [2]
[1] Department of Information Management, Chang Jung Christian University, Tainan 711, Taiwan
[2] Department of Finance, Chang Jung Christian University, Tainan 711, Taiwan
[3] Bachelor Degree Program in Medical Sociology and Health Care, Chang Jung Christian University, Tainan 711, Taiwan

ARTICLE INFORMATION

Article History:

Received 28 August 2025
Revised 03 November 2025
Accepted 04 December 2025

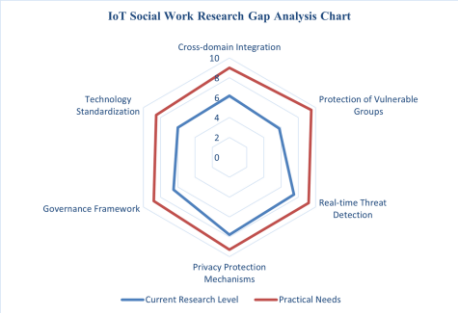
Keywords:

Internet of Things (IoT);
Social Work;
Cybersecurity;
Vulnerable Populations;
Governance Framework

Corresponding Author:

Yih-Chang Chen,
Department of Information Management, Chang Jung Christian University, Tainan 711, Taiwan.
Email: cheny@mail.cjcu.edu.tw

ABSTRACT



Social work practice is rapidly integrating Internet of Things (IoT) technologies to expand service delivery, yet this integration introduces significant cybersecurity and privacy vulnerabilities that disproportionately threaten vulnerable populations. Existing literature predominantly emphasizes technical security solutions while neglecting the ethical considerations, protective needs of vulnerable groups, and governance frameworks specific to social work contexts. Research Contribution: This study develops the first systematic multidimensional framework integrating engineering and social science perspectives to evaluate IoT cybersecurity, privacy risks, and governance requirements in social work applications. Using a Systematic Literature Review following PRISMA guidelines, we searched five major databases from January 2020 to September 2024. We employed qualitative thematic analysis combined with an innovative quantitative assessment algorithm to score technologies, threats, and governance components across 55 primary studies. Key Findings: Mental health services and vulnerable population support face "very high" privacy risks (PRS > 8.0), primarily from systemic infrastructure weaknesses in consumer-grade devices rather than sophisticated cyberattacks. Homomorphic encryption achieves the highest security score (9.8/10) but exhibits the highest implementation complexity (9.0/10). Federated learning provides an optimal balance (security 8.5, complexity 8.0, cost 6.0). Ethical guidelines demonstrate the highest implementation difficulty (8.2/10), reflecting challenges in translating abstract principles into technical specifications. Quantitative gap analysis identifies vulnerable population protection as the highest research priority (gap score 3.7/10). This study offers an evidence-driven agenda for practitioners and policymakers, proposing context-specific technology selection criteria and adaptive governance models that prioritize interdisciplinary collaboration, ensuring IoT advancements effectively promote social welfare while protecting at-risk individuals.

Document Citation:

Y.-C. Chen and C.-C. Lin, "Cybersecurity and Privacy Governance in IoT-enabled Social Work: A Systematic Review and Risk Framework," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 7, no. 4, pp. 955-979, 2025, DOI: 10.12928/biste.v7i4.14589.

1. INTRODUCTION

The swift progression and widespread adoption of Internet of Things (IoT) technologies are fundamentally transforming service delivery models and operational methodologies within the domain of social work. IoT applications encompass a broad spectrum of areas — including home care systems, community service platforms, monitoring devices for vulnerable populations, and mental health support tools — thereby presenting novel opportunities alongside intricate challenges for the field [1]-[4]. However, the growing prevalence of IoT devices in social services has concurrently intensified cybersecurity vulnerabilities and privacy concerns, posing significant risks to the rights and safety of service recipients [5]-[12].

1.1. Contextualizing IoT in Social Work: Vulnerability and Sensitivity

The implementation of IoT within social work is distinguished by unique characteristics that set it apart from general IoT applications. Primarily, service users often belong to vulnerable groups such as children, older adults, individuals with physical or mental disabilities, and those experiencing mental health conditions. These populations frequently demonstrate limited digital literacy, reduced awareness of privacy protections, and diminished capacity to advocate for their rights, rendering them especially susceptible to cyber threats and privacy violations [13]-[16]. Furthermore, social work routinely involves handling highly sensitive personal information — including health records, psychological evaluations, familial backgrounds, financial data, and behavioral histories. Breaches of such data can cause direct psychological and social harm to individuals, while simultaneously eroding public trust in social services and undermining institutional legitimacy. Empirical research has further documented the exacerbation of psychological harm when vulnerable individuals experience data breaches in connected healthcare and assistive technologies, particularly in contexts of intimate partner violence where data aggregation intensifies risk [14],[17].

1.2. Gaps in Existing Research

Despite extensive scholarly attention to IoT security and privacy in general contexts, there remains a marked deficiency of research specifically addressing the distinct needs of social work [18][19]. The extant literature predominantly concentrates on technical security solutions, with comparatively limited emphasis on ethical considerations relevant to social work practice, the protection of vulnerable populations, and the promotion of interdisciplinary collaboration. This lacuna has tangible practical implications: technically robust solutions may prove ethically unsuitable or operationally impracticable within social work settings [20]-[23]. Moreover, prevailing governance frameworks, largely derived from commercial or general public service domains, inadequately address the particular complexities inherent in social work — such as safeguarding dependent minors, fulfilling mandatory reporting obligations, and managing the inherent power asymmetries between professionals and service users [24]-[27].

1.3. Problem Statement and Justification

The imperative for this research is accentuated by several converging factors. The COVID-19 pandemic has accelerated digital transformation within social services, significantly increasing reliance on IoT technologies for remote care, health monitoring, and community-based support, with these modalities expected to persist beyond the immediate pandemic context [25],[28]-[31]. Concurrently, the frequency and sophistication of cyberattacks have escalated, heightening cybersecurity risks faced by social service organizations [32]-[35]. Additionally, emerging evidence concerning technology-enabled harm — particularly in intimate partner violence scenarios — illustrates how IoT data aggregation can concentrate power in the hands of abusers and commercial entities, disproportionately affecting vulnerable groups. Within this milieu, the development of a robust IoT security and privacy protection framework is both a necessary adaptation to technological evolution and a critical measure to safeguard the rights of vulnerable populations, embodying the principles of social equity and justice foundational to professional social work.

1.4. Research Contributions

This study offers several key contributions:

- **First**, it introduces the inaugural systematic, multidimensional analytical framework specifically designed to assess IoT security and privacy challenges within social work, thereby addressing a critical interdisciplinary gap bridging engineering technology and social sciences.
- **Second**, it presents transparent quantitative scoring methodologies for evaluating technical solutions, enabling practitioners and administrators to make contextually informed technology selection decisions with explicit clarity regarding weighting assumptions and evaluation procedures.

- **Third**, it proposes a comprehensive governance framework that integrates regulatory compliance, technical standards, and ethical considerations tailored explicitly to social work environments, acknowledging the distinctive protective responsibilities toward vulnerable populations inherent in social work practice.
- **Fourth**, it conducts a systematic gap analysis to identify and quantify research deficiencies, thereby establishing a data-driven research agenda with clearly prioritized areas for future investigation and highlighting domains requiring urgent attention.

Collectively, these contributions bridge the divide between rapid technological advancement and the protective imperatives of social work practice, offering both scholarly rigor and practical guidance.

2. METHODOLOGY

This study adopts a Systematic Literature Review (SLR) approach, rigorously adhering to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [36]. The principal aim is to conduct a comprehensive, impartial, and reproducible examination and synthesis of cybersecurity and privacy challenges, technical interventions, and governance frameworks relevant to IoT applications within the domain of social work. This methodological strategy addresses the limitations inherent in traditional narrative reviews by ensuring methodological rigor and enhancing the reliability of findings through a structured and transparent process.

2.1. Literature Search Strategy

To ensure the comprehensiveness and representativeness of the literature corpus, a multi-stage search strategy was implemented:

1. **Database Search:** Extensive searches were performed across five leading electronic academic databases selected to encompass diverse disciplinary perspectives: IEEE Xplore and ACM Digital Library (engineering and computer science); ScienceDirect and SpringerLink (interdisciplinary coverage); and PubMed (healthcare and biomedical literature). The temporal scope extended from January 2020 to September 2024, thereby capturing the most recent technological advancements, policy developments following the COVID-19 pandemic, and contemporary scholarly discourse.
2. **Justification for Temporal Scope:** The chosen five-year period reflects the post-COVID digital transformation era, recent regulatory changes (e.g., the UK Product Security & Telecommunications Infrastructure Act 2022, GDPR evolution), and mature research on IoT applications in healthcare and social services, while maintaining a manageable scope.
3. **Search Query Formulation:** Search queries were constructed using Boolean operators as follows: ("Internet of Things" OR "IoT" OR "Cyber-Physical Systems") AND ("social work" OR "social services" OR "vulnerable populations" OR "elderly care" OR "mental health" OR "community services" OR "child protection") AND ("security" OR "privacy" OR "cybersecurity" OR "data protection" OR "ethics" OR "governance"). Equivalent keyword combinations in Chinese were also incorporated to enhance inclusivity across academic traditions.
4. **Snowballing Techniques:** Both backward and forward snowballing methods were employed. Backward snowballing involved reviewing reference lists of selected studies, while forward snowballing utilized citation tracking tools (Google Scholar, Web of Science) to identify subsequent research citing key publications, thereby ensuring the inclusion of potentially overlooked but pertinent studies.

2.2. Study Selection Criteria and Quality Assessment

The screening process consisted of two sequential phases: initial title and abstract screening followed by full-text evaluation. Both phases were independently conducted by two researchers. Discrepancies were resolved through consensus discussions; if consensus was unattainable, a third reviewer rendered the final decision.

1. **Inclusion Criteria:** (1) Studies primarily focusing on the application of IoT technologies in social work or services targeting vulnerable populations; (2) Explicit consideration of cybersecurity, privacy, or related ethical issues; (3) Publications in peer-reviewed journals or leading international conferences with an h-index exceeding 50; (4) Clear articulation of research methodology supported by credible data or logical argumentation; (5) Publications in English or Chinese.
2. **Exclusion Criteria:** (1) Studies confined to theoretical technical discussions without practical application contexts; (2) Research with marginal relevance, such as general smart city analyses lacking a social work

focus; (3) Non-academic sources including news articles and commercial white papers; (4) Publications without accessible full texts; (5) Duplicate publications.

3. **Quality Assessment:** A customized version of the Critical Appraisal Skills Programme (CASP) checklist [37] was utilized to evaluate each included study. Assessment criteria encompassed clarity of research objectives, methodological appropriateness, rigor of study design, reliability of data collection and analysis, coherence between conclusions and evidence, and explicit consideration of vulnerable populations' perspectives. Studies rated as lower quality (CASP score below 12 out of 24) were assigned reduced weight during synthesis phases via sensitivity analysis, which confirmed the robustness of results despite ±20% weighting adjustments.

2.3. Data Extraction and Quantitative Framework Transparency

A structured data extraction tool was employed to systematically capture bibliographic information; research design; study populations or scenarios; core IoT technologies; identified security and privacy threats; proposed technical solutions; governance mechanisms; and principal research findings. The quantitative synthesis followed transparent procedures as outlined below:

1. **Data Value Extraction:** For each evaluated dimension (e.g., security efficacy of homomorphic encryption), research teams independently extracted values from the literature by recording explicit numeric data reported in empirical studies, tallying frequencies of cited advantages and disadvantages across studies, and extracting normalized performance benchmarks when available. Cross-validation between two coders ensured inter-rater reliability (Cohen's $\kappa > 0.75$).
2. **Standardization Method:** Original frequency data were normalized using min-max scaling to a 0–10 scale. Weighting coefficients were derived through expert elicitation involving four independent experts (two information security specialists and two social work scholars experienced with vulnerable populations), who rated the relative importance of components based on literature prevalence and practical impact. Final weights represent the mean of expert ratings, with sensitivity analysis confirming stability within ±0.2 weighting variance.
3. **Robustness Verification:** Sensitivity analyses assessed whether ±20% adjustments to weighting coefficients affected final technology rankings; no substantive changes in category assignments were observed, confirming result stability.

2.4. Technical Solution Evaluation Framework

The evaluation of technical solutions employed a multi-criteria decision analysis (MCDA) framework, establishing a comprehensive assessment system encompassing dimensions such as security efficacy, implementation complexity, cost-effectiveness, and applicability within resource-constrained social work environments [38][39]. Each technical solution was rated on a scale from 1 to 10 across each criterion, with weighted composite scores subsequently calculated. The analysis of governance frameworks utilized institutional analysis methodologies, examining both formal institutions (e.g., regulations, policies, standards) and informal institutions (e.g., cultural norms, ethical considerations, practical conventions) [40][41]. Comparative institutional analysis facilitated cross-national comparisons of governance models and identification of context-specific success factors. To enhance clarity, the methodological process is illustrated in Figure 1, which depicts the flow of information through the different phases of the review.

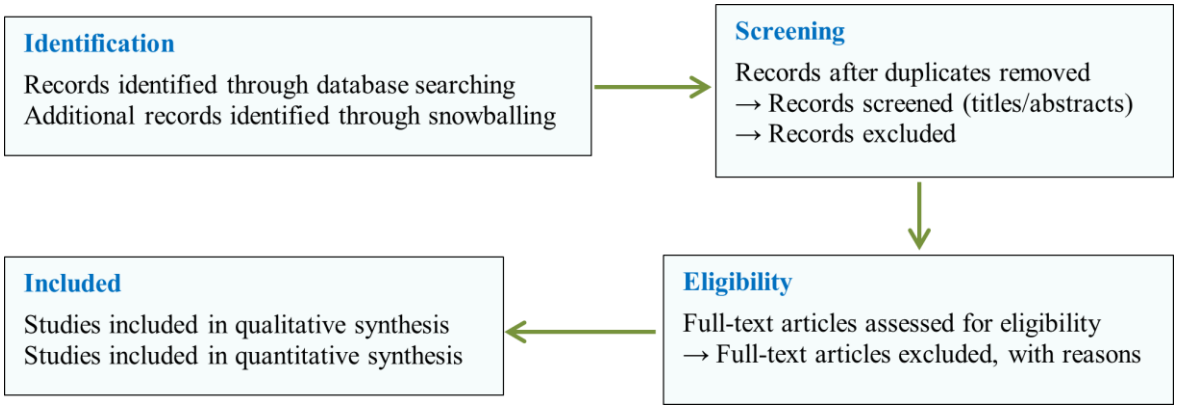


Figure 1. Research Methodology Flowchart - PRISMA

3. RESULTS AND DISCUSSION

3.1. Current IoT Applications in Social Work and the Corresponding Security Threat Landscape

3.1.1. Application Domains and Overview

A comprehensive literature review identified six primary domains in which Internet of Things (IoT) technologies have been integrated within social work practice: (1) home care, encompassing health monitoring and medication management; (2) community services, including location-based service delivery and behavioral analytics; (3) mental health support, such as mood tracking and crisis intervention; (4) services targeting vulnerable populations, involving cognitive assistance, behavioral monitoring, and facilitation of social connections; (5) long-term care, focusing on institutional care management and staff coordination; and (6) child protection, which involves activity monitoring and welfare tracking [1],[5],[42]-[47]. These implementations extend beyond the mere adoption of technology, encompassing complex and multifaceted risks inherently associated with the specific characteristics of each domain. A nuanced understanding of these interrelations is crucial to developing proportionate and effective security strategies.

3.1.2. Privacy Risk Assessment Framework and Results

Table 1 presents quantitative metrics derived from a systematic synthesis and multi-criteria evaluation of the reviewed literature. Qualitative risk levels — categorized as Very High, High, and Medium — are based on a semi-quantitative assessment framework that incorporates two principal dimensions:

1. Data Sensitivity (S_d): the extent and sensitivity of personal information collected, rated on a scale from 1 to 5.
2. Population Vulnerability (V_p): assessed by deficits in digital literacy and capacity for self-protection, also rated on a scale from 1 to 5.

The Privacy Risk Score (PRS) is calculated as follows:

$$PRS = w_s \cdot S_d + w_v \cdot V_p \quad (1)$$

where w_s and w_v are weighting coefficients, both set at 0.5 to reflect the equal importance of data characteristics and population vulnerability factors.

The values for S_d were obtained through content analysis of literature detailing the types of data collected (e.g., health metrics, behavioral patterns, social relationships), with sensitivity ratings assigned by an expert panel. The V_p values were derived from documented disparities in digital literacy and vulnerability characteristics of the populations studied, as reported in disability studies and gerontological research. The resulting PRS values correspond to qualitative categories as follows: Medium ($PRS \leq 5$), High ($5 < PRS \leq 8$), and Very High ($PRS > 8$). Detailed examination of Table 1 reveals significant differentiation across social work domains. Notably, mental health support and services for vulnerable groups both exhibit Very High privacy risk ratings despite differing levels of technical complexity. This apparent paradox can be explained by the fact that mental health systems involve higher technical complexity due to specialized monitoring hardware and real-time data processing requirements, whereas populations with limited digital literacy and reduced agency face elevated privacy risks through alternative pathways, such as an inability to recognize privacy violations and limited capacity to negotiate informed consent [48].

Table 1. Security Challenges Analysis of Application Areas

Application Area	Major Security Threats	Privacy Risk Rating	Technical Complexity	Scope of Impact
Home Care	Unauthorized device access, patient privacy breach	High	Medium	Individual
Community Services	Personal data leakage, location tracking	Medium	Low	Community
Mental Health Support	Theft of sensitive psychological data, tampering of treatment data	Very High	High	Individual
Services for Vulnerable Groups	Exposure of identification information, discriminatory attacks	Very High	High	Group
Long-term Care	Leakage of medical records, disruption of care services	High	Medium	Individual
Child Protection	Leakage of children's personal information, behavioral monitoring	Very High	Medium	Individual

Furthermore, child protection services demonstrate Very High privacy risks despite medium technical complexity. This reflects the inherent ethical tension between the obligation to monitor child welfare and the

respect for children's developing autonomy and future privacy interests — a dilemma that is distinctively social work-oriented and often absent from conventional technical security literature.

3.1.3. IoT Security Vulnerability Risk Assessment

Figure 2 depicts risk values across various layers of the IoT infrastructure. The assessment utilized a traditional information security risk model incorporating:

1. Likelihood of Exploitation (L_v): rated on a scale from 1 to 10, based on the frequency of reported vulnerabilities in the literature, accessibility of attack tools, and the technical complexity required to exploit them.
2. Impact Level (I_v): rated on a scale from 1 to 10, reflecting potential consequences such as individual privacy harm, disruption of service continuity, and damage to organizational reputation.

The overall Risk Value (RV) was computed using the Euclidean distance formula:

$$RV_v = \sqrt{L_v^2 + I_v^2} \tag{2}$$

This approach mitigates the disproportionate influence of extreme value combinations (e.g., very high impact coupled with very low likelihood), thereby providing a balanced representation of combined risk factors. The results were normalized to a 0-100 scale.

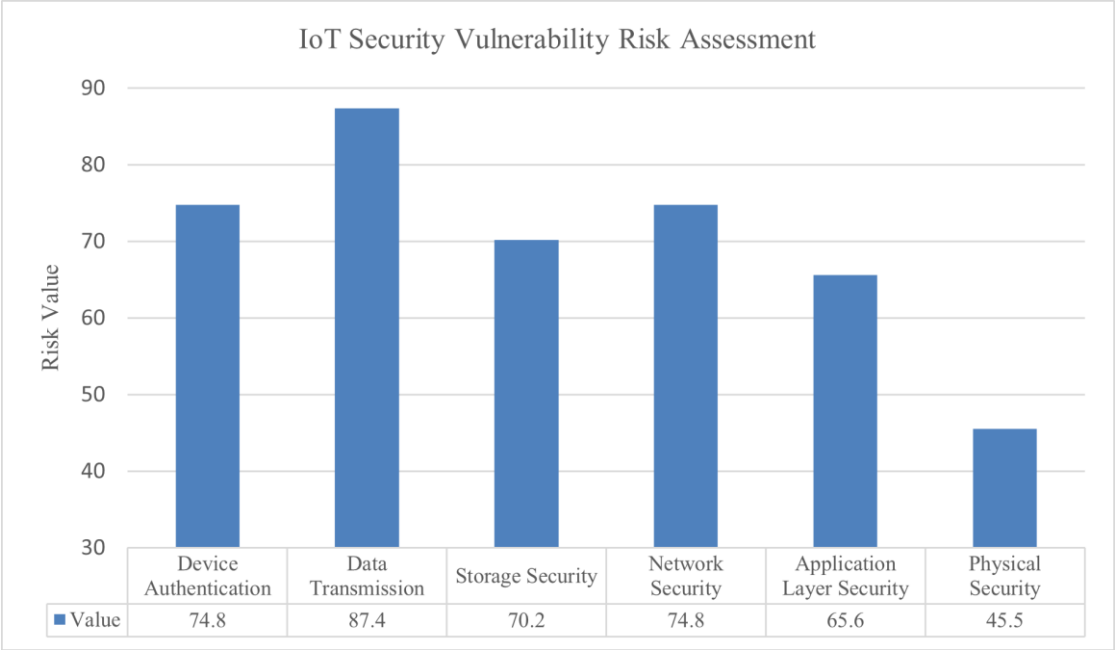


Figure 2. IoT Security Vulnerability Risk Assessment Chart

IoT applications in the realm of home care primarily include health monitoring devices, intelligent medical equipment, and environmental sensing technologies. The main security challenges stem from unauthorized access to devices and the potential exposure of patients' sensitive information [49]-[56]. Empirical studies reveal that more than 60% of IoT medical devices designed for domestic use suffer from fundamental security flaws, such as the use of default passwords and delays in firmware updates. Similarly, community service platforms that provide personalized services through methods like location tracking and behavioral analytics face risks related to personal data breaches and violations of location privacy [57]-[67].

Security concerns are especially pronounced in IoT applications supporting mental health, due to the highly sensitive nature of psychological health data involved. Research indicates that mental health monitoring devices routinely gather private information, including emotional states, behavioral patterns, and social interactions. Breaches of these devices can lead not only to privacy violations but also to adverse effects on patients' therapeutic progress and overall mental well-being [14],[24],[53],[68]-[72].

As outlined in Table 1, the risk scoring framework developed in this study categorizes privacy risk levels for mental health support and services aimed at vulnerable populations as "Very High." This classification

reflects both the inherent sensitivity of the data involved (e.g., emotional information, medical histories) and the structural disadvantages faced by these service users, particularly regarding digital literacy and limited negotiating power [13]-[16]. Malicious actors may exploit such data not only for theft but also to carry out discriminatory practices or social engineering attacks, thereby causing psychological and social harm that extends beyond financial loss [73]-[82].

The risk assessment results presented in Figure 2 provide a crucial insight: the predominant vulnerabilities are not advanced technical exploits in the traditional sense, but rather fundamental infrastructural weaknesses, such as inadequate device authentication and insecure data transmission. Over 60% of the reviewed literature highlights widespread issues including default passwords, unencrypted data transmissions, and the lack of timely firmware update mechanisms in consumer-grade IoT devices, including those used in social service settings [49]-[56]. This indicates that within the social work sector, many risks arise not from sophisticated zero-day attacks but from systemic vulnerabilities introduced by the deployment of "insecure-by-design" consumer products in high-risk environments. This finding poses significant challenges for the procurement policies of social service organizations and raises important ethical considerations for technology developers.

3.2. Comparative Assessment and Benchmarking of Technical Methodologies

In response to the previously identified security threats, the academic community has proposed a variety of advanced technical solutions. This section presents a multi-criteria comparative assessment of six leading-edge technologies: blockchain, homomorphic encryption, federated learning, differential privacy, zero-knowledge proofs, and secure multiparty computation [39],[83][84].

3.2.1. Evaluation Framework and Scoring Methodology

The quantitative evaluation score for each technology, denoted as S_{ij} under criterion (C_i), is calculated using the following formula:

$$S_{ij} = \alpha \cdot N_{pos} - \beta \cdot N_{neg} + \gamma \cdot P_{bench} \quad (3)$$

Where, N_{pos} represents the normalized frequency of positive contributions in the literature, scaled between 0 and 1. N_{neg} denotes the normalized frequency of reported negative effects, also scaled between 0 and 1. P_{bench} corresponds to normalized benchmark data derived from empirical studies, scaled between 0 and 1. α, β, and γ are weighting coefficients set at 0.5, 0.3, and 0.2 respectively, as determined through expert elicitation.

The rationale behind this formula is to integrate three critical dimensions of technology evaluation scholarly recognition of benefits, documented limitations, and empirical performance evidence. The relatively lower weight assigned to benchmark data (γ = 0.2) reflects the general paucity of empirical data for emerging technologies. Emphasizing both positive and negative scholarly attention ensures a balanced assessment, mitigating selection bias toward studies that highlight only successful outcomes. The weighting coefficients were established by consensus among an expert panel comprising information security specialists and social work scholars. Positive scholarly attention was accorded the highest weight (0.5) due to its indication of maturity and validation within the field. Documented limitations received a moderate weight (0.3), acknowledging the importance of critical evaluation. Empirical benchmarks were assigned a lower weight (0.2) in recognition of the limited availability of data specific to social work applications. The results of this multi-criteria analysis are summarized in Table 2. To further illustrate the trade-off between security performance and implementation complexity, Figure 3 provides a visual comparison of the evaluated technical solutions.

Table 2. Analysis of IoT Technical Solutions

Technical Solution	Security	Performance Impact	Implementation Complexity	Cost	Applicable Scenarios
Blockchain Technology	9.2	6.5	7.5	7.0	Data Integrity Verification
Homomorphic Encryption	9.8	4.2	9.0	8.5	Encrypted Computation
Federated Learning	8.5	7.8	8.0	6.0	Privacy-Preserving Training
Differential Privacy	8.0	8.5	6.5	5.5	Statistical Privacy
Zero-Knowledge Proof	9.5	5.8	8.8	8.0	Identity Authentication
Secure Multi-Party Computation	9.3	6.2	8.5	7.5	Multi-Party Collaboration

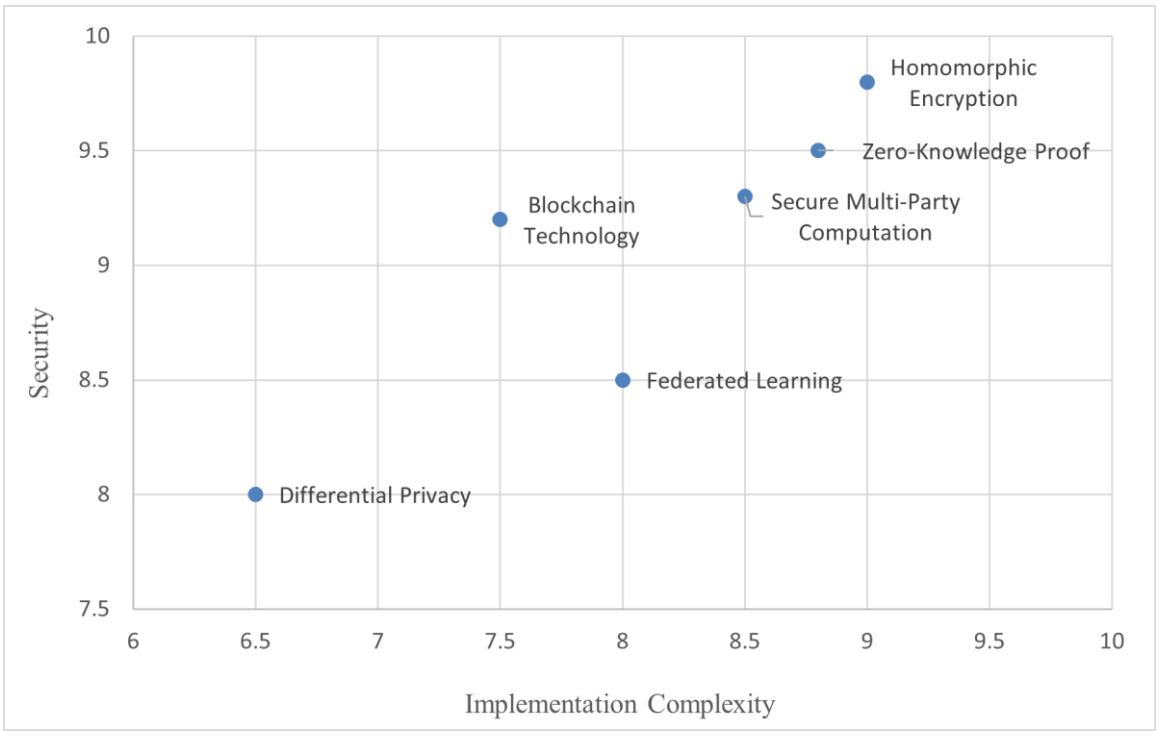


Figure 3. Technical Solution Performance-Complexity Analysis Chart

3.2.2. In-Depth Technical Solution Analysis with Implications for Social Work Applications

3.2.2.1. Homomorphic Encryption

Homomorphic encryption exhibits exceptional security performance, scoring 9.8 out of 10, by enabling computations on encrypted data without requiring decryption. This feature renders it particularly suitable for social work contexts that demand stringent protection of sensitive information, such as mental health records, histories of abuse, or family circumstances [83],[85][86]. However, significant limitations warrant explicit consideration. Homomorphic encryption demonstrates the highest implementation complexity (9.0/10) and imposes substantial computational overhead, markedly increasing system performance requirements. For social service organizations with limited IT infrastructure, this represents a considerable technical barrier. Current implementations incur performance overheads ranging from 100 to 1000 times that of unencrypted computations, rendering real-time processing of large datasets impractical [87]-[90]. Social Work Applicability: This technology is best suited for periodic batch processing of highly sensitive aggregated data — for example, annual statistical reporting on service outcomes — rather than real-time service delivery systems.

3.2.2.2. Zero-Knowledge Proof Technology

Zero-knowledge proofs achieve highly effective authentication, with a security score of 9.5, by enabling identity verification without disclosing underlying identifying information. This characteristic is especially advantageous in social service environments that require preservation of user identity privacy while ensuring accountability of service providers. Limitations include relatively high implementation complexity (8.8/10) and the necessity for specialized cryptographic expertise, which restricts accessibility primarily to large, well-resourced organizations. Additionally, emerging threats from quantum computing may compromise certain zero-knowledge proof schemes, necessitating ongoing cryptographic updates [91]-[95]. Social Work Applicability: Recommended for secure portal access by vulnerable service users and professionals, facilitating strong authentication without the need to store sensitive biometric identifiers.

3.2.2.3. Federated Learning Technology

Federated learning offers significant advantages for privacy-preserving collaborative machine learning, achieving a security score of 8.5 by enabling model training across multiple institutions without exchanging raw data. This approach is particularly relevant for data collaboration and analysis among multiple social service agencies. Its implementation complexity is moderate (8.0/10), and it incurs relatively low costs (6.0/10),

enhancing feasibility for deployment within resource-constrained social work sectors [96]-[104]. A novel consideration for social work is the explicit incorporation of ethical fairness constraints to prevent algorithmic bias against vulnerable populations. Models trained on federated data from multiple agencies may inadvertently amplify historical discrimination present in individual organizational datasets. Social Work Applicability: Highly recommended for multi-agency collaboration (e.g., child protective services, health, and education integration), enabling protective intelligence sharing while preserving individual client confidentiality.

3.2.2.4. Blockchain Technology

Blockchain technology effectively ensures data integrity verification, with a score of 9.2, by preventing tampering and forgery. This capability is critical for child protection records, court-related documentation, and treatment compliance verification, where data authenticity holds legal and therapeutic significance [105]. However, blockchain is characterized by high energy consumption and comparatively slow transaction speeds (e.g., Bitcoin processes approximately 7 transactions per second versus Visa's 65,000 transactions per second), posing scalability challenges for large-scale, real-time IoT deployments. For social work applications involving real-time care coordination, blockchain transaction latency may introduce unacceptable delays [84],[106]-[116]. Emerging solutions such as lightweight consensus mechanisms (e.g., Practical Byzantine Fault Tolerance) and sharding techniques show promise for IoT contexts [117], although research specific to social work applications remains limited. Social Work Applicability: Suitable for non-urgent, high-value records requiring immutable audit trails (e.g., consent documentation, incident reports) rather than for real-time monitoring systems.

3.2.2.5. Differential Privacy

Differential privacy technology offers theoretical advantages in statistical privacy protection, scoring 8.0, with relatively low implementation complexity (6.5/10) and moderate costs (5.5/10), thereby enhancing its feasibility for mainstream adoption. A persistent challenge lies in achieving an optimal balance between privacy budget allocation and data utility. Excessive consumption of the privacy budget diminishes analytical usefulness, whereas insufficient allocation risks privacy violations. This trade-off is particularly salient for social workers conducting needs assessments or outcome evaluations [118]-[123]. Social Work Applicability: Recommended for program evaluation and aggregate demographic reporting where individual-level accuracy is less critical than population-level insights.

3.2.2.6. Secure Multi-Party Computation

Secure multiparty computation enables multiple parties to jointly compute results without revealing individual inputs, achieving a security score of 9.3. This facilitates inter-organizational collaboration on sensitive matters, such as identifying children at risk across agency boundaries without disclosing individual identifiers. Its implementation complexity (8.5/10) and costs (7.5/10) position it between federated learning and homomorphic encryption in terms of accessibility.

3.2.3. Comparative Analysis Relative to Existing Literature

In contrast to Siddiqui and Alazzawi's [117] generic evaluation of IoT security technologies focused on consumer IoT sectors, the present study uniquely incorporates social work-specific implementation constraints, including limited IT capacity, vulnerable user populations, and legal reporting obligations, alongside ethical considerations such as fairness, dignity, and social justice. While Johnson et al.'s prior governance framework research provided general institutional analysis, this study specifies how formal governance mechanisms (e.g., regulations) and informal institutions (e.g., ethical codes, professional norms) distinctly influence technology adoption within social work contexts.

3.2.4. Synthesized Recommendations: Hybrid Technical Approaches

A key insight derived from this analysis is that no single technology constitutes a universally optimal solution. Instead, future developments should prioritize context-specific hybrid approaches that integrate multiple technologies. Exemplary Implementation Scenario: Multi-Institutional Child Protection Data Sharing

- Data Collection Phase (Resource Layer): Employ differential privacy techniques (complexity: 6.5/10; cost: 5.5/10) during initial data gathering from field social workers and institutional partners to minimize the collection of identifiable information at the outset.
- Model Training Phase (Collaborative Layer): Implement a federated learning framework (security: 8.5/10; complexity: 8.0/10) enabling multiple child protective service agencies to collaboratively train

predictive risk models on local, non-shared datasets. Each agency retains data on local servers, with only model parameters exchanged.

- Data Aggregation Phase (Privacy Layer): Reapply differential privacy techniques during parameter aggregation to ensure that global model updates do not reveal outlier patterns specific to any single agency.
- Critical Record Authentication (Integrity Layer): Utilize blockchain technology (security: 9.2/10) to immutably record high-stakes decisions (e.g., removal orders, placement changes), thereby maintaining an audit trail essential for legal accountability and longitudinal child outcome tracking.
- Access Control Phase (Authentication Layer): Deploy zero-knowledge proof technology to facilitate portal access for professionals and authorized family members, enabling identity verification without storing biometric identifiers.

Cost-Benefit Projection: This hybrid approach achieves comprehensive security across multiple dimensions — including privacy, integrity, authentication, and confidentiality — while maintaining moderate average implementation complexity (mean 7.6/10) and costs (mean 6.6/10). This represents a substantially more feasible solution compared to single-technology approaches such as homomorphic encryption, which exhibits higher complexity (9.0/10) and cost (8.5/10).

3.3. Analysis of Governance Framework Components

Effective governance of the IoT necessitates systematic consideration of six core components: regulatory compliance, technical standards, ethical guidelines, risk management, data management, and incident response. Each component exhibits unique attributes concerning its significance, implementation complexity, scope of applicability, and frequency of updates [124].

3.3.1. Detailed Assessment of Governance Framework Components

Table 3 presents a comprehensive evaluation of these governance components. The importance scores are derived from weighted metrics that reflect the prevalence and mandatory nature of provisions within key regulatory instruments — such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the UK Product Security and Telecommunications Infrastructure Act 2022 — as well as relevant standards like ETSI EN 303 645 and professional codes of ethics in social work. Implementation difficulty scores are based on the frequency and severity of documented challenges, including financial costs, technical complexity, interdepartmental coordination, and cultural resistance.

Table 3. Governance Framework Components Analysis

Governance Framework Component	Importance Score	Implementation Difficulty	Coverage Scope	Update Frequency
Regulatory Compliance	9.5	7.5	Comprehensive	Annually
Technical Standards	8.8	6.8	Technical Layer	Continuously
Ethical Guidelines	9.2	8.2	Comprehensive	Annually
Risk Management	9.0	7.0	Comprehensive	Quarterly
Data Management	8.7	6.5	Data Layer	Continuously
Incident Response	8.5	6.0	Operational Layer	Real-time

3.3.2. In-Depth Examination of Critical Components

3.3.2.1. Regulatory Compliance: Foundational Element or Illusory Assurance?

Regulatory compliance is widely regarded as the foundational pillar of governance frameworks, receiving the highest importance rating (9.5 out of 10). It primarily involves adherence to legal mandates such as GDPR, personal data protection laws, and health-related regulations analogous to HIPAA [125]-[127]. However, a critical paradox emerges: despite its paramount importance, regulatory compliance typically follows an annual update cycle, which lags significantly behind the rapid evolution of technical standards and the continuously emerging threat landscape. This temporal discrepancy engenders a “compliance trap,” wherein social service organizations may achieve formal regulatory compliance while deploying technologies that harbor novel vulnerabilities not yet encompassed by existing regulatory frameworks [17],[128]-[130].

For instance, GDPR requirements finalized in 2018 emphasize transparency in data collection and processing, as well as the protection of individual rights. Nevertheless, advanced technologies developed subsequently — such as homomorphic encryption, which enables computation on encrypted data, and federated learning, which facilitates distributed model training — introduce capabilities that create regulatory gaps.

These gaps allow technically compliant implementations to potentially facilitate new forms of privacy violations unforeseen by current regulations. In social work contexts, this challenge is further complicated by the involvement of dependent individuals (e.g., children or clients under court orders), whose data processing may be legally justified by protective mandates. This situation generates tension between regulatory privacy frameworks and professional obligations to safeguard vulnerable populations.

3.3.2.2. Ethical Guidelines: Translating Principles into Practice

Ethical guidelines hold particular prominence within social work, receiving a high importance rating (9.2 out of 10) due to their emphasis on foundational values such as human dignity, social justice, and non-maleficence [131]-[138]. Nonetheless, the translation of these abstract ethical principles into practical implementation poses significant challenges, as reflected by the highest implementation difficulty rating among all components (8.2 out of 10). This difficulty underscores the fundamental challenge of operationalizing ethical concepts into concrete technical specifications. The literature on value-sensitive design attempts to bridge this gap; however, the operationalization of principles such as "do no harm" into measurable fairness metrics within federated learning algorithms or the development of equitable privacy budget allocation strategies for differential privacy remains underdeveloped theoretically [139]-[143]. Specific ethical-technical tensions in social work IoT applications include:

- **Confidentiality versus Child Safety:** Home monitoring systems for at-risk children must balance respect for privacy with the need for welfare surveillance. Determining the threshold of behavioral anomalies that should trigger automated intervention alerts remains unresolved.
- **Autonomy versus Vulnerability:** The rights of elderly or cognitively impaired individuals to make independent decisions may conflict with paternalistic protective interventions enabled by monitoring technologies.
- **Equity versus Stigmatization:** Ensuring that vulnerable populations benefit from IoT applications without fostering a "surveillance society" that disproportionately targets marginalized groups.

These tensions lack definitive technical solutions and necessitate ongoing ethical deliberation within multidisciplinary teams.

3.3.2.3. Technical Standards: The Challenge of Innovation Outpacing Standardization

Technical standards play a crucial role in ensuring the security of IoT devices, with an importance rating of 8.8 out of 10. International security standards such as ETSI EN 303 645 and IEC 62443 have been established for consumer IoT devices. However, a significant limitation is that these standards address general IoT contexts and do not adequately account for the specific requirements of social work applications [144]-[151]. Notably absent are standards pertaining to:

- Data sensitivity classification schemes tailored to social work contexts
- Authentication mechanisms designed to accommodate users with cognitive or sensory disabilities
- Protocols for detecting fairness and bias in algorithmic decision-making related to child protection or care allocation
- Privacy-preserving techniques compatible with mandatory reporting obligations

3.3.3. Requirements for a Dynamic Governance Model

The foregoing analysis indicates that governance frameworks cannot remain static or solely compliance-driven. Instead, effective governance must be inherently dynamic and adaptive, incorporating the following elements [152]-[161]:

- **Rapid Feedback Mechanisms:** Implementing quarterly risk management reviews, as opposed to relying solely on annual regulatory updates, to facilitate timely identification of emerging vulnerabilities.
- **Standing Ethics Committee:** Establishing a multidisciplinary committee comprising technical experts, social workers, legal professionals, disability rights advocates, and service recipients to address ethical and social risks arising from emerging technologies not yet covered by existing regulations.
- **Continuous Standards Development:** Accelerating the development of standards that address social work-specific IoT requirements, potentially through participatory standard-setting processes involving practitioners.
- **Scenario Planning:** Proactively identifying and assessing the governance implications of emerging technological combinations — such as federated learning, differential privacy, and blockchain — prior to their deployment.

3.4. Research Limitations and Theoretical Contributions

3.4.1. Study Limitations

This investigation acknowledges several constraints that inherently affect the generalizability of its findings:

1. **Limitation 1:** Emerging Research Domain: The integration of IoT technologies within social work is an emergent field, characterized by a relatively limited corpus of empirical studies compared to broader IoT or healthcare informatics research. Although the 55 studies included herein represent a comprehensive survey of extant literature, this limited volume may restrict the empirical robustness of the conclusions drawn. This limitation is partially addressed through a hybrid qualitative-quantitative synthesis approach, which combines textual evidence with explicit scoring methodologies.
2. **Limitation 2:** Regulatory and Cultural Heterogeneity: Governance frameworks and contexts for IoT implementation vary considerably across different countries and regions. For instance, European contexts governed by the GDPR differ markedly from United States environments regulated under the HIPAA, as well as from social protection systems in the Global South. The framework proposed in this study emphasizes generic principles; however, users are advised to adapt its components to align with specific regulatory and cultural settings.
3. **Limitation 3:** Risk of Temporal Obsolescence: Given the rapid pace of technological advancement, some conclusions — particularly those related to technical solution rankings and standards recommendations — may become outdated within two to three years. This necessitates planned updates to the research and ongoing surveillance of emerging technologies.
4. **Limitation 4:** Language Scope: The search strategy prioritized publications in English and Chinese, potentially underrepresenting relevant research published in Spanish, Portuguese, or other languages. This limitation may restrict the inclusion of insights from social work contexts in the Global South.

3.4.2. Quantitative Gap Analysis Results

Table 4 presents a systematic identification and prioritization of research gaps. The gap scoring methodology is defined as follows:

The Current Research Level (L_R) is calculated by the formula:

$$L_R = k_1 \cdot \log\left(N_{pub}\right) + k_2 \cdot M_{index} \tag{4}$$

where N_{pub} denotes the number of publications within a specific research domain, M_{index} is a research maturity index on a scale from 1 to 5 reflecting the proportion of empirical studies, reviews, and theoretical frameworks, and k_1, k_2 are standardization coefficients used to normalize these components.

Table 4. Analysis of Research Gaps

Research Area	Current Research Level	Practical Needs	Research Gap	Priority Level
Cross-domain Integration	6.2	9.0	2.8	High
Protection of Vulnerable Groups	5.8	9.5	3.7	Very High
Real-time Threat Detection	7.5	9.2	1.7	Medium
Privacy Protection Mechanisms	7.8	9.3	1.5	Medium
Governance Framework	6.5	8.8	2.3	High
Technology Standardization	6.0	8.5	2.5	Medium

The Practical Needs (N_p) metric, ranging from 1 to 10, is derived through content analysis of social work organizational reports, policy documents, and literature references to "future challenges" or "practical difficulties." The Research Gap (G_R) is then computed as:

$$G_R = N_P - L_R \tag{5}$$

Priority levels are classified as Medium ($G_R < 2.0$), High ($2.0 \leq G_R < 3.0$), and Very High ($G_R \geq 3.0$). Interpretation of the gap analysis reveals a pronounced disparity between academic research focus and practical organizational needs across six research domains. Notably, the domain of "Protection of Vulnerable Groups" exhibits the largest gap score (3.7), indicating a significant deficiency in research despite urgent practical demand. This finding substantiates the prioritization recommendations outlined in subsequent sections. These research gaps are visually summarized in the chart presented in Figure 4.

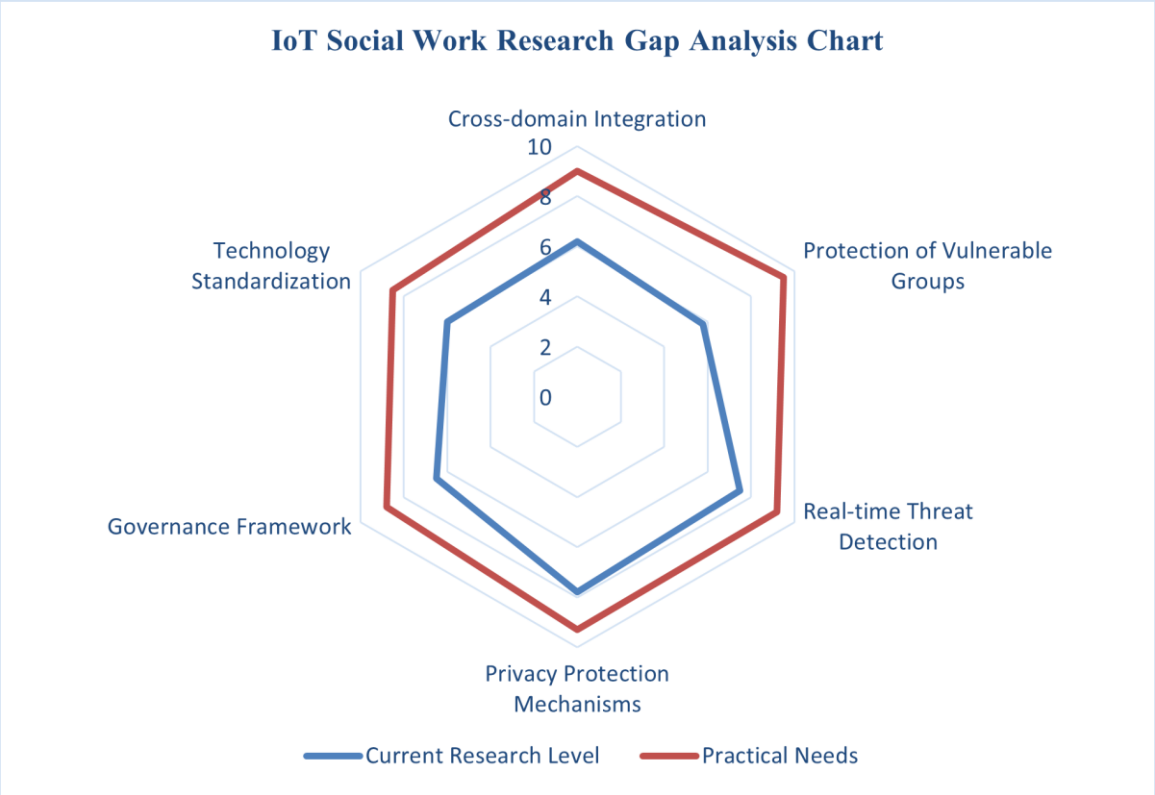


Figure 4. IoT Social Work Research Gap Analysis Chart

3.4.3. Theoretical Contributions

Despite the aforementioned limitations, this study advances the field through several key theoretical contributions:

1. **Contribution 1:** Inaugural Systematic Interdisciplinary Framework: This work constitutes the first systematic effort to develop a multidimensional analytical framework specifically designed to evaluate IoT security and privacy risks, technologies, and governance within the context of social work. The framework bridges a critical interdisciplinary gap by integrating engineering and social science perspectives, which have previously been addressed in isolation.
2. **Contribution 2:** Transparent Quantitative Synthesis Methodology: By explicitly detailing the quantitative assessment algorithms (Formula (1) to Formula (5)), the rationale for weighting, and the scoring procedures, this study offers a replicable methodological approach for future research endeavors. This transparency facilitates:
   - Reproduction of analyses with updated literature
   - Adaptation of methodologies to other professional domains such as nursing and education
   - Meta-evaluations assessing the robustness of the methodology
   - Critical scrutiny and methodological refinement
3. **Contribution 3:** Social Work-Specific Risk Taxonomy: Rather than employing generic cybersecurity risk frameworks, this study develops a taxonomy tailored to the unique characteristics of social work. This taxonomy accounts for factors such as dependent service users, mandatory reporting obligations, the dual imperatives of autonomy and safety, and the heightened risks of stigma.

3.5. Practical Implications and Contextualized Recommendations

3.5.1. Recommendations for Social Service Organizations

Social service organizations are advised to systematically enhance their cybersecurity posture by implementing the following measures:

1. **Comprehensive Cybersecurity Management Systems:** Appoint a dedicated cybersecurity officer with direct reporting lines to executive leadership. Conduct quarterly risk assessments utilizing the framework

outlined in Table 1 and Figure 2. Develop and enforce configuration management protocols for device firmware updates, addressing the critical deficiencies identified in Figure 2.

2. **Workforce Cybersecurity Awareness:** Mandate annual cybersecurity training for all personnel, emphasizing password hygiene, phishing detection, and incident reporting procedures. Provide specialized training for staff managing high-risk systems, such as mental health monitoring and child protection databases. Additionally, implement digital literacy programs for service users to enhance their capacity for informed consent.
3. **Technology Selection Criteria:** Favor contextually tailored combinations of security technologies, as discussed in Section 3.2.4, rather than relying on singular solutions. Require vendors to demonstrate compliance with ETSI EN 303 645 standards at a minimum, supplemented by privacy assessments specific to social work contexts. Prioritize technologies with lower implementation complexity (rated between 6.0 and 7.0) to accommodate organizational capacity constraints.
4. **Vulnerability Management:** Establish mechanisms to ensure timely firmware updates, potentially leveraging federated learning approaches to coordinate updates across multiple organizations. Conduct annual penetration testing of critical systems. Maintain incident response protocols with clearly defined escalation pathways to senior management and legal counsel.

3.5.2. Recommendations for Policymakers

Policymakers should consider the following actions:

1. **Accelerated Standards Development:** Commission the creation of social work-specific IoT security standards that address critical gaps identified in this study, including disability-accessible authentication methods, fairness assessment protocols for algorithmic decision-making in child protection and care allocation, privacy-preserving techniques compatible with mandatory reporting obligations, and vulnerability disclosure procedures suitable for resource-constrained organizations [124]. Foster government-industry-academia partnerships to facilitate participatory standard-setting processes that meaningfully incorporate social work expertise, moving beyond treating social work as a passive regulatory compliance domain. Transition from annual regulatory updates to quarterly governance review cycles to maintain alignment with evolving technical standards and threat landscapes.
2. **Regulatory Clarification and Enhancement:** Develop explicit guidance regarding the regulatory status of emerging technologies under existing frameworks such as GDPR and HIPAA equivalents. Clarify the implications of federated learning, differential privacy, homomorphic encryption, and zero-knowledge proofs, specifying whether these constitute additional safeguards or introduce novel compliance obligations. Establish clear legal frameworks to reconcile tensions between privacy regulations and mandatory reporting requirements — for example, determining whether differential privacy techniques that reduce data precision still satisfy child protection reporting thresholds. Institute breach notification requirements tailored to social work, including protocols for psychological harm assessment and victim support when data concerning vulnerable populations is compromised. Introduce safe harbor provisions for social service organizations that implement good-faith security measures in accordance with recommended frameworks, thereby mitigating litigation risks and encouraging proactive adoption [162].
3. **Resource Allocation and Implementation Support:** Provide targeted funding for digital infrastructure upgrades within social service organizations, recognizing that private-sector cost-sharing models are unsuitable for non-profit entities. Support workforce development through scholarships, certification programs, and knowledge-sharing networks to build internal cybersecurity expertise. Develop shared security infrastructures, such as government-supported secure cloud platforms incorporating federated learning and encrypted data repositories, to reduce individual implementation costs via economies of scale.

3.5.3. Recommendations for Technology Developers

Technology developers are encouraged to:

1. **Integrate Social Work-Specific Design Requirements:** Engage in participatory design processes that include social workers, service users, disability advocates, and family members from the outset, ensuring that technical designs reflect lived experiences, ethical considerations, and practical constraints. Incorporate accessibility-by-design principles to accommodate users with cognitive, sensory, or motor disabilities, addressing both ethical imperatives and practical necessities. Apply value-sensitive design frameworks to systematically translate social work ethical principles — such as dignity, justice, and non-maleficence — into technical specifications and design constraints, advancing beyond generic privacy-by-design approaches [163].

2. **Enhance Device Security and Manageability:** Commit to eliminating default credentials by requiring unique credential creation during device initialization prior to deployment. Implement secure firmware update mechanisms that support over-the-air updates with cryptographic integrity verification and rollback capabilities, thereby addressing the firmware update deficiencies identified in Section 3.1.C. Provide transparent, accessible security documentation that includes non-technical summaries of device security features, update procedures, and known limitations, tailored for social workers and administrators.
3. **Promote Interdisciplinary Collaboration:** Establish enduring partnerships with social work educational institutions and practitioner organizations to create feedback loops that ensure ongoing alignment between technological development and professional practice. Support open standards and interoperability to prevent vendor lock-in and maintain technological flexibility for social work organizations. Contribute resources and personnel to collaborative government-industry-academia initiatives focused on social work IoT standards development, recognizing this as a strategic investment in long-term market legitimacy.

3.6. Directions for Future Research

Figure 4 presents a radar chart delineating research gaps in IoT applications within social work, thereby providing a data-driven agenda for future scholarly inquiry.

3.6.1. Primary Priority: Protection of Vulnerable Groups

This domain exhibits the highest research gap score (3.7), reflecting a significant deficiency in targeted academic solutions despite urgent practical needs. Future research should focus on:

1. **Developing Adaptive Protection Mechanisms:** Advance beyond generic security models by creating context-specific technologies that accommodate the unique characteristics of vulnerable populations. Research areas include cognitive accessibility in security design — such as the functionality of multi-factor authentication for individuals with cognitive disabilities — and equity-aware fairness constraints for algorithmic decision-making in child protection IoT systems. Investigate trauma-informed technology design that balances necessary protection with the avoidance of re-traumatization, recognizing that surveillance-like monitoring can trigger adverse responses. Explore the integration of digital literacy support within IoT systems to embed protection mechanisms that require minimal user security expertise.
2. **Employing Participatory Design Methodologies:** Actively involve vulnerable populations — including children (with age-appropriate methods), individuals with disabilities, elderly service users, and family members — in design and evaluation processes. This approach transcends traditional accessibility compliance by embedding lived expertise throughout development. Particular attention should be given to managing representation and power dynamics to ensure that research findings authentically reflect participants' priorities rather than researcher assumptions. Conduct longitudinal implementation studies spanning two or more years to assess technology deployment effects on vulnerable populations, measuring both security outcomes and unintended consequences such as surveillance anxiety, autonomy reduction, and widening digital divides [125],[164][165].

3.6.2. Secondary Priorities: Cross-Domain Integration and Governance Frameworks

These areas demonstrate substantial research gaps (2.8 and 2.3, respectively). Future investigations should address:

1. **Cross-Domain Integration Research:** Move beyond disciplinary silos to establish integrated research platforms synthesizing perspectives from information engineering, social work, law, ethics, and organizational management. Key research questions include formalizing social work ethical principles — such as dignity, social justice, and non-maleficence — into computable constraints within federated learning, differential privacy, and related technical systems. Evaluate the operationalization of established value-sensitive design frameworks in practice [163]. Examine multi-agency data governance models that comply with legal mandates while maintaining technical feasibility and ethical appropriateness, including privacy-by-design specifications for child protective services data sharing. Investigate participatory standard-setting processes that meaningfully integrate social work expertise alongside technical expertise to develop standards that address genuine professional needs rather than generic compliance.
2. **Governance Framework Localization:** Conduct comparative analyses of IoT governance approaches across regions, such as GDPR-regulated Europe, HIPAA-influenced United States, and emerging South Asian social protection contexts, identifying transferable principles and context-specific requirements. Develop realistic organizational readiness assessments to evaluate social service organizations' capacity

to implement governance frameworks, including feasible timelines and resource needs based on organizational size and IT maturity. Explore governance adaptations suitable for underfunded social service organizations in low-resource settings, identifying minimal viable frameworks that provide meaningful protection while remaining implementable.

3.6.3. Tertiary Research Priorities

Additional important research areas warranting attention include:

1. **Real-Time Threat Detection** (Gap: 1.7): Although existing scholarship addresses this area, specific applications within social work remain underdeveloped. Research should investigate behavioral anomaly detection tailored to social work IoT contexts, differentiating "normal" device behavior across child protection monitoring, mental health support, and elderly care systems, while minimizing false positives that could trigger unwarranted interventions. Examine supply chain security challenges faced by social work organizations lacking procurement expertise, and develop mechanisms for supply chain transparency and device verification [166].
2. **Privacy Protection Mechanisms** (Gap: 1.5): Adapt emerging privacy-preserving techniques to social work contexts, including federated learning models that accommodate mandatory reporting obligations requiring individual-level data access. Investigate enforcement of fairness constraints across federated nodes. Explore methods for conducting privacy-preserving outcome evaluations — such as cost-per-outcome, client satisfaction, and service quality metrics — on encrypted or federated data without compromising analytical rigor.
3. **Technology Standardization** (Gap: 2.5): Prioritize rapid development of social work-specific technical standards within 12 to 24 months, contrasting with traditional multi-year cycles. Develop meaningful IoT security certification schemes that complement ETSI EN 303 645 standards and specifically address social work vulnerabilities and ethical considerations, enabling organizations to identify compliant solutions.

3.6.4. Methodological Recommendations for Future Research

Future research endeavors should:

1. Employ mixed-methods designs that integrate quantitative security assessments with qualitative phenomenological studies exploring service users' experiences of technology-enabled protection or surveillance.
2. Conduct pilot implementation studies involving at least two to three social work organizations to evaluate proposed frameworks in real-world settings, documenting implementation challenges and necessary adaptations prior to broader scaling.
3. Establish longitudinal tracking studies spanning multiple years to measure security outcomes, organizational transformations, and service recipient experiences, acknowledging that the effects of IoT governance manifest gradually.
4. Facilitate iterative theory development through successive refinement as empirical evidence accumulates, recognizing that IoT applications in social work constitute an emergent domain requiring dynamic theoretical frameworks rather than static hypothesis testing.

4. CONCLUSION

This systematic literature review introduces an innovative, multidimensional framework designed to address the complex cybersecurity and privacy challenges associated with the integration of IoT technologies within the field of social work. Distinct from the generalized application of frameworks derived from healthcare or smart city contexts, this study develops a tailored analytical perspective specific to social work by synthesizing technical, governance, and ethical considerations. The principal findings and their implications are elaborated below.

A key contribution of this research lies in delineating the threat landscape unique to social work. The analysis indicates that the predominant risks are not primarily attributable to advanced cyberattacks but rather to systemic infrastructural vulnerabilities. More than 60% of the reviewed studies highlight the widespread use of consumer-grade IoT devices characterized by "insecure-by-design" features — such as default passwords, unencrypted data transmission, and absence of firmware update capabilities — within critical professional settings. This insight shifts the focus of mitigation efforts from complex attack methodologies toward fundamental security practices. Additionally, the study proposes a social work-specific risk taxonomy that incorporates contextual variables, including service users' limited digital literacy and reduced capacity to provide informed consent. These factors elevate privacy risk assessments in domains such as mental health

services to a "Very High" category (Privacy Risk Score > 8.0). This vulnerability, rooted in the socio-economic and cognitive characteristics of the client population, represents a distinctive aspect of the social work environment.

In the evaluation of technical interventions, the findings caution against a uniform, "one-size-fits-all" strategy, advocating instead for a context-sensitive, hybrid approach. Although homomorphic encryption offers the highest level of security (rated 9.8/10), its considerable implementation complexity (9.0/10) limits its practicality for social service organizations with constrained resources. In contrast, federated learning emerges as a more balanced alternative, delivering robust privacy protection (8.5/10) alongside manageable implementation complexity (8.0/10), rendering it particularly appropriate for multi-agency collaborations. This analysis provides pragmatic guidance for organizations, emphasizing that optimal security outcomes — encompassing confidentiality, integrity, and availability — are best achieved through the integration of complementary technologies within feasible operational parameters.

The study further critically assesses governance frameworks, uncovering a paradox wherein formal regulatory compliance, typically characterized by slow, annual update cycles, fails to adequately safeguard against the rapid evolution of technological threats. The greatest challenge identified is not the adherence to technical standards but the translation of abstract ethical principles (rated 9.2/10 in importance) into concrete organizational policies and technical specifications. This finding underscores the imperative for governance mechanisms to be dynamic and adaptive rather than static and compliance-driven. To address this, the study advocates for the establishment of permanent, multi-stakeholder ethics committees — including technologists, social workers, legal experts, and service users — as a vital mechanism for navigating emergent ethical challenges.

Methodologically, this research contributes in two significant ways. First, it introduces a transparent and replicable quantitative assessment framework that facilitates critical evaluation of both technological solutions and governance models. Second, it pioneers a novel algorithm for systematically quantifying research gaps, thereby providing a data-driven foundation for prioritizing future scholarly inquiry. The analysis identifies the protection of vulnerable populations as the most pressing research gap (gap score: 3.7/10), warranting immediate academic attention.

The implications of this study are threefold, offering actionable recommendations for principal stakeholders. For social service organizations, it is advised to establish dedicated cybersecurity roles, conduct regular risk assessments, and prioritize technologies with moderate implementation complexity. Policymakers are encouraged to develop IoT security standards tailored specifically to social work, provide "safe harbor" provisions to incentivize responsible technology adoption, and allocate resources toward digital infrastructure and workforce development. For technology developers, the study calls for a paradigm shift toward participatory design and "ethics-by-design" approaches, embedding security and accessibility considerations from the outset in collaboration with social work professionals and their clients.

In conclusion, the responsible integration of IoT technologies within social work transcends a mere technical challenge, constituting an ethical imperative intimately connected to the profession's foundational mission of promoting social justice and safeguarding vulnerable populations. This study offers a foundational framework and delineates a clear research agenda to support this endeavor. It advocates for sustained, collaborative engagement among researchers, practitioners, policymakers, and technology developers to ensure that technological advancements uphold, rather than undermine, the fundamental rights and dignity of all individuals.

REFERENCES

[1] K. Hjelm and L. Hedlund, "Internet-of-Things (IoT) in healthcare and social services – experiences of a sensor system for notifications of deviant behaviours in the home from the users' perspective," *Health Informatics Journal*, vol. 28, no. 1, 2022, https://doi.org/10.1177/14604582221075562.

[2] H. Wan and K. Chin, "Exploring internet of healthcare things for establishing an integrated care link system in the healthcare industry," *International Journal of Engineering Business Management*, vol. 13, 2021, https://doi.org/10.1177/18479790211019526.

[3] L.-P. Hung, N.-C. Hsieh, L.-J. Lin, and Z.-J. Wu, "Using Internet of things technology to construct an integrated intelligent sensing environment for long-term care service," *International Journal of Distributed Sensor Networks*, vol. 17, 2021, https://doi.org/10.1177/15501477211059392.

[4] Liyakathunisa, A. Alsaeedi, S. Jabeen, and H. Kolivand, "Ambient Assisted Living Framework for Elderly Care Using Internet of Medical Things, Smart Sensors, and GRU Deep Learning Techniques," *Journal of Ambient Intelligence and Smart Environments*, vol. 14, no. 1, pp. 5-23, 2021, https://doi.org/10.3233/AIS-210162.

[5] P. Kourtesis, "A Comprehensive Review of Multimodal XR Applications, Risks, and Ethical Challenges in the Metaverse," *Multimodal Technologies and Interaction*, vol. 8, no. 11, p. 98, 2024, https://doi.org/10.3390/mti8110098.
[6] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-Assisted IoT Applications, Cybersecurity Threats, AI-Enabled Solutions, Open Challenges With Future Research Directions," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 4, pp. 4583-4605, 2024, https://doi.org/10.1109/TIV.2023.3309548.
[7] V. Bentotahewa, M. Yousif, C. Hewage, L. Nawaf, and J. Williams, "Privacy and Security Challenges and Opportunities for IoT Technologies During and Beyond COVID-19," in *Privacy, Security And Forensics in The Internet of Things (IoT)*, pp. 51-76, 2022, https://doi.org/10.1007/978-3-030-91218-5_3.
[8] M. V. K. Reddy, P. Chithaluru, P. Narsimhulu, and M. Kumar, "Security, privacy, and trust management of IoT and machine learning-based smart healthcare systems," *Advances in Computers*, vol. 137, pp. 141-174, 2025, https://doi.org/10.1016/bs.adcom.2024.06.006.
[9] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT — A Survey," *IEEE Access*, vol. 9, pp. 16849-16865, 2021, https://doi.org/10.1109/ACCESS.2021.3052850.
[10] S. Datta Burton, L. M. Tanczer, S. Vasudevan, S. Hailes, and M. Carr, "The UK code of practice for consumer IoT cybersecurity: where we are and what next," *The PETRAS National Centre of Excellence for IoT Systems Cybersecurity*, 2022, https://doi.org/10.14324/000.rp.10117734.
[11] L. Das, D. Singh, S. Vats, K. Taliyan, D. Bhargava, and D. Bhatnagar, "Smart Healthcare in Improving the Quality of Life: Revolutionizing with Application of IoT and Block Chain Technology," in *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, pp. 1-7, 2024, https://doi.org/10.1109/IC3SE62002.2024.10593009.
[12] T. Poleto, T. C. C. Nepomuceno, V. D. H. de Carvalho, L. C. B. d. O. Friaes, R. C. P. de Oliveira, and C. J. J. Figueiredo, "Information Security Applications in Smart Cities: A Bibliometric Analysis of Emerging Research," *Future Internet*, vol. 15, no. 12, p. 393, 2023, https://doi.org/10.3390/fi15120393.
[13] H. Lee, Y. Park, H. Kim, N. Kang, G. Oh, I. Jang, and E. Lee, "Discrepancies in Demand of Internet of Things Services Among Older People and People With Disabilities, Their Caregivers, and Health Care Providers: Face-to-Face Survey Study," *Journal of Medical Internet Research*, vol. 22, no. 4, p. e16614, 2020, https://doi.org/10.2196/16614.
[14] K. Assa-Agyei, F. Olajide, and A. Lotfi, "Security and Privacy Issues in IoT Healthcare Application for Disabled Users in Developing Economies," *Journal of Internet Technology and Secured Transactions*, vol. 10, no. 1, pp. 770-779, 2022, https://doi.org/10.20533/jitst.2046.3723.2022.0095.
[15] A. Zanella, F. Mason, P. Pluchino, G. Cisotto, V. Orso, and L. Gamberini, "Internet of things for elderly and fragile people," *arXiv preprint arXiv:2006.05709*, 2020, https://doi.org/10.48550/arXiv.2006.05709.
[16] E. Blasioli and E. Hassini, "e-Health Technological Ecosystems: Advanced Solutions to Support Informal Caregivers and Vulnerable Populations During the COVID-19 Outbreak," *Telemedicine and e-Health*, vol. 28, no. 2, pp. 138-149, 2021, https://doi.org/10.1089/tmj.2020.0522.
[17] S. Piasecki and J. Chen, "Complying with the GDPR when vulnerable people use smart devices," *International Data Privacy Law*, vol. 12, no. 2, pp. 113-131, 2022, https://doi.org/10.1093/idpl/ipac001
[18] S. Arisdakessian, O. A. Wahab, A. Mourad, H. Otrok, and M. Guizani, "A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4059-4092, 2023, https://doi.org/10.1109/JIOT.2022.3203249.
[19] M. Carr and F. Lesniewska, "Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance," *International Relations*, vol. 34, no. 3, pp. 391-412, 2020, https://doi.org/10.1177/0047117820948247.
[20] M. J. Carey and M. Taylor, "The impact of interprofessional practice models on health service inequity: an integrative systematic review," *Journal of Health Organization and Management*, vol. 35, pp. 682-700, 2021, https://doi.org/10.1108/JHOM-04-2020-0165.
[21] J. L. K. Murray, V. Hernandez-Santiago, F. Sullivan, et al., "Interprofessional Collaborative Practice in Health and Social Care for People Living with Multimorbidity: A Scoping Review Protocol," *Systematic Reviews*, vol. 14, p. 3, 2025, https://doi.org/10.1186/s13643-024-02730-x.
[22] D. J. Mallinson and S. Shafi, "Smart Home Technology: Challenges and Opportunities for Collaborative Governance and Policy Research," *Review of Policy Research*, vol. 39, no. 3, pp. 330-352, 2022, https://doi.org/10.1111/ropr.12470.
[23] K. Klode, A. Ringer, and B. Hølge-Hazelton, "Interprofessional and intersectoral collaboration in the care of vulnerable pregnant women: An interpretive study," *Journal of Interprofessional Care*, vol. 39, no. 4, pp. 599-608, 2020, https://doi.org/10.1080/13561820.2020.1761306.
[24] N. Tiffin, A. George, and A. E. LeFevre, "How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low-income and middle-income countries," *BMJ Global Health*, vol. 4, p. e001395, 2019, https://doi.org/10.1136/bmjgh-2019-001395.
[25] P. H. Cheong and P. Nyaupane, "Smart campus communication, Internet of Things, and data governance: Understanding student tensions and imaginaries," *Big Data & Society*, vol. 9, no. 1, 2022, https://doi.org/10.1177/20539517221092656.

[26] T. Hanjahanja-Phiri, M. Lotto, A. Oetomo, J. Borger, Z. Butt, and P. P. Morita, "Ethical considerations of public health surveillance in the age of the internet of things technologies: A perspective," *Digital Health*, vol. 10, 2024, https://doi.org/10.1177/20552076241296578.
[27] J. A. Martínez, J. L. Hernández-Ramos, V. Beltrán, A. Skarmeta, and P. M. Ruiz, "A user-centric Internet of Things platform to empower users for managing security and privacy concerns in the Internet of Energy," *International Journal of Distributed Sensor Networks*, vol. 13, no. 8, 2017, https://doi.org/10.1177/1550147717727974.
[28] A. Alexandru, M. Ianculescu, I. E. Giura, and F. Pop, "Managing Cybersecurity Threats for Seniors' Digital Needs Using Age-Friendly Remote Healthcare Monitoring Model," in *2022 E-Health and Bioengineering Conference (EHB)*, pp. 1-4, 2022, https://doi.org/10.1109/EHB55594.2022.9991316.
[29] K. Nordesjö and G. Scaramuzzino, "Digitalization, stress, and social worker–client relationships during the COVID-19 pandemic," *Journal of Social Work*, vol. 23, no. 6, pp. 1080-1098, 2023, https://doi.org/10.1177/14680173231180309.
[30] D. Huang, Y. Luo, and J. Lu, "Towards Digital Adaption: An Exploration of Chinese Social Workers' Experiences of Digital Service Challenges and Coping Strategies in the Context of COVID-19," *The British Journal of Social Work*, vol. 55, no. 1, pp. 45–64, 2025, https://doi.org/10.1093/bjsw/bcae125.
[31] L. Fiorini, E. Rovini, A. Sorrentino, O. Khalid, L. Coviello, L. Radi, L. Toccafondi, and F. Cavallo, "Can assistive technology support social services during Covid-19 emergency? Barriers and opportunities," *Int J Interact Des Manuf*, vol. 16, pp. 359–370, 2022, https://doi.org/10.1007/s12008-021-00836-3.
[32] A. Kumar and K. Sharma, "Digital Transformation and Emerging Technologies for COVID-19 Pandemic: Social, Global, and Industry Perspectives," in *Artificial Intelligence and Machine Learning for COVID-19*, vol. 924, 2021. https://doi.org/10.1007/978-3-030-60188-1_4.
[33] M. A. Habib *et al*., "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019, https://doi.org/10.1177/1550147719875653.
[34] N. Shirvanian, M. Shams, A. M. Rahmani, J. Lansky, S. Mildeova, and M. Hosseinzadeh, "The Internet of Things in Elderly Healthcare Applications: A Systematic Review and Future Directions," *IEEE Access*, vol. 13, pp. 71335-71373, 2025, https://doi.org/10.1109/ACCESS.2025.3562147.
[35] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023, https://doi.org/10.3390/s23156666.
[36] L. J. Ramirez Lopez, P. A. Buitrago Pineda, J. M. Perez Rincon, and W. M. Rojas Reales, "A systematic review on blockchain in electronic prescriptions and electronic medical records using PRISMA methodology in databases," *Informatics in Medicine Unlocked*, vol. 50, p. 101525, 2024, https://doi.org/10.1016/j.imu.2024.101525.
[37] H. A. Long, D. P. French, and J. M. Brooks, "Optimising the value of the critical appraisal skills programme (CASP) tool for quality appraisal in qualitative evidence synthesis," *Research Methods in Medicine & Health Sciences*, vol. 1, no. 1, pp. 31-42, 2020, https://doi.org/10.1177/2632084320947559.
[38] H. El-Sofany, S. A. El-Seoud, O. H. Karam, *et al.*, "Using machine learning algorithms to enhance IoT system security," *Scientific Reports*, vol. 14, p. 12077, 2024, https://doi.org/10.1038/s41598-024-62861-y.
[39] S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, "A Blockchain-based IoT Security Solution Using Multichain," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1105-1111, 2023, https://doi.org/10.1109/CCWC57344.2023.10099128.
[40] E. Korol and S. Korol, "Governing the Commons through Rule Hybridity: Interactions Between Formal Institutions and Informal Norms in CPR Management," *Journal of Business and Management Studies*, vol. 7, pp. 88-102, 2025, https://doi.org/10.32996/jbms.2025.7.4.4.
[41] H. Wang, W. Lu, J. Söderlund, and K. Chen, "The Interplay Between Formal and Informal Institutions in Projects: A Social Network Analysis," *Project Management Journal*, vol. 49, no. 4, pp. 20-35, 2018, https://doi.org/10.1177/8756972818781629.
[42] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," *Universal Access in the Information Society*, vol. 18, pp. 837–869, 2019, https://doi.org/10.1007/s10209-018-0618-4.
[43] I. de la Torre Díez, S. G. Alonso, S. Hamrioui, E. M. Cruz, L. M. Nozaleda, and M. A. Franco, "IoT-Based Services and Applications for Mental Health in the Literature," *J Med Syst*, vol. 43, no. 1, p. 11, 2018, https://doi.org/10.1007/s10916-018-1130-3.
[44] S. Y. Y. Tun, S. Madanian, and F. Mirza, "Internet of things (IoT) applications for elderly care: a reflective review," *Aging Clin Exp Res*, vol. 33, no. 4, pp. 855-867, 2021, https://doi.org/10.1007/s40520-020-01545-9.
[45] A. Carboni, D. Russo, D. Moroni, and P. Barsocchi, "Privacy by Design in Systems for Assisted Living, Personalised Care, and Wellbeing: A Stakeholder Analysis," *Frontiers in Digital Health*, vol. 4, p. 934609, 2023, https://doi.org/10.3389/fdgth.2022.934609.
[46] Y. Yamout, T. S. Yeasar, S. Iqbal, and M. Zulkernine, "Beyond smart homes: An in-depth analysis of smart aging care system security," *ACM Computing Surveys*, vol. 56, no. 2, pp. 1-35, 2023, https://doi.org/10.1145/3610225.
[47] C. H. E. N. Mengxuan, "Privacy Protection and Robocare in Long Term Care," *Revista Facultății de Drept Oradea*, vol. 1, no. 1, pp. 97-110, 2023, https://www.ceeol.com/search/article-detail?id=1327978.

[48] V. Fiorentino, M. Romakkaniemi, T. Harrikari, S. Saraniemi, and L. Tiitinen, "Towards digitally mediated social work - the impact of the COVID-19 pandemic on encountering clients in social work," *Qualitative Social Work*, vol. 22, no. 3, pp. 448-464, 2023, https://doi.org/10.1177/14733250221075603.
[49] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe, and A. Welhenge, "Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions," *Sustainability*, vol. 13, no. 21, p. 11645, 2021, https://doi.org/10.3390/su132111645.
[50] A. Chacko and T. Hayajneh, "Security and Privacy Issues with IoT in Healthcare," *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, no. 16, p. e4, 2018, https://doi.org/10.4108/eai.13-7-2018.155079.
[51] O. I. Obaid and S. Salman, "Security and Privacy in IoT-based Healthcare Systems: A Review," *Mesopotamian Journal of Computer Science*, pp. 46-55, 2022, https://doi.org/10.58496/MJCSC/2022/007.
[52] W. Shafik, "Smart biomedical devices for smart healthcare," in *Machine Learning Models and Architectures for Biomedical Signal Processing*, pp. 421-448, 2025, https://doi.org/10.1016/B978-0-443-22158-3.00017-X.
[53] M. N. H. Zarkia and S. Usman, "IoT Data Breaches and Privacy Issues in Healthcare System", *OIJI*, vol. 13, no. 1, pp. 41–55, 2025. https://doi.org/10.11113/oiji2025.13n1.327.
[54] P. Harvey, O. Toutsop, K. Kornegay, E. Alale, and D. Reaves, "Security and Privacy of Medical Internet of Things Devices for Smart Homes," in *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1-6, 2020, https://doi.org/10.1109/IOTSMS52051.2020.9340231.
[55] G. Nithyavani and G. Raja, "A Comprehensive Survey on Security and Privacy Challenges in Internet of Medical Things Applications: Deep Learning and Machine Learning Solutions, Obstacles, and Future Directions," *IEEE Access*, pp. 1-1, 2025, https://doi.org/10.1109/ACCESS.2025.3588489.
[56] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and Security Concerns in IoT-Based Healthcare Systems," in *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, pp. 101–122, 2021, https://doi.org/10.1007/978-3-030-75220-0_6
[57] R. Katsuya and X. M. Liu, "Policy and Management Implications of Firmware Vulnerabilities in Medical IoT Devices: A Multi-Case Analysis," *Journal of Science and Technology Policy Management*, 2025, https://doi.org/10.1108/JSTPM-09-2024-0346.
[58] L. Jedrzejczyk, B. A. Price, A. K. Bandara, and B. Nuseibeh, "I Know What You Did Last Summer: Risks of Location Data Leakage in Mobile and Social Computing," *Technical Report*, 2009, https://doi.org/10.21954/ou.ro.0001608c.
[59] C. M. Mejía-Granda, J. L. Fernández-Alemán, J. M. Carrillo-de-Gea, and J. A. García-Berná, "Security vulnerabilities in healthcare: an analysis of medical devices and software," *Med Biol Eng Comput*, vol. 62, no. 1, pp. 257-273, 2024, https://doi.org/10.1007/s11517-023-02912-0.
[60] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy Leakage of Location Sharing in Mobile Social Networks: Attacks and Defense," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 646-660, 2018, https://doi.org/10.1109/TDSC.2016.2604383.
[61] T. Bakhshi, B. Ghita, and I. Kuzminykh, "A Review of IoT Firmware Vulnerabilities and Auditing Techniques," *Sensors*, vol. 24, no. 2, Art. no. 708, 2024, https://doi.org/10.3390/s24020708.
[62] K. P. Tang, P. Keyani, J. Fogarty, and J. I. Hong, "Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06)*, 2006, pp. 93-102, https://doi.org/10.1145/1124772.1124788.
[63] S. Madanian, T. Chinbat, M. Subasinghage, D. Airehrour, F. Hassandoust, and S. Yongchareon, "Health IoT Threats: Survey of Risks and Vulnerabilities," *Future Internet*, vol. 16, no. 11, p. 389, Nov. 2024, https://doi.org/10.3390/fi16110389.
[64] A. Karanja, D. W. Engels, G. Zerouali, and A. Francisco, "Unintended Consequences of Location Information: Privacy Implications of Location Information Used in Advertising and Social Media," *SMU Data Science Review*, vol. 1, no. 3, p. 13, 2018, https://scholar.smu.edu/datasciencereview/vol1/iss3/13/.
[65] L. Baruh and M. Popescu, "Big data analytics and the limits of privacy self-management," *New Media & Society*, vol. 19, no. 4, pp. 579-596, 2015, https://doi.org/10.1177/1461444815614001.
[66] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey," *ACM Computing Surveys*, vol. 54, no. 1, p. 4, 2022, https://doi.org/10.1145/3423165.
[67] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, pp. 203–220, 2012, https://doi.org/10.1007/s11257-011-9110-z.
[68] L. J. Gutierrez, K. Rabbani, O. J. Ajayi, S. K. Gebresilassie, J. Rafferty, L. A. Castro, and O. Banos, "Internet of Things for Mental Health: Open Issues in Data Acquisition, Self-Organization, Service Level Agreement, and Identity Management," *Int J Environ Res Public Health*, vol. 18, no. 3, p. 1327, 2021, https://doi.org/10.3390/ijerph18031327.
[69] M. R. Abdmeziem and A. A. Nacer, "Leveraging IoT and LLM for Depression and Anxiety Disorders: A Privacy Preserving Perspective," *Security and Privacy*, vol. 8, no. 4, 2025, https://doi.org/10.1002/spy2.70061.
[70] E. S. N. Joshua, D. Bhattacharyya, and N. T. Rao, "Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: a complete systematic approach," in *Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems*, pp. 291-310, 2022, https://doi.org/10.1016/B978-0-323-90032-4.00007-9.

[71] C. Mehra and A. K. Sharma, "Safeguarding the Landscape of Mental Wellness: Analyzing Cyber Threats and Mitigation Strategies in Digital Healthcare," *Procedia Computer Science*, vol. 260, pp. 22-31, 2025, https://doi.org/10.1016/j.procs.2025.03.173.
[72] A. S. Malik, S. Acharya, and S. Humane, "Exploring the Impact of Security Technologies on Mental Health: A Comprehensive Review," *Cureus*, vol. 16, no. 2, p. e53664, 2024, https://doi.org/10.7759/cureus.53664.
[73] S. Sannon and A. Forte, "Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next," *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. CSCW2, p. 455, 2022, https://doi.org/10.1145/3555556.
[74] N. Warford, T. Matthews, K. Yang, O. Akgul, S. Consolvo, and P. G. Kelley, "SoK: A Framework for Unifying At-Risk User Research," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, pp. 2344-2360, https://doi.org/10.1109/SP46214.2022.9833643.
[75] T. Wilson, "The Unintended Harm of IoT Devices in Assistive Technology Distribution Programs," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 658-665, 2024, https://doi.org/10.1109/EuroSPW61312.2024.00080.
[76] Y. Zou, K. Sun, T. Afnan, R. Abu-Salma, R. Brewer, and F. Schaub, "Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, no. 1, pp. 133–150, 2024, https://doi.org/10.56553/popets-2024-0009.
[77] M. Pérez-Escolar and F. Canet, "Research on vulnerable people and digital inclusion: toward a consolidated taxonomical framework," *Universal Access in the Information Society*, vol. 22, pp. 1059–1072, 2023, https://doi.org/10.1007/s10209-022-00867-x.
[78] P. Phiayura, F. Hassandoust, and A. Liew, "Digital Safety and Vulnerable Groups: A Systematic Review of Barriers, Enablers, and Multi-Level Interventions," *The University of Auckland Business School Research Paper*, 2025, https://doi.org/10.2139/ssrn.5414835.
[79] K. Renaud and L. Coles-Kemp, "Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge," *SN Computer Science*, vol. 3, no. 346, 2022, https://doi.org/10.1007/s42979-022-01239-1.
[80] C. K. Sanders and E. Scanlon, "The Digital Divide Is a Human Rights Issue: Advancing Social Inclusion Through Social Work Advocacy," *Journal of Human Rights and Social Work*, vol. 6, no. 2, pp. 130–143, 2021, https://doi.org/10.1007/s41134-020-00147-9.
[81] U. Chibunna, O. Hamza, A. Collins, J. Onoja, A. Eweje, A. Daraojimba, and A. Pub, "Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 1, no. 1, pp. 125-138, 2020, https://doi.org/10.54660/.IJMRGE.2020.1.1.125-138.
[82] P. N. Rambharak, "Managing Technology Risk among Senior Citizens and People Living with Disabilities in Guyana," *Texila International Journal of Management*, vol. 11, no. 2, p. ART039, 2025, https://doi.org/10.21522/TIJMG.2015.11.02.ART039.
[83] B. Duc Manh, C.-H. Nguyen, D. Thai Hoang, D. N. Nguyen, M. Zeng, and Q.-V. Pham, "Privacy-Preserving Cyberattack Detection in Blockchain-Based IoT Systems Using AI and Homomorphic Encryption," *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 16478-16492, 2025, https://doi.org/10.1109/JIOT.2025.3535792.
[84] F. Fang, L. Feng, J. Xie, J. Liu, Z. Yuan, and X. Deng, "BCFL: A Trustworthy and Efficient Federated Learning Framework Based on Blockchain In IoT," in *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 2394-2399, 2024,https://doi.org/10.1109/CSCWD61410.2024.10580415.
[85] S. Ullah, J. Li, J. Chen, I. Ali, S. Khan, and M. T. Hussain, "Homomorphic Encryption Applications for IoT and Light-Weighted Environments: A Review," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 1222-1246, 2025, https://doi.org/10.1109/JIOT.2024.3472029.
[86] R. Hamza, A. Hassan, A. Ali, M. B. Bashir, S. M. Alqhtani, T. M. Tawfeeg, and A. Yousif, "Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms," *Entropy*, vol. 24, no. 4, p. 519, 2022, https://doi.org/10.3390/e24040519.
[87] A. Eleyan, H. Ahmed, and T. Bejaoui, "Leveraging A Deep Learning-Based Privacy Compliance Framework For IoT Applications," in *2025 5th IEEE Middle East and North Africa Communications Conference (MENACOMM)*, pp. 1-6, 2025, https://doi.org/10.1109/MENACOMM62946.2025.10911034.
[88] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," *ACM Computing Surveys*, vol. 51, no. 4, 2019, https://doi.org/10.1145/3214303.
[89] M. El-Hajj, A. E. Attar, A. Fadllallah, and R. Khatoun, "Securing Fault Diagnosis in IoT-Enabled Industrial Systems Using Homomorphic Encryption," in *2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 280-287, 2025, https://doi.org/10.1109/NTMS65597.2025.11076966.
[90] J. H. Cheon, D. Kim, and D. Kim, "Efficient Homomorphic Comparison Methods with Optimal Complexity," in *Advances in Cryptology – ASIACRYPT 2020*, pp. 241–270, 2020, https://doi.org/10.1007/978-3-030-64834-3_8.
[91] A. Szczegielniak-Rekiel, K. Kanciak, and J. M. Kelner, "Zero-Knowledge Proof in 5G and Beyond Technologies: State of the Arts, Practical Aspects, Applications, Security Issues, Open Challenges, and Future Trends," *IEEE Access*, vol. 13, pp. 138352-138380, 2025, https://doi.org/10.1109/ACCESS.2025.3596122.
[92] A. D. Dwivedi, R. Singh, U. Ghosh, and C. S. Rathore, "Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, pp. 4639–4649, 2022, https://doi.org/10.1007/s12652-021-03459-4.

[93] A. Khamesra, P. Selvaraj, and I. Singh, "Data Encryption in 6G Networks: A Zero- Knowledge Proof Model," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 577-585, 2024, https://doi.org/10.1109/I-SMAC61858.2024.10714853.
[94] A. T. Kudiwahove, "Authentication Model for KYC Optimization in Zimbabwean Businesses Implementing Zero Knowledge Proof for Enhanced Privacy and Secure Customer Onboarding," *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 14, no. 6, pp. 155-163, 2025, https://doi.org/10.47760/IJCSMC.2025.V14I06.016.
[95] S. Prabowo, A. G. Putrada, I. D. Oktaviani, M. Abdurohman, M. Janssen, and H. H. Nuha, "Privacy-Preserving Tools and Technologies: Government Adoption and Challenges," *IEEE Access*, vol. 13, pp. 33904-33934, 2025, https://doi.org/10.1109/ACCESS.2025.3540878.
[96] Y. Chen, X. Lin, G. Li, L. Chen, J. Wang, and S. Liao, "Trading Trust for Privacy: Socially-Motivated Personalized Privacy-Preserving Collaborative Learning in IoT," in *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 935-940, 2024, https://doi.org/10.1109/CSCWD61410.2024.10580732.
[97] T. Z. Sana, S. Abdulla, A. Nag, A. Das, M. M. Hassan, and Z. Z. Fiza, "Advancing Federated Learning: A Systematic Literature Review of Methods, Challenges, and Applications," *IEEE Access*, vol. 13, pp. 153817-153844, 2025, https://doi.org/10.1109/ACCESS.2025.3605165.
[98] R. Haripriya, N. Khare, and M. Pandey, "Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings," *Scientific Reports*, vol. 15, p. 12482, 2025, https://doi.org/10.1038/s41598-025-97565-4.
[99] Y. S. Narule and K. S. Thakre, "Privacy preservation using optimized Federated Learning: A critical survey," *Intelligent Decision Technologies*, vol. 18, no. 1, pp. 135-149, 2024, https://doi.org/10.3233/IDT-230104.
[100] S. S. Matta and M. Bolli, "Federated Learning for Privacy-Preserving Healthcare Data Sharing: Enabling Global AI Collaboration," *American Journal of Scholarly Research and Innovation*, vol. 04, pp. 320-351, 2025, https://doi.org/10.63125/jga18304.
[101] E. Nowell and S. Gallus, "Advancing Privacy-Preserving AI: A Survey on Federated Learning and Its Applications," *Preprints*, 2025, https://doi.org/10.20944/preprints202501.0685.v1.
[102] S. Pati *et al.*, "Privacy Preservation for Federated Learning in Health Care," *Patterns (N Y)*, vol. 5, no. 7, p. 100974, 2024, https://doi.org/10.1016/j.patter.2024.100974.
[103] F. EL-Husseini, H. N. Noura, and F. Vernier, "Security and privacy-preserving for machine learning models: attacks, countermeasures, and future directions," *Annals of Telecommunications*, 2025, https://doi.org/10.1007/s12243-025-01107-y.
[104] R. Haripriya, N. Khare, M. Pandey, and S. Biswas, "Navigating the fusion of federated learning and big data: a systematic review for the AI landscape," *Cluster Comput.*, vol. 28, no. 1, p. 303, 2025, https://doi.org/10.1007/s10586-024-05070-6.
[105] A. Syaefudin, N. A. Setiawan, and M. N. Rizal, "Blockchain Technology to Maintain Data Integrity: A Systematic Literature Review," in *2024 International Conference on Smart Computing, IoT and Machine Learning (SIML)*, 2024, pp. 303-308, https://doi.org/10.1109/SIML61815.2024.10578276.
[106] S. S. Sefati, R. Craciunescu, B. Arasteh, S. Halunga, O. Fratu, and I. Tal, "Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT)," *Smart Cities*, vol. 7, no. 5, pp. 2802-2841, 2024, https://doi.org/10.3390/smartcities7050109.
[107] H. Alshahrani, N. Islam, D. Syed, A. Sulaiman, M. S. Al Reshan, K. Rajab, A. Shaikh, J. Shuja-Uddin, and A. Soomro, "Sustainability in Blockchain: A Systematic Literature Review on Scalability and Power Consumption Issues," *Energies*, vol. 16, no. 3, p. 1510, 2023, https://doi.org/10.3390/en16031510.
[108] M. Hussain, M. Khairul, I. Bhuiyan, S. A. Sumon, S. Akter, M. Hossain, and A. Akther, "Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach," *Advances in Artificial Intelligence and Machine Learning*, vol. 4, no. 4, p. 2883, 2024, https://doi.org/10.54364/AAIML.2024.44168.
[109] I. S. Rao, M. L. Mat Kiah, M. M. Hameed, and Z. A. Memon, "Scalability of blockchain: a comprehensive review and future research direction," *Cluster Comput*, vol. 27, pp. 5547–5570, 2024, https://doi.org/10.1007/s10586-023-04257-7.
[110] B. L. Y. Quan, N. H. A. Wahab, A. Al-Dhaqm, A. Alshammari, A. Aqarni, and S. A. Razak, "Recent Advances in Sharding Techniques for Scalable Blockchain Networks: A Review," *IEEE Access*, vol. 13, pp. 21335-21366, 2025, https://doi.org/10.1109/ACCESS.2024.3523256.
[111] H. Lakhlef, T. Lerner, A. Kebir, N. El Atia, X. Du, and V. Ingardin, "Blockchain-Enabled SDN Solutions for IoT: Advancements, Discussions, and Strategic Insights," in *2024 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1-6, 2024, https://doi.org/10.1109/ISCC61673.2024.10733649.
[112] E. U. Haque, A. Shah, J. Iqbal, M. Al-Rakhami, A. Al-Qarni, and A. Gumaei, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Scientific Reports*, vol. 14, p. 7841, 2024, https://doi.org/10.1038/s41598-024-58578-7.
[113] T. Fernández-Caramés and P. Fraga-Lamas, "A Comprehensive Survey on Green Blockchain: Developing the Next Generation of Energy Efficient and Sustainable Blockchain Systems," *arXiv preprint arXiv:2410.20581*, 2024, https://doi.org/10.48550/arXiv.2410.20581.

[114] N. Khan, R. Mir, and M. A. Chishti, "BEFF-SIGS: blockchain-enhanced fog framework- securing IoT data integrity and green sustainability through scalable authentication-authorization," *International Journal of Computers and Applications*, vol. 47, pp. 1-19, 2024, https://doi.org/10.1080/1206212X.2024.2380654.
[115] T. A. Alghamdi, R. Khalid, and N. Javaid, "A Survey of Blockchain Based Systems: Scalability Issues and Solutions, Applications and Future Challenges," *IEEE Access*, vol. 12, pp. 79626-79651, 2024, https://doi.org/10.1109/ACCESS.2024.3408868.
[116] Z. Chen, X. Chen, and Y. Li, "Performance and Security Analysis of Distributed Ledger Under the Internet of Things Environments With Network Instability," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4213-4225, 2023, https://doi.org/10.1109/JIOT.2022.3216586.
[117] T. Siddiqui and S. S. B. Alazzawi, "Comparative Analysis of Internet of Things (IoT) Security Models," in *Advanced Informatics for Computing Research. ICAICR 2020*, pp. 177-188, 2021, https://doi.org/10.1007/978-981-16-3653-0_15.
[118] F. Liu, "Generalized Gaussian Mechanism for Differential Privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 4, pp. 747-756, 2019, https://doi.org/10.1109/TKDE.2018.2845388.
[119] L. Zhang, T. Zhu, P. Xiong, W. Zhou, and P. S. Yu, "More than Privacy: Adopting Differential Privacy in Game-theoretic Mechanism Design," *ACM Computing Surveys*, vol. 54, no. 7, p. 136, 2022, https://doi.org/10.1145/3460771.
[120] M. A. Husnoo, A. Anwar, R. K. Chakrabortty, R. Doss, and M. J. Ryan, "Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 153276-153304, 2021, https://doi.org/10.1109/ACCESS.2021.3124309.
[121] N. Phan, X. Wu, H. Hu, and D. Dou, "Adaptive Laplace Mechanism: Differential Privacy Preservation in Deep Learning," in *2017 IEEE International Conference on Data Mining (ICDM)*, pp. 385-394, 2017, https://doi.org/10.1109/ICDM.2017.48.
[122] H. Liu, Z. Wu, Y. Zhou, C. Peng, F. Tian, and L. Lu, "Privacy-Preserving Monotonicity of Differential Privacy Mechanisms," *Applied Sciences*, vol. 8, no. 11, p. 2081, 2018, https://doi.org/10.3390/app8112081.
[123] N. Holohan, S. Antonatos, S. Braghin, and P. M. Aonghusa, "The Bounded Laplace Mechanism in Differential Privacy," *Journal of Privacy and Confidentiality*, vol. 10, no. 1, pp. 1-28, 2019, https://doi.org/10.29012/jpc.715.
[124] A. Sedrati, A. Mezrioui, and A. Ouaddah, "IoT-Gov: A structured framework for internet of things governance," *Computer Networks*, vol. 233, p. 109902, 2023, https://doi.org/10.1016/j.comnet.2023.109902.
[125] S. Piasecki, "Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons," *Information & Communications Technology Law*, vol. 32, no. 3, pp. 385-417, 2023, https://doi.org/10.1080/13600834.2023.2231326.
[126] G. Malgieri and J. Niklas, "Vulnerable data subjects," *Computer Law & Security Review*, vol. 37, 105415, 2020, https://doi.org/10.1016/j.clsr.2020.105415.
[127] J. Breuer, R. Heyman, and R. van Brakel, "Data protection as privilege — Factors to increase meaning of GDPR in vulnerable groups," *Frontiers in Sustainable Cities*, vol. 4, 2022, p. 977623, https://doi.org/10.3389/frsc.2022.977623.
[128] Anupriya and K. D. Singh Chauhan, "Securing informational privacy in India's IoT governance: Looking through the lens of FASTag," *Journal of Data Protection & Privacy*, vol. 7, no. 2, 2025, https://doi.org/10.69554/UBZH7994.
[129] G. Georgiadis and G. Poels, "Establishing a Comprehensive Data Protection Impact Assessment Methodology for Big Data Analytics in Compliance with the General Data Protection Regulation," *Research Square*, 2025, https://doi.org/10.21203/rs.3.rs-5821174/v1.
[130] M. Choroszewicz and B. Mäihäniemi, "Developing a Digital Welfare State: Data Protection and the Use of Automated Decision-Making in the Public Sector across Six EU Countries," *Global Perspectives*, vol. 1, no. 1, p. 12910, Mar. 2020, https://doi.org/10.1525/gp.2020.12910.
[131] Y.-C. Chen and C.-C. Lin, "The Role of Social Work in the Construction of Smart Cities: Practices and Prospects of Digital Services", *Digital Technol. Res. Appl.*, vol. 4, no. 2, pp. 109–124, 2025, https://doi.org/10.54963/dtra.v4i2.1301.
[132] B. Mittelstadt, "Ethics of the health-related internet of things: a narrative review," *Ethics and Information Technology*, vol. 19, no. 3, pp. 157–175, 2017, https://doi.org/10.1007/s10676-017-9426-4.
[133] F. Reamer, "Artificial Intelligence in Social Work: Emerging Ethical Issues," *International Journal of Social Work Values and Ethics*, vol. 20, pp. 52-71, 2023, https://doi.org/10.55521/10-020-205.
[134] A. R. Garcia, "AI, IoT, Big Data, and Technologies in Digital Economy with Blockchain at Sustainable Work Satisfaction to Smart Mankind: Access to 6th Dimension of Human Rights," in *Smart Governance for Cities: Perspectives and Experiences*, pp. 85–100, 2020, https://doi.org/10.1007/978-3-030-22070-9_6.
[135] A. Shahraki and Ø. Haugen, "Social ethics in Internet of Things: An outline and review," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 509-516, 2018, https://doi.org/10.1109/ICPHYS.2018.8390757.
[136] R. P. Pradhan, A. K. Sarangi, and A. Sabat, "The effect of ICT development on innovation: evidence from G-20 countries," *Eurasian Econ Rev*, vol. 12, pp. 361-371, 2022, https://doi.org/10.1007/s40822-021-00189-y.
[137] H. Bangui, B. Buhnova, and M. Ge, "Social Internet of Things: Ethical AI Principles in Trust Management," *Procedia Computer Science*, vol. 220, pp. 553-560, 2023, https://doi.org/10.1016/j.procs.2023.03.070.
[138] S. Tzafestas, "Ethics and Law in the Internet of Things World," *Smart Cities*, vol. 1, pp. 98-120, 2018, https://doi.org/10.3390/smartcities1010006.

[139] F. G. Reamer, "Clinical Social Work in a Digital Environment: Ethical and Risk-Management Challenges," *Clinical Social Work Journal*, vol. 43, pp. 120–132, 2015, https://doi.org/10.1007/s10615-014-0495-0.
[140] F. G. Reamer, "Social Work in a Digital Age: Ethical and Risk Management Challenges," *Social Work*, vol. 58, no. 2, pp. 163–172, 2013, https://doi.org/10.1093/sw/swt003.
[141] A. Rodríguez-Martínez, M. T. Amezcua Aguilar, J. Cortés Moreno, and J. J. Jiménez-Delgado, "Ethical Issues Related to the Use of Technology in Social Work Practice. A Systematic Review," *SAGE Open*, vol. 14, no. 3, 2024, https://doi.org/10.1177/21582440241274842.
[142] A. M. L. Taylor-Beswick, "Digitalizing social work education: preparing students to engage with twenty-first century practice need," *Social Work Education*, vol. 42, no. 1, pp. 44-64, 2023, https://doi.org/10.1080/02615479.2022.2049225.
[143] E. Beaumont, P. Chester, and H. Rideout, "Navigating Ethical Challenges in Social Media: Social Work Student and Practitioner Perspectives," *Australian Social Work*, vol. 70, no. 2, pp. 221–228, 2017, https://doi.org/10.1080/0312407X.2016.1274416.
[144] F. Körner, "Current challenges of implementing ETSI EN 303 645 as a baseline security standard for consumer IoT security certification," *TechRxiv*, 2023, https://doi.org/10.36227/techrxiv.24711672.
[145] N. U. Prince, M. A. A. Mamun, A. Olajide, O. Khan, A. Akeem, and A. Sani, "IEEE Standards and Deep Learning Techniques for Securing Internet of Things (IoT) Devices Against Cyber Attacks", *Journal of Computational Analysis and Applications (JoCAAA)*, vol. 33, no. 07, pp. 1270–1289, 2024, https://eudoxuspress.com/index.php/pub/article/view/1210.
[146] O. K. Greuter and D. K. Sarmah, "The Baseline of Global Consumer Cyber Security Standards for IoT: Quality Evaluation," *Journal of Cyber Security Technology*, vol. 6, no. 4, pp. 175–200, 2022, https://doi.org/10.1080/23742917.2022.2105192.
[147] F. Casarosa, "Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework," *Computer Law & Security Review*, vol. 53, 105982, 2024, https://doi.org/10.1016/j.clsr.2024.105982.
[148] R. Kaksonen, K. Halunen, M. Laakso, and J. Röning, "Automating IoT Security Standard Testing by Common Security Tools," in *Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP*, pp. 42-53, 2024, https://doi.org/10.5220/0012345900003648.
[149] B. Sereda and J. Jaskolka, "An Evaluation of IoT Security Guidance Documents: A Shared Responsibility Perspective," *Procedia Computer Science*, vol. 201, pp. 281-288, 2022, https://doi.org/10.1016/j.procs.2022.03.038.
[150] E. M. Kalogeraki and N. Polemi, "A taxonomy for cybersecurity standards," *Journal of Surveillance, Security and Safety*, vol. 5, pp. 95-115, 2024, https://doi.org/10.20517/jsss.2023.50.
[151] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," *Computers*, vol. 14, no. 2, p. 61, 2025, https://doi.org/10.3390/computers14020061.
[152] K. Bližnák, M. Munk, and A. Pilková, "A Systematic Review of Recent Literature on Data Governance (2017–2023)," *IEEE Access*, vol. 12, pp. 149875-149888, 2024, https://doi.org/10.1109/ACCESS.2024.3476373.
[153] M. R. C. Santos and R. M. S. Laureano, "Developing a Vulnerability-Based Conceptual Model for Managing Risk in Non-Profit Projects: A Multicase Study in a European Country," *Public Management Review*, vol. 25, no. 2, pp. 313-339, 2021, https://doi.org/10.1080/14719037.2021.1972685.
[154] C. Oko-Odion and A. Omogbeme, "Risk management frameworks for financial institutions in a rapidly changing economic landscape," *International Journal of Science and Research Archive*, vol. 14, no. 01, pp. 1182–1204, 2025, https://doi.org/10.30574/ijsra.2025.14.1.0155.
[155] L. Dominelli, *Social work practice during times of disaster: A transformative green social work model for theory, education and practice in disaster interventions*. Routledge. 2023, https://doi.org/10.4324/9781003105824.
[156] R. Napitupulu, R. Sukmana, and A. Rusydiana, "Governance of Islamic social finance: learnings from existing literature," *International Journal of Islamic and Middle Eastern Finance and Management*, vol. 17, pp. 523-541, 2024, https://doi.org/10.1108/IMEFM-06-2023-0222.
[157] T. Sim, M. He, and L. Dominelli, "Social Work Core Competencies in Disaster Management Practice: An Integrative Review," *Research on Social Work Practice*, vol. 32, no. 3, pp. 310-321, 2022, https://doi.org/10.1177/10497315211055427.
[158] P.-J. Schweizer and S. Juhola, "Navigating systemic risks: governance of and for systemic risks," *Global Sustainability*, vol. 7, p. e38, 2024, https://doi.org/10.1017/sus.2024.30.
[159] L. Brown and S. P. Osborne, "Risk and Innovation: Towards a framework for risk governance in public services," *Public Management Review*, vol. 15, no. 2, pp. 186–208, 2012, https://doi.org/10.1080/14719037.2012.707681.
[160] A. Brown, D. Harkin, and L. M. Tanczer, "Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design," *Violence Against Women*, vol. 31, no. 5, pp. 1039-1062, 2024, https://doi.org/10.1177/10778012231222486.
[161] E. Giorgi, "How Technology Devices Can Help or Harm Vulnerable Communities in Technocene. Issues for Designers, Architects, and Policy Makers," in *Design for Vulnerable Communities. The Urban Book Series*, pp. 15-28, 2022, https://doi.org/10.1007/978-3-030-96866-3_2.
[162] G. Kołaczek, "Internet of Things (IoT) Technologies in Cybersecurity: Challenges and Opportunities," *Applied Sciences*, vol. 15, no. 6, p. 2935, 2025, https://doi.org/10.3390/app15062935.

[163] B. Friedman and D. G. Hendry, *Value Sensitive Design: Shaping Technology with Moral Imagination*. The MIT Press, 2019, https://doi.org/10.7551/mitpress/7585.001.0001.
[164] J. Bae, S. Lee, and C. J. W. Choi, "Expansion of Digital Technology Use in the Korean Social Work Field," *Journal of Social Service Research*, vol. 51, no. 3, pp. 663–677, 2024, https://doi.org/10.1080/01488376.2024.2402520.
[165] J. A. Osian-Gabrie, "The impact of digital disruption on social inequality: Challenges and opportunities for social work practice", *AJBMR*, vol. 11, no. 2, pp. 45–49, Dec. 2024.
[166] Y. Liu, A. Sharma, S. Rani, and J. Yang, "Supply Chain Security, Resilience and Agility in IoT-driven Healthcare," *IEEE Internet of Things Journal*, https://doi.org/10.1109/JIOT.2025.3545962.

AUTHOR BIOGRAPHY

Yih-Chang Chen holds a Master of Science in Information Systems Security from the London School of Economics and Political Science (LSE), University of London, as well as a Doctorate in Computer Science from the University of Warwick, United Kingdom. He presently serves as an Assistant Professor in both the Bachelor Degree Program in Medical Sociology and Health Care and the Department of Information Management at Chang Jung Christian University in Taiwan. His academic expertise encompasses a range of interdisciplinary fields, including artificial intelligence (AI), software engineering, machine learning, social media applications, social work management, and long-term care. His research is motivated by a dedication to bridging the divide between technology and its social applications. He actively participates in cross-disciplinary initiatives that merge information technology, management science, and social welfare to address complex societal and healthcare issues. In addition to his academic duties, he is currently an Audit Committee Member in the President Office at Chang Jung Christian University and leads projects under the auspices of Taiwan's Ministry of Labor, specifically aimed at the development and implementation of Employment-Oriented Curriculum Programs.

Chia-Ching Lin received her Ph.D. from Kobe University, Japan. She is currently an Assistant Professor in the Department of Finance at Chang Jung Christian University, Taiwan. Her research expertise spans across multiple domains including investment, portfolio management, financial management, insurance, international financial management, and financial securities regulations. Her academic contributions are marked by an interdisciplinary approach, integrating financial theory with practical insights to address globally relevant issues in economics and management. In addition to her academic endeavors, she had led the Ministry of Labor-funded employment program initiatives aimed at advancing career-oriented curriculum development and workforce readiness. Her professional trajectory reflects a deep commitment to bridging academic research with policy application and cross-sector collaboration in finance, management, and public service.