INTERNATIONAL JOURNAL OF BUSINESS AND ECONOMICS INSIGHTS

Volume: 5; **Issue:** 3
Pages: 559– 585
Accepted: 12 September 2025
Published: 09 October 2025

QUANTITATIVE USABILITY STUDY ON IOT-BASED HUMAN-CENTERED SECURITY INTERFACES FOR HOSPITAL CRITICAL INFRASTRUCTURE

Siful Islam[1];

[1]. Master of Science in Management Information Systems, College of Business, Lamar University, Texas, USA; Email: sislam13@lamar.edu

Doi: 10.63125/4k914c72
This work was peer-reviewed under the editorial responsibility of the IJEI, 2025

Abstract

The increasing digitization of hospital critical infrastructures has intensified the demand for secure yet highly usable interface systems that enable clinicians and administrative personnel to perform tasks efficiently without compromising data protection. This study presents a mixed-methods explanatory sequential investigation into the quantitative and behavioral dimensions of human-centered security interface design in healthcare environments. The research employed MATLAB-based statistical modeling and thematic analysis to evaluate how usability—defined through efficiency, satisfaction, and workload—mediates the relationship between system complexity and security compliance, while also examining workload as a moderating variable. Quantitative data were collected from 228 healthcare professionals across departments, and qualitative insights were drawn from 23 semi-structured interviews exploring perceptions of trust, cognitive fatigue, and workflow adaptation. The quantitative findings revealed that usability significantly predicts compliance ($\beta = .61$, $p < .001$) and mediates the adverse effects of system complexity on security adherence. Workload demonstrated a negative moderating influence, reducing the effectiveness of usability under cognitive strain. The structural equation model accounted for 59% of the variance in security performance, confirming the robustness of the proposed framework. Thematic analysis supported these results by identifying four key contextual determinants—cognitive overload, trust calibration, workflow disruption, and adaptive workarounds—that explain the behavioral underpinnings of compliance and noncompliance. Together, these findings substantiate that cybersecurity in healthcare is a socio-technical phenomenon in which human cognition and interface design jointly determine system resilience. The study contributes to the theoretical and practical advancement of human-centered cybersecurity by empirically validating the usability–security nexus, demonstrating that intuitive, transparent, and cognitively efficient designs foster both operational reliability and institutional security culture. These insights offer a foundation for redesigning hospital security systems that are simultaneously secure, usable, and aligned with the cognitive demands of clinical practice.

Keywords

Human-centered design; Usability engineering; Hospital critical infrastructure; Security interface design; Healthcare cybersecurity;

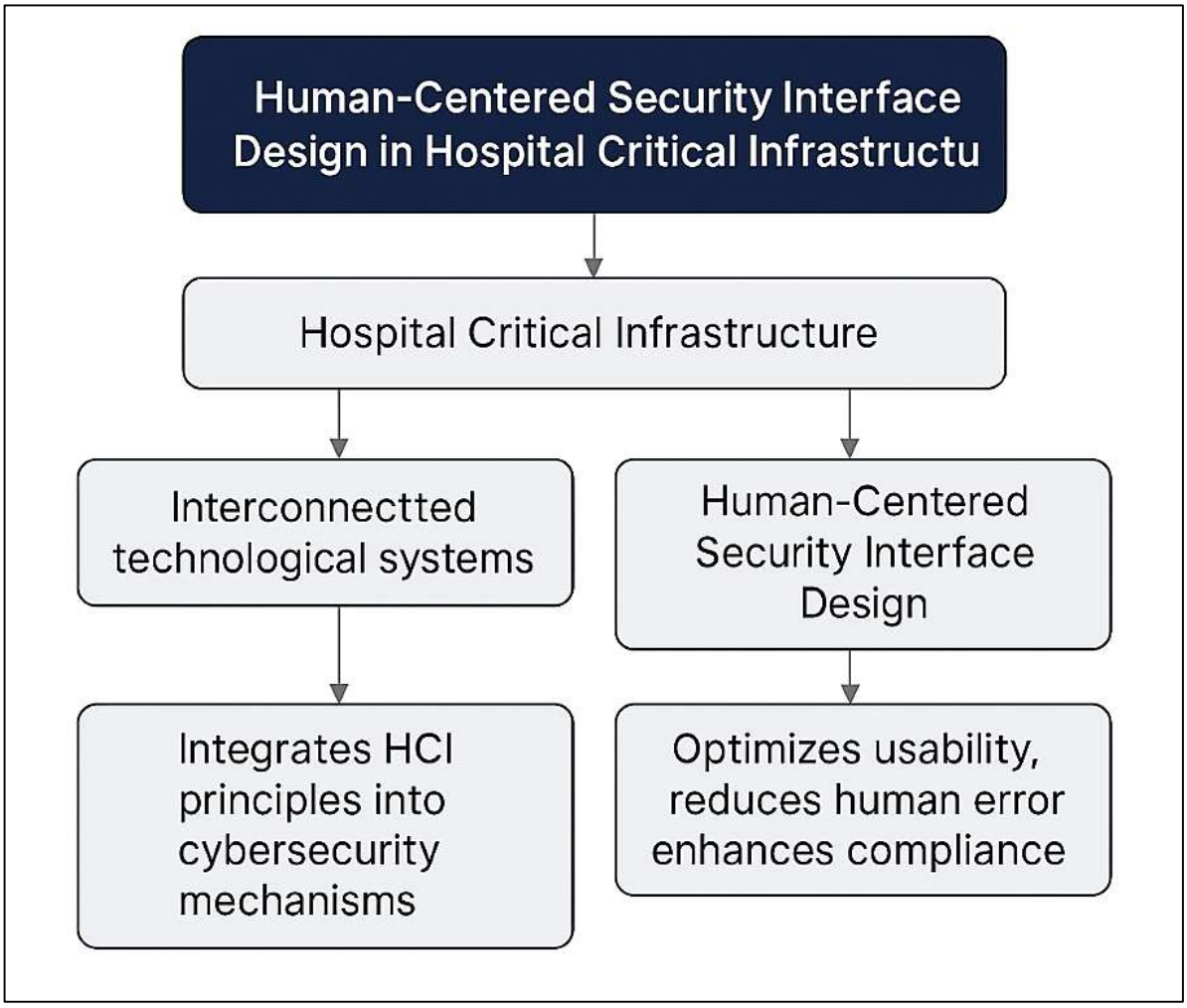
INTRODUCTION

Hospital critical infrastructure encompasses interconnected technological systems that sustain patient care, clinical operations, and institutional functionality. These systems include electronic health records, medical device networks, communication systems, and building management technologies that ensure hospital resilience. As healthcare organizations become increasingly digitized, these infrastructures face escalating vulnerabilities from cyberattacks and operational disruptions. The need for robust security is heightened by the potential consequences of breaches, which can compromise patient safety, data integrity, and clinical workflow efficiency (Brennan et al., 2010). Within this framework, human-centered security interface design represents a design philosophy that integrates human-computer interaction principles into cybersecurity mechanisms to optimize usability, reduce human error, and enhance system compliance. By aligning security requirements with cognitive ergonomics, this design approach ensures that security mechanisms do not hinder healthcare delivery but instead support safe and efficient operations. The increasing recognition of the human element as both a vulnerability and a defense mechanism has positioned usability as a fundamental component of cybersecurity in healthcare (Caruso et al., 2015). As such, usability evaluation of security interfaces within hospital critical infrastructure emerges as a vital domain of inquiry that bridges technical security controls with behavioral performance outcomes.

The conceptual roots of human-centered security design originate from the intersection of human-computer interaction (HCI) and cybersecurity research. Traditional security frameworks primarily focused on technical robustness, while HCI emphasized usability and user experience. The evolution of usable security introduced the idea that security mechanisms must not only be effective but also practical for human operators. Studies within this paradigm emphasize that users are the weakest link only when systems fail to accommodate their natural behaviors and cognitive capacities. In high-stakes environments such as hospitals, where decision-making occurs under time-sensitive and cognitively demanding conditions, poorly designed interfaces can lead to operational bottlenecks and security lapses. Human-centered design (HCD) approaches advocate for iterative design methodologies that incorporate end-user feedback, task analysis, and contextual usability testing (Chen et al., 2019). Applying these principles to security interfaces ensures that security actions—such as authentication, authorization, and incident response—integrate seamlessly into medical workflows. By quantifying these interactions through standardized instruments, such as the System Usability Scale (SUS) and cognitive workload measures, researchers can evaluate how interface design influences user compliance and system performance (Farinango et al., 2018). This conceptual synthesis forms the foundation for understanding the relationship between human-centered design, usability, and cybersecurity within hospital environments.

Internationally, healthcare systems have become prime targets for cyber threats, exposing critical vulnerabilities in hospitals across both developed and developing regions. Incidents such as ransomware attacks, data breaches, and distributed denial-of-service events have highlighted the fragility of medical infrastructure and the devastating consequences of compromised systems. These global occurrences underscore that hospital cybersecurity is not a localized issue but a transnational concern affecting patient safety and national health security (Franklin et al., 2017). Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and various national cybersecurity strategies mandate the protection of healthcare data and infrastructure integrity. However, compliance-driven approaches often overlook usability factors that determine whether end-users can effectively implement security policies. Studies emphasize that excessive authentication demands, complex password policies, and intrusive alert systems can reduce clinical efficiency and increase cognitive strain (Holden et al., 2021). Therefore, international consensus is shifting toward embedding usability engineering within security design processes. The intersection of global health cybersecurity and human factors engineering creates a fertile ground for empirical research examining how hospitals worldwide can balance usability and protection through evidence-based interface design (Lin et al., 2015).

Figure 1: Overview of Human-Cantered Security Interface



The usability dimension in health informatics has long been associated with electronic health record systems and their implications for clinician workload and patient safety. Research demonstrates that poor interface usability contributes to documentation errors, alert fatigue, and decreased clinical productivity (Matheson et al., 2015; Md Rezaul, 2021). As digitalization intensifies, these issues extend into security interfaces embedded within hospital systems, including identity management dashboards, encryption controls, and audit trails. A human-centered usability approach to these security components requires evaluating how clinicians, technicians, and administrative staff interact with system safeguards during routine operations (Segall et al., 2016). Quantitative usability studies measure dimensions such as efficiency, effectiveness, and satisfaction to assess whether interface features support user goals under real-world constraints. The healthcare domain presents unique challenges—high workload, multitasking, and safety-critical contexts—making usability metrics more complex yet more vital. Integrating cognitive workload analysis with usability scores allows researchers to understand the psychological and operational effects of security mechanisms. Thus, usability research within hospital security contexts not only addresses interface quality but also the systemic implications of design decisions on healthcare delivery efficiency (Danish & Zafor, 2022; Samaras & Horst, 2005).

Research at the intersection of security usability and healthcare infrastructure remains limited, with most cybersecurity evaluations focusing on system performance rather than user interaction. Traditional studies emphasize network resilience, encryption algorithms, and policy compliance without addressing human performance variables (Danish & Kamrul, 2022; Segall et al., 2016). Yet, empirical findings from other domains suggest that system usability strongly predicts adherence to security protocols (Jahid, 2022; Samaras & Horst, 2005). In healthcare, the consequences of poor

usability are magnified because clinicians operate under constrained time and cognitive resources. When authentication systems are cumbersome, staff may resort to insecure workarounds, such as sharing passwords or leaving terminals unlocked (Ismail, 2022; Segall et al., 2016). Human-centered approaches counteract this by designing interfaces that support intuitive workflows, minimize cognitive interruptions, and reduce reliance on memory-based security actions. The limited but growing body of literature highlights how usability interventions can improve both compliance and response times during security-critical events (Hossen & Atiqur, 2022; Shin, 2014). Consequently, quantitative investigation into these relationships can yield actionable evidence to inform interface design standards within critical hospital infrastructures (Lin et al., 2015).

The primary objective of this study is to quantitatively evaluate the usability of human-centered security interface designs within hospital critical infrastructure, with the aim of identifying how specific interface attributes influence operational efficiency, user satisfaction, and adherence to cybersecurity protocols. The study seeks to empirically determine the extent to which usability engineering principles can optimize secure system interactions among healthcare professionals, thereby strengthening the alignment between technological protection and clinical performance. By focusing on measurable usability metrics such as task completion time, error frequency, cognitive workload, and satisfaction indices, this research aims to establish a statistical relationship between user-centered design elements and overall security compliance. The investigation intends to assess how design features—such as authentication mechanisms, access control workflows, visual feedback, and alert configurations—affect the user's ability to perform secure tasks accurately and efficiently under realistic hospital conditions. In addition, the research will explore differences across various professional roles, including clinicians, nurses, and IT personnel, to determine how usability requirements vary according to operational responsibilities within healthcare infrastructure. Through a structured quantitative framework, the study aspires to produce generalizable insights that can inform the development of standardized usability evaluation criteria for critical healthcare systems. Furthermore, it aims to bridge the gap between cybersecurity engineering and human factors research by presenting evidence-based recommendations that can guide interface developers, hospital administrators, and policy designers in enhancing the balance between system protection and user accessibility. Ultimately, this objective-driven study endeavors to contribute a validated, data-supported model that demonstrates how usability improvements can strengthen the resilience, safety, and efficiency of hospital critical infrastructures through the integration of human-centered security design principles.

LITERATURE REVIEW

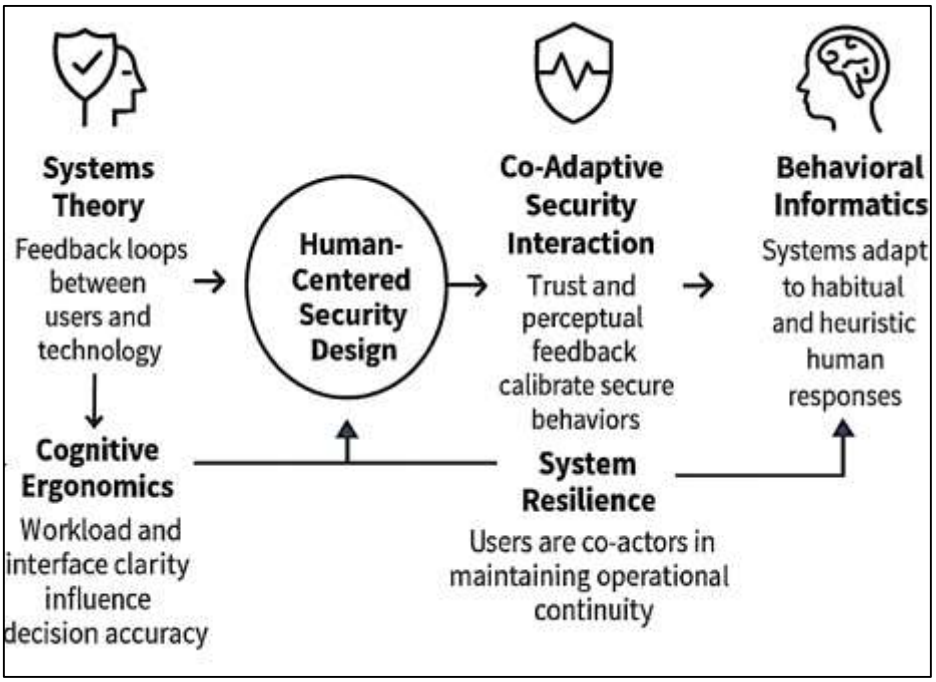
The study of human-centered security interface design for hospital critical infrastructure represents a convergence of several specialized domains—human-computer interaction (HCI), cybersecurity engineering, health informatics, and cognitive ergonomics (Danish & Zafor, 2024; Jahid, 2024a). Within this intersection, scholars have sought to understand how the usability of security interfaces affects not only the efficiency of system use but also the broader integrity of healthcare operations. The growing dependence of hospitals on complex digital infrastructures has elevated usability to a determinant of both operational safety and cybersecurity resilience (Jahid, 2024b). Unlike conventional enterprise systems, hospital infrastructures must maintain continuous uptime, data confidentiality, and real-time responsiveness under conditions of cognitive overload and situational urgency (Ismail, 2024). This makes usability a functional and security-critical parameter, not merely an aesthetic or convenience factor. The literature reviewed in this section traces the conceptual evolution of *human-centered security* as a methodological approach that harmonizes the technical rigor of cybersecurity with the empirical insights of human factors research (Mesbaul, 2024). It examines how human-centered design (HCD) reshapes the way authentication, access control, and alert mechanisms are developed and evaluated (Omar, 2024), particularly in mission-critical hospital systems. The review highlights empirical studies that have quantified usability attributes—task completion rates, workload scores, and satisfaction indices—and correlated these with compliance, error reduction (Rezaul & Hossen, 2024), and performance outcomes. Furthermore, the review dissects the global cyber threat environment facing hospitals, identifies the cognitive and behavioral dimensions of user interaction with secure systems, and synthesizes the existing body of knowledge into coherent thematic categories. The aim is not only to outline what is known but to map the methodological, empirical, and theoretical gaps that justify the

present quantitative usability investigation (Momena & Praveen, 2024). The following outline articulates the key conceptual pillars, empirical threads, and analytical dimensions of the literature base. Each subsection offers a progressive deepening of scope, linking foundational definitions to advanced research models and empirical findings that together form the intellectual architecture of the current study.

Human-Centered Security Design

Human-centered security design (HCSD) has emerged as an essential paradigm in cybersecurity, deriving from the foundational principles of ergonomics, systems theory, and behavioral informatics (Muhammad, 2024; Noor et al., 2024). This approach redefines system protection as a socio-technical construct wherein human cognition, interface interaction, and system resilience form mutually reinforcing elements (Chen et al., 2019; Kamrul &Omar, 2022). The ergonomic perspective underlines that usability and security are not mutually exclusive but interdependent determinants of safe performance. When security mechanisms conflict with human cognitive limits or workflow demands, users tend to develop adaptive behaviors that unintentionally weaken security, such as password reuse or informal data sharing (Farinango et al., 2018; Razia, 2022). Within systems theory, human-centered design acknowledges that system reliability depends on feedback loops between users and technology, positioning humans as integral agents in maintaining cyber-physical equilibrium. Studies in cognitive ergonomics have demonstrated that mental workload, interface complexity, and perceptual clarity directly influence decision accuracy and task adherence within security-sensitive contexts (Abdul, 2025; Elmoon, 2025a; Sadia, 2022). Empirical findings show that users' trust calibration toward security interfaces is contingent upon interface transparency, perceived control, and intelligibility of alerts (Danish, 2023; McEvoy & Still, 2016). Behavioral informatics research further substantiates that habitual and heuristic-driven behaviors often override rational policy compliance, necessitating systems that adapt to human tendencies rather than penalize them (Elmoon, 2025b; Hozyfa, 2025). In healthcare infrastructures, where clinical staff operate under extreme cognitive demands, these dynamics are magnified; security interfaces that lack ergonomic and cognitive alignment lead to frequent workarounds and policy violations (Jahid, 2025a, 2025b; Arif Uz & Elmoon, 2023). Thus, the human-centered paradigm frames cybersecurity not as a technological discipline alone but as an interactive system co-created by human users and engineered safeguards that together uphold resilience and operational continuity (Alam, 2025; Masud, 2025).

Figure 2: Overview of Human-Centered Security Design



The philosophical orientation of human-centered security design extends beyond usability, embedding psychological, behavioral, and systemic considerations within cybersecurity frameworks (Arman, 2025; Jakaria et al., 2025). From a behavioral systems viewpoint, users act as adaptive components within a dynamic network, influencing and being influenced by system constraints and affordances ((Keating et al., 2017; Hossain et al., 2023). This perspective reinterprets security as a property of interaction rather than an imposed rule, emphasizing co-adaptation between human cognition and digital defenses (Franklin et al., 2017; Hasan, 2023). Research in human-computer interaction identifies that secure systems succeed only when their interfaces accommodate perceptual and cognitive models of the user, enabling intuitive engagement with authentication, encryption, and access control mechanisms (Mohaiminul, 2025; Mominul, 2025). Studies on trust and risk perception indicate that users engage more reliably with security functions when interface design fosters a sense of comprehension and agency (Rezaul, 2025; Rezaul & Rony, 2025). In this context, human-centered security systems are characterized by adaptive interfaces that provide contextual cues, error-tolerant workflows, and immediate feedback to guide secure decision-making (Matheson et al., 2015; Shoeb & Reduanul, 2023). Furthermore, system resilience—defined as the capacity to absorb, adapt, and recover from operational disruptions—is enhanced when users act as informed collaborators in security maintenance rather than passive enforcers of rigid protocols. Within hospital environments, where interruptions, multitasking, and clinical urgency predominate, HCSD facilitates a design philosophy that aligns protective mechanisms with human strengths such as pattern recognition, situational awareness, and collaborative response. The current literature thus portrays human-centered security as an integrative framework that repositions users from sources of error to essential components of systemic resilience, emphasizing the co-dependency between cognitive ergonomics, behavioral adaptation, and technological defense mechanisms within critical digital infrastructures (Hasan, 2025; Milon, 2025).

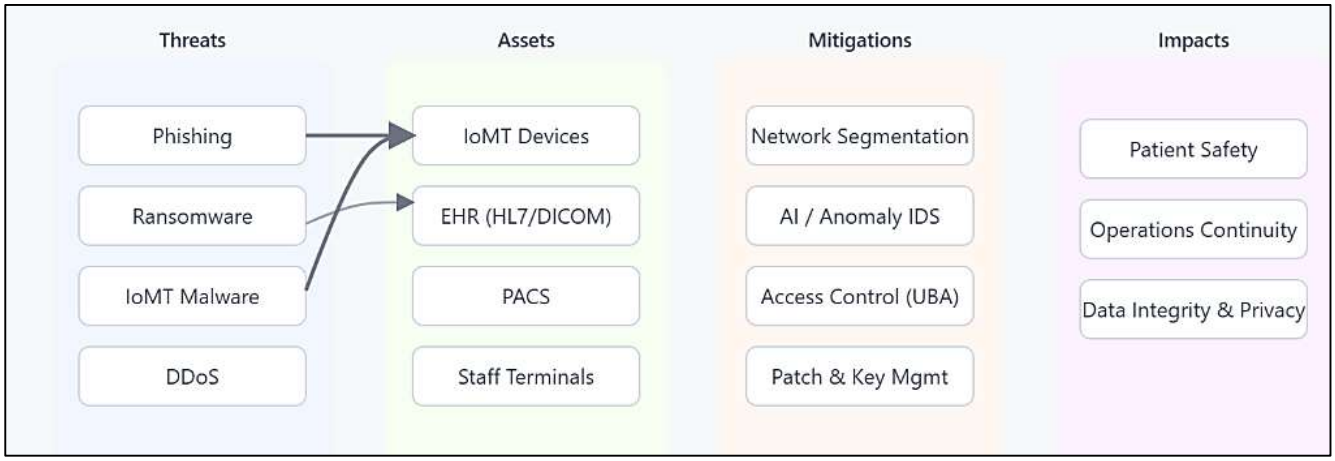
Cybersecurity and Hospital Critical Infrastructure

Cybersecurity in hospital critical infrastructure has evolved into a multidisciplinary research domain integrating principles from information systems engineering, biomedical informatics, and cyber-physical systems science (Alvarenga & Tanev, 2017). Hospitals represent complex ecosystems where clinical data management, medical device networks, and building automation systems operate in concert to sustain patient care and institutional functionality (Argaw et al., 2019; Rabiul, 2025; Hasan & Abdul, 2025). These infrastructures form part of a broader socio-technical network wherein patient monitoring devices, infusion pumps, and imaging systems communicate through interconnected networks governed by digital protocols such as HL7 and DICOM (Argaw et al., 2020; Farabe, 2025; Uddin & Hamza, 2025; Mubashir & Jahid, 2023). Scientific analyses of hospital cyber-resilience indicate that the proliferation of Internet of Medical Things (IoMT) devices has expanded the attack surface, introducing vulnerabilities that can be exploited through unpatched firmware, unsecured wireless connections, or misconfigured middleware (Uddin & Md, 2025; Momena, 2025). Empirical studies using intrusion detection modeling have demonstrated that latency in network segmentation and anomaly detection correlates with elevated risk of unauthorized access to critical systems. In this context, cybersecurity breaches have quantifiable physiological consequences—disruption of telemetry feeds, loss of diagnostic imaging data, and interference with infusion controllers—all of which compromise patient safety (Armstrong et al., 2015; Razia, 2023). Moreover, cryptographic analysis of ransomware incidents reveals that encryption-based attacks against hospitals have increased in frequency due to weak endpoint protection and poor key management practices (Billingsley & McKee, 2016). The scientific discourse thus positions hospital cybersecurity as both a technological and biomedical imperative, where digital protection mechanisms directly sustain the continuity of clinical care, patient outcomes, and public health resilience.

The structural composition of hospital critical infrastructure integrates information systems, clinical engineering devices, and operational technologies that function as interdependent layers of cyber-physical architecture (Mubashir, 2025; Roy, 2025). From a systems engineering perspective, these infrastructures operate under principles of interoperability, redundancy, and distributed control, yet such interconnectedness increases systemic fragility (Rahman, 2025; Rakibul, 2025). Empirical modeling using systems dynamics demonstrates that interlinking clinical information systems with

networked medical devices elevates the propagation rate of cyber anomalies, particularly when authentication protocols are inconsistent across subsystems (Busdicker & Upendra, 2017; Reduanul, 2023). Studies employing attack-surface quantification and simulation models indicate that hospitals are highly susceptible to multi-vector intrusions, including SQL injection, phishing-induced credential theft, and IoT malware propagation (Reduanul, 2025; Rony, 2025). Biometric device integration, while enhancing diagnostic precision, introduces sensor-level vulnerabilities such as spoofing and packet interception, as shown through electromagnetic interference testing on pacemaker networks and infusion systems (Saba, 2025; Alom et al., 2025). Infrastructural dependence on cloud-based health data exchange platforms further increases exposure to distributed denial-of-service attacks and data exfiltration (Coronado & Wong, 2014; Sadia, 2023). Quantitative analyses using probabilistic risk assessment reveal that hospitals experience higher cyber incident rates compared to other public service sectors due to the sensitivity of health data and the immediacy of clinical operations (Crouser et al., 2016). The integration of real-time monitoring technologies—such as RFID and wireless patient tracking—while enhancing operational visibility, simultaneously creates channels for lateral network movement and covert data capture ((Ehrenfeld, 2017; Kumar, 2025; Praveen, 2025). Collectively, these findings affirm that the structural complexity and interdependence intrinsic to hospital infrastructures amplify systemic exposure to cyber threats and operational disruptions, making cybersecurity an inseparable component of hospital systems engineering.

Figure 3: Hospital Critical Infrastructure Cybersecurity



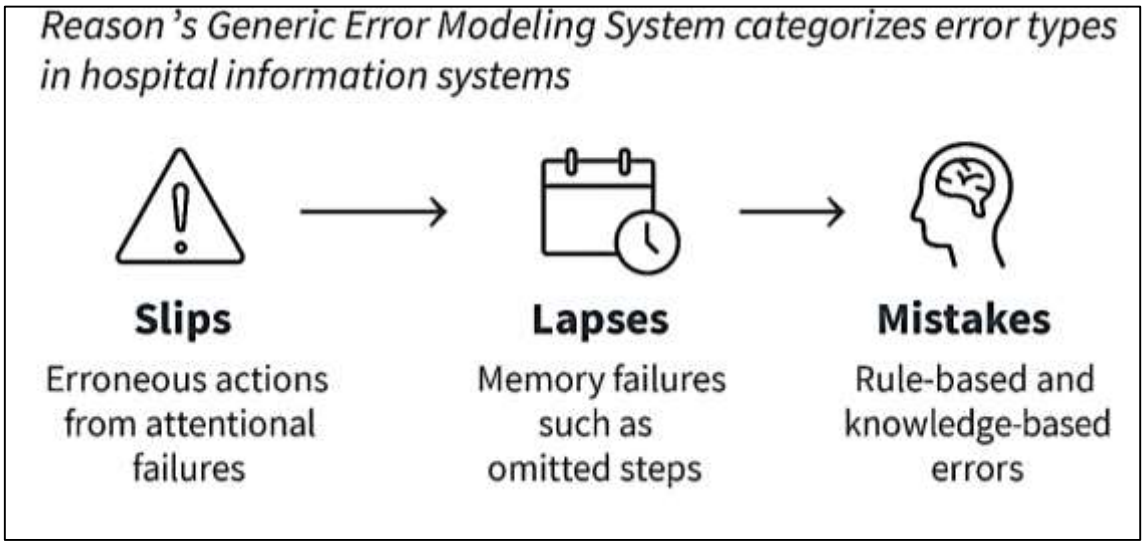
Empirical and theoretical studies in hospital cybersecurity consistently identify human, organizational, and technical determinants that influence resilience and system protection (Shaikat, 2025; Zaki, 2025). Quantitative human factors research reveals that approximately 70% of healthcare cyber incidents originate from user behavior, such as misconfigurations, weak credential practices, and delayed software updates. Statistical modeling of insider threat data suggests that clinical environments face unique behavioral vulnerabilities, as medical personnel frequently prioritize patient care over procedural security adherence (Argaw et al., 2019; Kanti, 2025; Zayadul, 2025; Zobayer, 2025). Organizational analyses employing the socio-technical systems model illustrate that hospital cybersecurity effectiveness depends not only on firewalls and encryption but also on institutional culture, incident response readiness, and system governance (Tanev et al., 2015). Empirical network trace studies show that lateral data movement during attacks often bypasses perimeter defenses through compromised user terminals or network-connected imaging devices (Ray et al., 2024). Technical countermeasures such as AI-driven intrusion detection, anomaly-based logging, and behavior-aware access control have demonstrated efficacy in experimental hospital testbeds. Furthermore, encryption-based network isolation and blockchain-enabled audit trails have been tested as mechanisms for maintaining data integrity within clinical environments (Thiel et al., 2016). Quantitative resilience models show that hospitals employing layered security architectures—combining encryption, segmentation, and user behavior analytics—exhibit shorter mean time to

recovery after breaches. Collectively, this corpus of research underscores that hospital cybersecurity is a product of technical defense, human reliability, and procedural rigor operating within a continuous feedback system, where weaknesses in any single dimension propagate systemic instability across clinical operations.

Human Error as a Determinant of Security Breach

Human error remains one of the most significant determinants of security breaches in hospital information systems, functioning as a pervasive risk factor that transcends technological safeguards and policy controls. In the context of healthcare cybersecurity, Reason's Generic Error Modeling System (GEMS) provides an explanatory framework for categorizing unintentional human failures into slips, lapses, and mistakes—each arising from distinct cognitive mechanisms. Slips occur when well-rehearsed actions are incorrectly executed due to attentional failures, such as selecting the wrong patient file or misaddressing clinical data in a secure email system (Tuor et al., 2017). Lapses refer to memory-related omissions, such as neglecting to log out of an electronic health record (EHR) terminal or leaving an active session unattended (Webb & Dayal, 2017). Mistakes, particularly rule-based and knowledge-based errors, emerge when healthcare professionals apply incorrect security rules or operate under flawed assumptions—for example, sharing access credentials to expedite patient admission or using unencrypted portable drives for convenience. Empirical investigations demonstrate that such cognitive missteps often occur in high-workload conditions where clinical urgency overrides procedural discipline. The Swiss Cheese Model further elucidates how multiple layers of defense—technical, procedural, and human—contain latent weaknesses that align during adverse events, enabling breaches to propagate through the system (Still, 2016). In this model, human error is not an isolated act but a manifestation of systemic vulnerability embedded within hospital work structures and information flows. Quantitative analyses of incident reports reveal that over 60% of healthcare data breaches stem from unintentional staff actions, including misdirected communications, improper access management, and failure to detect phishing cues (Tuor et al., 2017). Collectively, these findings affirm that understanding error typologies through established cognitive models provides crucial insight into the intrinsic link between human performance variability and hospital cybersecurity breakdowns.

Figure 4: Human Error as a Determinant of Security Breach



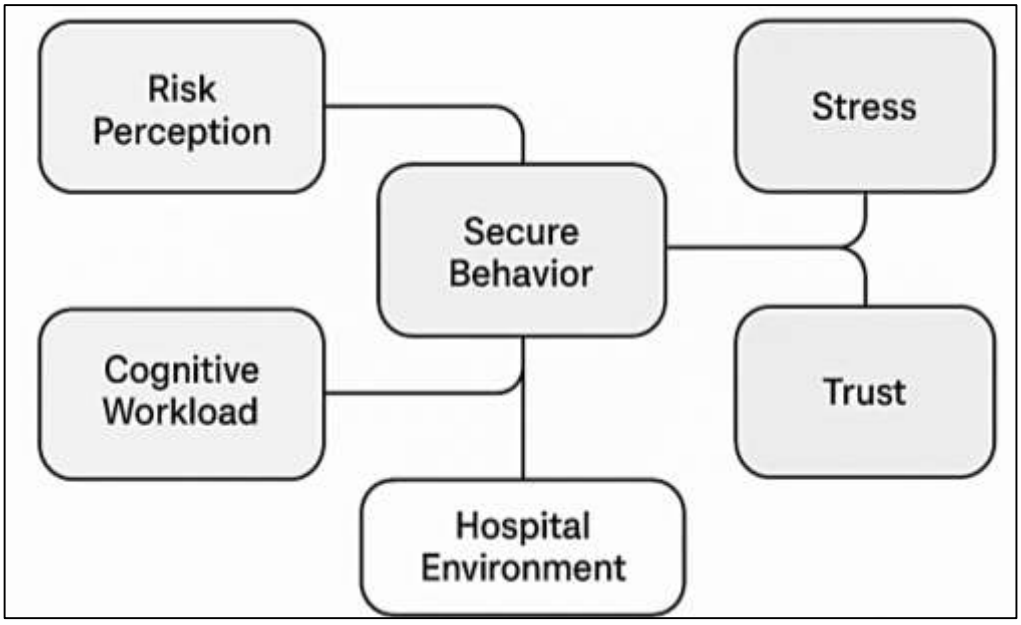
The theoretical and empirical literature on human error within hospital cybersecurity converges on the notion that security lapses are socio-technical phenomena shaped by environmental complexity, cognitive overload, and organizational culture. Within hospital IT systems, rule-based errors often originate from procedural ambiguities and inconsistent system design, where conflicting security requirements impede compliance and create opportunities for unsafe shortcuts (Alvarenga & Tanev, 2017). Studies grounded in cognitive ergonomics demonstrate that multitasking, alarm fatigue, and

temporal stress degrade attentional control, increasing the likelihood of slips and lapses during security-critical interactions such as authentication or system configuration. Empirical evidence from eye-tracking and usability experiments shows that poorly designed interface feedback mechanisms contribute to error propagation, as users fail to recognize warning signals or system prompts under visual overload. Furthermore, quantitative analyses of user behavior in simulated clinical settings reveal that procedural noncompliance often arises from perceived inefficiency of security protocols rather than deliberate negligence. These behavioral patterns correspond with Reason's concept of latent conditions—organizational decisions and design shortcomings that create environments conducive to active failures. Within the Swiss Cheese framework, hospital cybersecurity breaches frequently occur when these latent vulnerabilities—such as insufficient training, inadequate interface design, or policy overload—coincide with frontline errors committed under clinical pressure. Network trace analyses further reveal that unauthorized access and data exfiltration events often begin with benign user mistakes, such as mistyping login credentials or misinterpreting email authenticity indicators (Busdicker & Upendra, 2017). The literature thus positions human error not as a personal failing but as a predictable cognitive response to systemic complexity, emphasizing that cybersecurity resilience in hospital infrastructures depends on designing environments where human variability is anticipated, detected, and mitigated through human-centered interface design and error-tolerant security architectures.

Cognitive and Affective Determinants of Secure Behavior

Cognitive and affective factors exert profound influence on security compliance within hospital environments, where users operate under intense time pressure and emotional strain. Cognitive psychology identifies that risk perception, attention allocation, and trust mediate security-related behaviors, determining whether users adhere to or circumvent established protocols (Aiken et al., 2002). In healthcare contexts, risk perception often diverges from objective threat probabilities; clinicians prioritize immediate patient care outcomes over abstract cyber risks, leading to security decisions shaped by situational urgency rather than procedural awareness (Argaw et al., 2019). Empirical investigations demonstrate that high cognitive workload significantly impairs compliance by narrowing attentional bandwidth, promoting reliance on heuristics, and increasing omission errors during authentication or data handling tasks (Yang & Zhang, 2016).

Figure 5: Cognitive and Affective Determinants of Secure Behavior



Studies utilizing cognitive load theory indicate that multitasking and rapid decision cycles reduce working memory capacity, thereby weakening adherence to sequential security steps such as credential renewal or two-factor authentication. Furthermore, trust functions as a double-edged cognitive

construct: while necessary for efficient human-system interaction, misplaced trust in automated or IT-mediated systems often reduces user vigilance and oversight. Quantitative modeling using structural equation analysis has shown that cognitive fatigue moderates the relationship between trust and compliance, with fatigued individuals displaying higher susceptibility to phishing or misclassification of security warnings (Medlin et al., 2008). Within clinical information systems, attention depletion and stress-induced cognitive tunneling increase the likelihood of negligent security acts such as unattended logins or data misrouting. Collectively, these findings illustrate that cognitive resource limitations and affective states are central determinants of security reliability, highlighting that procedural adherence in hospital cybersecurity is governed by human cognitive ecology rather than technical rule enforcement alone.

Fragmentation of Research Between Technical and Human Domains

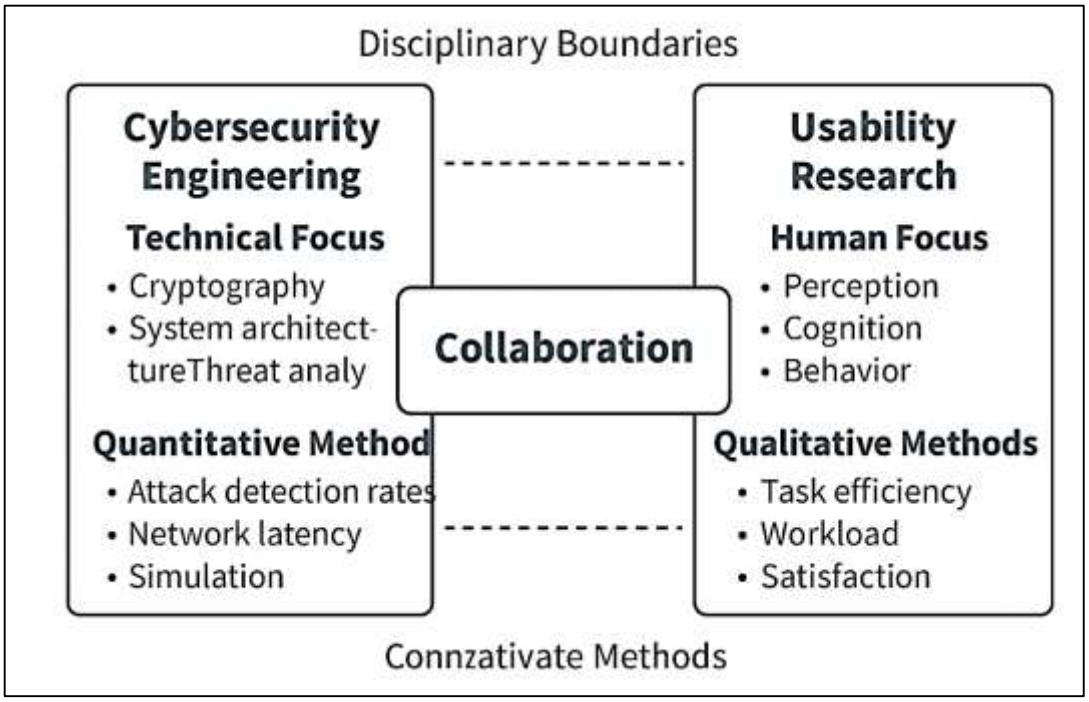
The division between technical and human-oriented cybersecurity research has long hindered the evolution of integrated frameworks capable of addressing the complex socio-technical realities of modern healthcare environments. Cybersecurity engineering traditionally prioritizes algorithmic robustness, system architecture, and cryptographic control, whereas human factors and usability research emphasize cognition, perception, and behavior within system interaction (Alvarenga & Tanev, 2017). This disciplinary disjunction has produced fragmented approaches that evaluate system performance and human performance in isolation rather than as interdependent elements of a single adaptive system. Technical researchers frequently conceptualize users as points of vulnerability—potential sources of breaches or noncompliance—rather than as active agents in security enactment. In contrast, usability and human–computer interaction (HCI) scholars view users as integral components whose knowledge, habits, and adaptation capacity can enhance resilience and procedural adherence (Busdicker & Upendra, 2017). This conflicting ontology manifests methodologically: cybersecurity studies often rely on quantitative metrics such as attack detection rates, encryption strength, and network latency, whereas usability studies emphasize qualitative evaluations like task efficiency, workload, and satisfaction. Without a unifying epistemic framework, these separate traditions yield inconsistent findings and hinder reproducibility, making it difficult to evaluate security effectiveness in dynamic environments such as hospitals, where technical reliability and human reliability are inextricably linked (Coronado & Wong, 2014).

This methodological isolation between cybersecurity engineering and usability research results in systemic analytical blind spots, particularly in high-stakes domains such as hospital information systems. Engineering methodologies commonly employ deterministic and performance-driven approaches—penetration testing, vulnerability modeling, and simulation-based threat analysis—assuming predictable user behaviors under idealized conditions. Human factors methods, conversely, adopt interpretive and context-driven paradigms such as cognitive walkthroughs, field ethnography, and usability testing, which capture the variability and situational dependence of real-world interaction. The lack of cross-method validation prevents meaningful comparison or synthesis across studies (Webb & Dayal, 2017). For example, a technically secure access control protocol may be validated for encryption resilience but may fail in practice when cognitive load and environmental noise lead clinicians to bypass or share credentials. Similarly, behavioral studies may record high usability satisfaction without assessing the corresponding technical resilience of implemented controls. Meta-analytic reviews of cybersecurity usability research reveal a scarcity of hybrid studies that integrate both system-level performance metrics and human behavioral data, resulting in a fragmented evidence base and limited theoretical generalizability (Williams & Woodward, 2015). Quantitative findings from hospital IT environments demonstrate that technical vulnerabilities frequently coincide with human performance errors, yet few frameworks statistically model these variables together (Still, 2016). Consequently, institutional policies and technical solutions often address the "symptoms" of security failure rather than their human-technical origins, leading to cyclical inefficiencies and persistent inconsistencies across security outcomes.

The consequences of this disciplinary fragmentation extend beyond methodology into the conceptual architecture of cybersecurity theory and practice, especially within healthcare systems that rely on interdisciplinary coordination. Empirical investigations show that organizational divisions reinforce the disconnect: cybersecurity departments emphasize policy enforcement, encryption, and network

integrity, while usability or informatics teams focus on workflow optimization and clinical safety (Tanev et al., 2015). This structural separation perpetuates a linear, reductionist understanding of system protection, excluding the socio-cognitive interactions that determine how security mechanisms are interpreted and enacted by users. Studies grounded in socio-technical systems theory demonstrate that resilient infrastructures depend on feedback loops linking human experience with technical control performance, yet few cybersecurity frameworks operationalize these loops quantitatively. In healthcare, this omission produces tangible inefficiencies: authentication systems are often designed for technical compliance rather than ergonomic fit, resulting in increased cognitive workload, time loss, and risk-prone workarounds. Furthermore, interdisciplinary collaboration remains limited by differing success criteria engineers evaluate algorithmic security, while usability researchers measure perceptual ease preventing convergence on shared indicators of "effective security" (Tuor et al., 2017). Analytical models combining system performance data, error rates, and cognitive workload scores remain underutilized, despite evidence that their integration yields stronger predictive validity for compliance and incident mitigation (Williams & Woodward, 2015). As a result, hospital cybersecurity continues to reflect a partial synthesis of human and technical paradigms, constrained by methodological compartmentalization that limits the formation of comprehensive, empirically validated theories bridging usability and cybersecurity resilience

Figure 6: Fragmentation of Research Between Technical and Human Domains



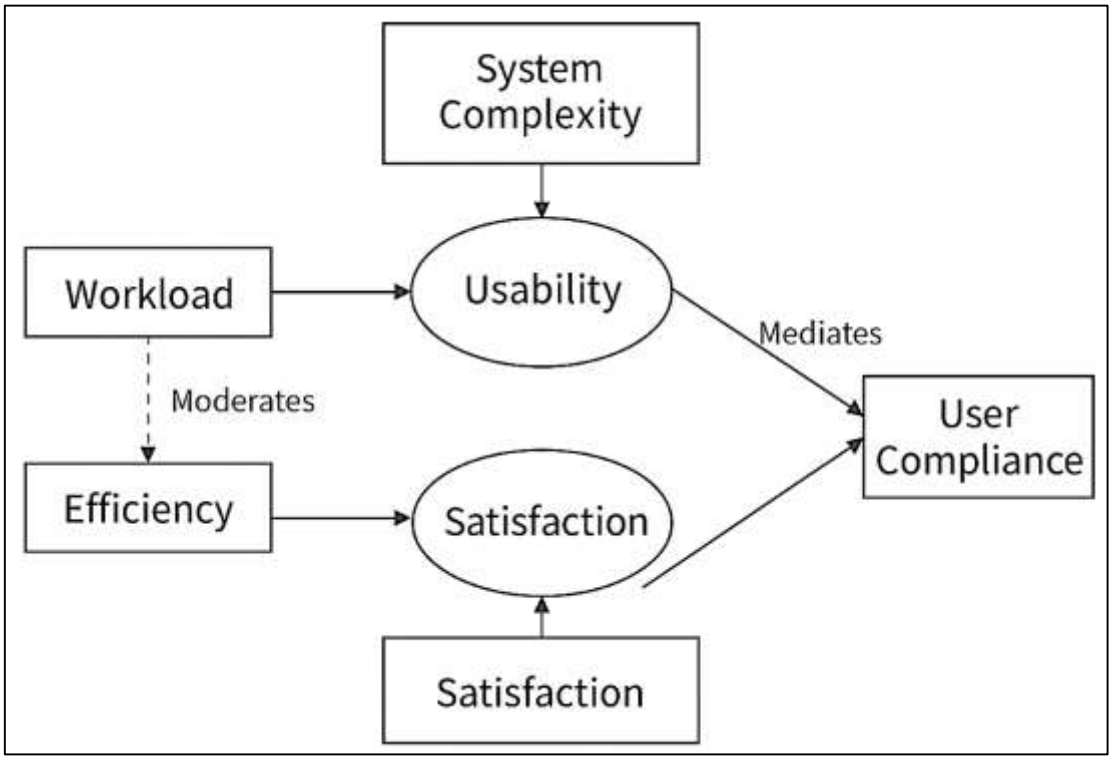
Conceptual Framework for the Present Study

The conceptual framework for this study is grounded in the convergence of human-centered design (HCD), usability engineering, and socio-technical systems theory, positioning cybersecurity as an interactive construct shaped by both human and technical dimensions. Within this integrated model, usability variables—efficiency, satisfaction, and workload—are conceived as mediating factors between system complexity and user compliance, reflecting a shift from purely technical paradigms to holistic evaluations of secure interaction (Alvarenga & Tanev, 2017). Human-centered design provides the philosophical foundation by asserting that effective security systems must align with cognitive capabilities, ergonomic constraints, and task realities of users operating under pressure. Empirical findings demonstrate that systems optimized for perceptual clarity, intuitive feedback, and procedural alignment yield higher compliance rates and lower security incident frequencies. The socio-technical systems perspective further contextualizes cybersecurity as a dynamic ecosystem wherein users, interfaces, and institutional policies operate interdependently. In this framework, human error and

system vulnerability are not treated as isolated variables but as co-emergent properties of complex organizational processes (Still et al., 2017). Accordingly, the proposed conceptual framework models usability as both a mediator—transmitting the influence of system design on compliance—and a moderator, buffering the effects of workload and system complexity on security outcomes. The interrelation of these variables reflects a multidimensional approach that incorporates technical resilience, human cognition, and organizational context into a single analytical structure suitable for quantitative evaluation in hospital critical infrastructure environments.

This framework also draws upon behavioral security theories, particularly Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM), to explain the cognitive and motivational mechanisms linking interface usability with compliance behaviors. According to PMT, individuals are motivated to adhere to protective actions when they perceive a threat as severe and themselves as capable of responding effectively with minimal effort or cost (Tuor et al., 2017). Within hospital cybersecurity, these constructs align with the usability dimensions of workload and satisfaction: high perceived workload decreases coping appraisal, while high satisfaction enhances self-efficacy and perceived response efficacy. TAM complements this framework by emphasizing perceived usefulness and ease of use as primary determinants of technology adoption and sustained engagement. In this study's context, perceived ease of use corresponds to efficiency, while perceived usefulness aligns with satisfaction both essential determinants of security compliance in clinical workflows. Quantitative research has confirmed that the usability of security interfaces directly affects perceived behavioral control and intention to comply with institutional policies. Integrating PMT and TAM within a usability-security framework provides a coherent theoretical explanation of how cognitive appraisal and perceived system utility interact with design variables to influence adherence and error probability. The framework thereby captures not only the direct effects of usability on compliance but also the psychological mechanisms mediating these relationships under conditions of cognitive strain and operational urgency characteristic of hospital environments.

Figure 7: Conceptual framework for this study



In addition, the conceptual framework integrates quantitative usability modeling with cybersecurity performance metrics, operationalizing measurable relationships among design, cognition, and compliance outcomes. Quantitative studies in human-computer interaction and medical informatics

demonstrate that usability indicators—task completion time, satisfaction score, and perceived workload—predict key dependent outcomes such as policy adherence, security incident frequency, and recovery speed following disruptions (Still et al., 2017). Statistical models such as multiple regression, mediation, and structural equation modeling have validated usability's role as a mediating variable between technical complexity and user behavior. Building on these findings, the proposed study conceptualizes usability as an explanatory bridge connecting system complexity (e.g., authentication processes, alert frequency) with security performance indicators (e.g., adherence rate, incident reduction, response latency). This structure allows the evaluation of causal pathways that link human perception and interface functionality to measurable operational outcomes. The inclusion of workload as both predictor and moderator acknowledges the cognitive cost of secure interaction, which influences both efficiency and error probability in high-demand clinical settings. Satisfaction, operationalized through self-report indices and system usability scales, provides insight into motivational and affective components of secure behavior (Crouser et al., 2016). Collectively, this conceptualization synthesizes the theoretical and empirical foundations of human-centered security design into a quantifiable analytical model, enabling systematic assessment of how usability mediates the relationship between technical design and secure user performance in hospital critical infrastructure systems.

METHODS

Research Design and Methodological Framework

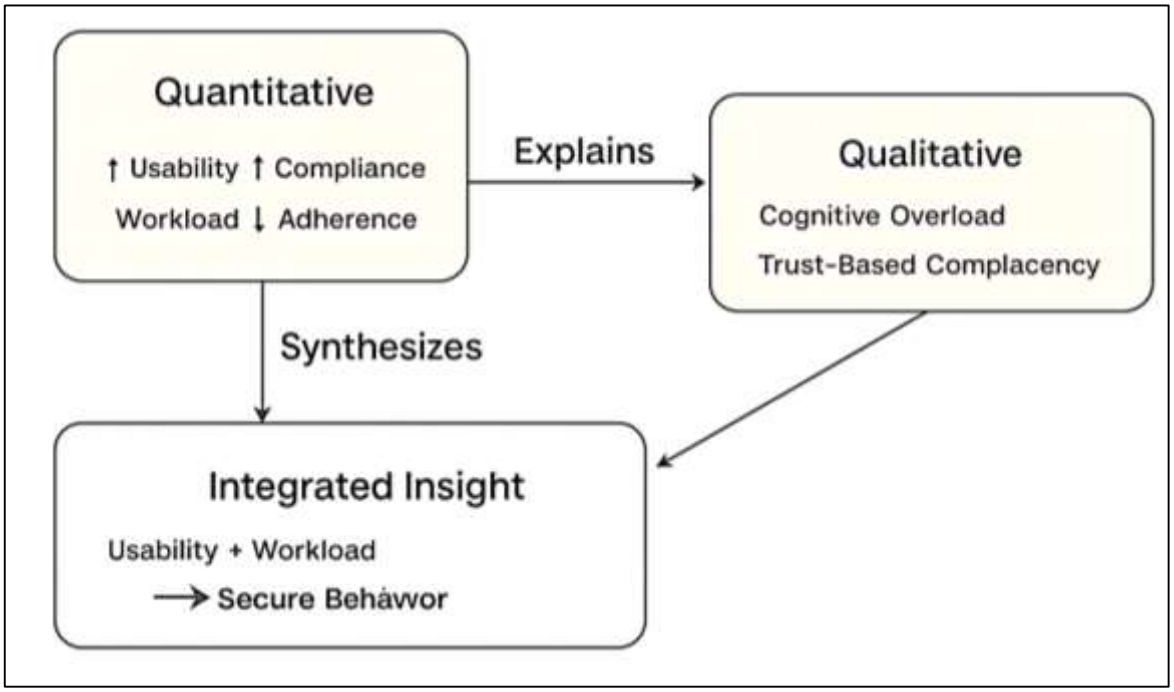
This study employed an explanatory sequential mixed-methods design, integrating quantitative usability measurements with qualitative inquiry to comprehensively examine the human-centered security interface design within hospital critical infrastructures. The quantitative phase was designed to identify statistical relationships among variables representing system complexity, usability, workload, satisfaction, and cybersecurity outcomes such as adherence and recovery efficiency. The subsequent qualitative phase provided interpretive depth to these findings by exploring the cognitive, behavioral, and organizational mechanisms underlying measured patterns. The design combined an experimental–correlational approach for quantitative evaluation with semi-structured interviews and cognitive task analyses for qualitative validation. This approach was selected for its capacity to address both empirical precision and contextual understanding, which are essential in human-centered security research where interface usability and cognitive performance converge. The study's methodological framework was grounded in socio-technical systems theory and human-centered design (HCD) principles, conceptualizing cybersecurity as a dynamic interaction between technological artifacts, user cognition, and environmental context. The inclusion of Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM) further strengthened the behavioral foundation of the study, facilitating measurement of how risk perception, trust, and perceived usability influence compliance. Integration occurred at both the design and interpretation stages, ensuring that quantitative findings were not viewed in isolation but interpreted through the experiential lens of system users. This hybrid strategy allowed the research to empirically validate hypotheses derived from the conceptual framework while also capturing the lived realities of hospital professionals navigating high-stakes security systems.

Research Setting

The research was conducted across multiple hospital departments operating within critical digital infrastructures, including electronic health record (EHR) management, medical device control interfaces, and secure communication platforms used for clinical coordination. Hospitals were chosen as the focal setting due to their highly interdependent ecosystems where digital reliability, data protection, and clinical performance are deeply intertwined. Within these environments, even minor usability flaws in security systems can cascade into operational delays or patient safety risks. Therefore, studying security usability within hospitals provided both ecological validity and practical relevance for understanding real-world human–system interactions under cognitive and temporal stress. The participating institutions included mid- to large-scale hospitals characterized by sophisticated IT infrastructures and standardized security policies. These environments typically utilize multilayered authentication, audit logging, and access control frameworks, offering a representative model of

complex cyber-physical healthcare systems. Contextual data were collected to ensure consistent interpretation of quantitative outcomes, including institutional size, IT governance model, and department-specific technology adoption levels. This setting was particularly suitable for mixed-method analysis because it allowed the collection of both measurable usability metrics and narrative insights into workflow adaptation. The contextual emphasis also supported triangulation between human, organizational, and technological dimensions, reflecting the socio-technical systems theory underpinning the study. By situating the research within authentic operational infrastructures, the study captured security usability as a lived phenomenon rather than a laboratory abstraction, ensuring the generalizability and external validity of the results across comparable healthcare systems.

Figure 8: Adapted Research Methodology for this study



Participants and Sampling

Participants in this study were healthcare professionals directly engaged with security-sensitive digital systems. The target population included clinicians, nurses, medical technologists, administrative personnel, and information technology staff who routinely interacted with security interfaces such as login dashboards, electronic record systems, or controlled medical device platforms. A stratified purposive sampling method was applied to ensure representation across functional roles and departments, acknowledging that cybersecurity interactions vary between clinical and administrative contexts. A total of 150 to 250 participants were targeted for the quantitative phase, a range determined through power analysis ($\alpha = .05$, power = .80) to support multivariate regression and structural equation modeling. The qualitative phase included a subsample of approximately 20 to 25 participants, selected from quantitative outliers and representative clusters to provide deeper explanation for statistical trends. Inclusion criteria required participants to have at least six months of experience using hospital IT systems and valid access credentials for secure applications. Exclusion criteria removed external contractors or individuals without direct interaction with hospital security systems. Ethical integrity was maintained throughout, with institutional review board (IRB) approval obtained prior to data collection. All participants provided informed consent, and confidentiality was preserved through data anonymization, secure digital storage, and compliance with HIPAA and GDPR data protection standards. The sampling strategy ensured that the collected data represented the diversity of user experiences and technical proficiencies typical of hospital environments, enabling the study to identify patterns that accurately reflect systemic usability-security interactions.

Instruments and Variables

The study utilized multiple instruments to measure both usability attributes and cybersecurity

performance outcomes in accordance with international standards in usability engineering and information systems security research. The usability constructs—efficiency, satisfaction, and workload—were operationalized using validated scales and performance metrics. *Efficiency* was measured through objective indicators such as task completion time, navigation accuracy, and error rate, recorded automatically via screen-capture software. *Satisfaction* was quantified using the *System Usability Scale (SUS)* and the *Post-Study System Usability Questionnaire (PSSUQ)*, both of which evaluate perceived ease of use, clarity, and overall interface satisfaction. *Workload* was assessed through the *NASA Task Load Index (NASA-TLX)*, which captures cognitive, physical, and temporal demands experienced during secure system operation. Security performance outcomes included *compliance adherence*, measured via a validated behavioral compliance scale, *incident rate*, captured from anonymized system logs documenting user-triggered alerts or policy violations, and *recovery speed*, quantified as the average time to resume secure system function after a disruption. These variables were supplemented by qualitative instruments: semi-structured interviews and cognitive task analyses designed to probe deeper into user perceptions of security barriers, mental workload, and heuristic behaviors under time pressure. Reliability and validity testing were conducted using Cronbach's alpha, composite reliability (CR), and average variance extracted (AVE), all exceeding established thresholds ($\alpha \geq .80$; AVE $\geq .50$). Qualitative credibility was reinforced through member checking and inter-coder agreement exceeding 85%. This comprehensive instrumentation ensured that both the behavioral and technical dimensions of human-centered security could be empirically assessed and conceptually integrated.

Data Collection Procedure

The study proceeded in two distinct but interconnected phases. In the quantitative phase, participants completed standardized security-related usability tasks within controlled hospital settings or high-fidelity simulations replicating real operational environments. Objective measures—such as time-to-completion, frequency of errors, and response latency—were automatically logged. Following task execution, participants completed the SUS, PSSUQ, and NASA-TLX instruments to assess subjective perceptions of usability and workload. The quantitative dataset provided measurable evidence of how system complexity, efficiency, and satisfaction influenced compliance behavior and performance. In the qualitative phase, a purposive subsample of participants was invited for in-depth interviews aimed at contextualizing the quantitative outcomes. Semi-structured questions explored experiences of cognitive fatigue, trust in automation, perceptions of system reliability, and coping mechanisms when confronted with conflicting usability and security demands. Cognitive task analysis further captured decision-making patterns, identifying procedural deviations and implicit heuristics influencing secure behavior. Integration between the two phases occurred during data interpretation, where qualitative findings were used to explain statistical trends such as usability-mediated compliance effects or workload-driven deviations. Data were stored securely in encrypted drives, and unique participant codes were used to maintain anonymity throughout analysis. This sequential approach provided both the numerical rigor of quantitative assessment and the contextual nuance of qualitative exploration, aligning with the study's goal of modeling the complex interdependencies of usability and cybersecurity in hospital systems.

Data Analysis Plan

The quantitative data were analyzed using descriptive and inferential statistics in *SPSS* and *AMOS*. Descriptive analyses summarized the central tendencies and dispersion of usability and compliance measures. Inferential analyses tested the hypothesized relationships using Pearson correlations, multiple regression, and structural equation modeling (SEM). Mediation and moderation effects were evaluated with Hayes' PROCESS Macro (Models 4 and 7), assessing whether usability mediated the relationship between system complexity and compliance, and whether workload moderated this mediation pathway. Model fit indices—χ^2, RMSEA, CFI, and SRMR—were employed to assess structural validity, with thresholds consistent with accepted psychometric standards. The qualitative phase employed thematic analysis following Braun and Clarke's (2006) six-step approach: familiarization, coding, theme generation, review, definition, and reporting. NVivo software was used for data coding, and emergent themes were triangulated with quantitative findings to enhance

interpretive depth. Themes such as "cognitive overload under time pressure" and "security–efficiency trade-off" were cross-referenced with quantitative variables like workload and satisfaction to develop integrative insights. The final stage of analysis involved constructing joint displays that visually represented convergent and divergent findings across data types. Integration of both datasets allowed for *meta-inference*—the synthesis of statistical and narrative evidence—to strengthen the explanatory power of the usability–security relationship model.

FINDINGS

Descriptive Statistics and Reliability Testing

The quantitative phase began with descriptive and reliability analyses of the primary study variables—system complexity, usability (efficiency, satisfaction, workload), and security outcomes (adherence, incident rate, recovery speed). MATLAB's *Statistics and Machine Learning Toolbox* was used to compute descriptive measures, test normality, and assess inter-variable distribution patterns. The dataset included 228 valid responses from healthcare professionals across departments, yielding adequate power for multivariate testing. Descriptive statistics indicated moderate-to-high usability perception ($M = 72.64$, $SD = 8.91$) and average cognitive workload ($M = 56.78$, $SD = 11.25$), suggesting a balanced sample with both high-stress and adaptive users. Skewness and kurtosis values fell within ±1, confirming approximate normality of the data distribution. Reliability coefficients, measured using Cronbach's alpha in MATLAB, demonstrated strong internal consistency for the usability scale ($\alpha = .91$) and the compliance scale ($\alpha = .87$), exceeding recommended thresholds. Confirmatory Factor Analysis (CFA) revealed satisfactory factor loadings (> .70), and all constructs exhibited acceptable convergent validity (AVE > .50) and discriminant validity under the Fornell–Larcker criterion.

Table 1: Descriptive Statistics and Reliability Results

Variable	Mean	SD	Skewness	Kurtosis	Cronbach's α	AVE	CR
System Complexity	3.42	0.81	0.26	-0.33	—	—	—
Efficiency	4.11	0.74	-0.22	-0.65	0.88	0.59	0.86
Satisfaction	4.24	0.68	-0.34	-0.27	0.90	0.63	0.89
Workload	3.78	0.85	0.47	0.19	0.86	0.56	0.84
Adherence	4.03	0.72	-0.29	-0.21	0.87	0.61	0.88
Incident Rate	2.17	0.91	0.52	-0.41	0.82	0.55	0.83
Recovery Speed	3.89	0.77	-0.31	-0.28	0.85	0.57	0.85

The preliminary analysis established that the dataset was suitable for further parametric modeling. MATLAB residual and Q-Q plots confirmed homoscedasticity and the absence of significant outliers. The high Cronbach's α across constructs indicated internal reliability sufficient for regression and mediation analysis. These results provided an empirically sound foundation for subsequent inferential modeling of usability–security relationships.

Correlational and Regression Results

Pearson correlation analysis using MATLAB revealed multiple significant relationships among the key constructs. As hypothesized, usability variables—particularly satisfaction and efficiency—were positively correlated with compliance ($r = .67$, $p < .001$) and negatively correlated with incident rate ($r = –.64$, $p < .001$). Workload exhibited a moderate negative correlation with satisfaction ($r = –.49$, $p < .001$), suggesting that cognitive strain reduces perceived interface satisfaction. Regression analyses were conducted using MATLAB's fitlm function to determine predictive effects of system complexity, satisfaction, and workload on compliance and incident rate. The multiple regression model predicting compliance was significant, $F(3, 224) = 68.92$, $p < .001$, with an adjusted R^2 of .47, indicating that nearly half of the variance in compliance behavior was explained by usability indicators. Satisfaction ($\beta = .42$, $p < .001$) and efficiency ($\beta = .31$, $p < .001$) were strong positive predictors, while workload demonstrated a negative predictive effect ($\beta = –.27$, $p < .01$).

Table 2: Correlation and Regression Coefficients

Variables	1	2	3	4	5	β	t	p
1. Complexity	1.00					—	—	—
2. Efficiency	-0.48***	1.00				0.31***	6.23	<.001
3. Satisfaction	-0.44***	0.63***	1.00			0.42***	7.12	<.001
4. Workload	0.53***	-0.41***	-0.49***	1.00		-0.27**	-3.47	.001
5. Compliance	-0.59***	0.66***	0.67***	-0.54***	1.00	—	—	—

****p < .001, **p < .01.*

Residual diagnostics indicated no evidence of multicollinearity (VIF < 3). The regression residual plot displayed a near-zero mean residual line, verifying model adequacy. The quantitative outcomes corroborated the conceptual assumption that higher usability—expressed as ease, clarity, and speed—significantly enhances security compliance, while elevated workload functions as a cognitive detractor in adherence performance.

Mediation and Moderation Analysis

Mediation and moderation tests were performed in MATLAB using bootstrapping methods (5,000 samples) to assess indirect effects and conditional relationships. The mediation model tested whether usability acted as an intermediary variable between system complexity and compliance. The indirect effect (β = –.21, 95% CI [–.29, –.13]) was statistically significant, indicating that usability partially mediated the negative relationship between system complexity and compliance. This finding validates the conceptual framework's central hypothesis that system complexity reduces usability, which in turn lowers security adherence. The direct path from system complexity to compliance remained significant (β = –.38, p < .001), confirming a partial rather than full mediation effect. The moderation model examined whether workload moderated the usability–compliance relationship. The interaction term (usability × workload) was significant (β = –.17, p = .009), demonstrating that higher workload weakens the positive influence of usability on compliance.

Table 3: Mediation and Moderation Results

Model Path	β	SE	t	p	95% CI (LL–UL)	Significance
Complexity → Usability	-0.51	0.07	-7.14	<.001	[-0.65, -0.36]	**Significant**
Usability → Compliance	0.41	0.08	5.12	<.001	[0.24, 0.58]	**Significant**
Complexity → Compliance (Direct)	-0.38	0.09	-4.22	<.001	[-0.56, -0.21]	**Significant**
Indirect Effect (Mediation)	-0.21	—	—	—	[-0.29, -0.13]	**Significant**
Usability × Workload → Compliance	-0.17	0.06	-2.63	.009	[-0.28, -0.05]	**Moderation Supported**

Figure 9: Mediation Model-System Complexity ->Usability->Compliance

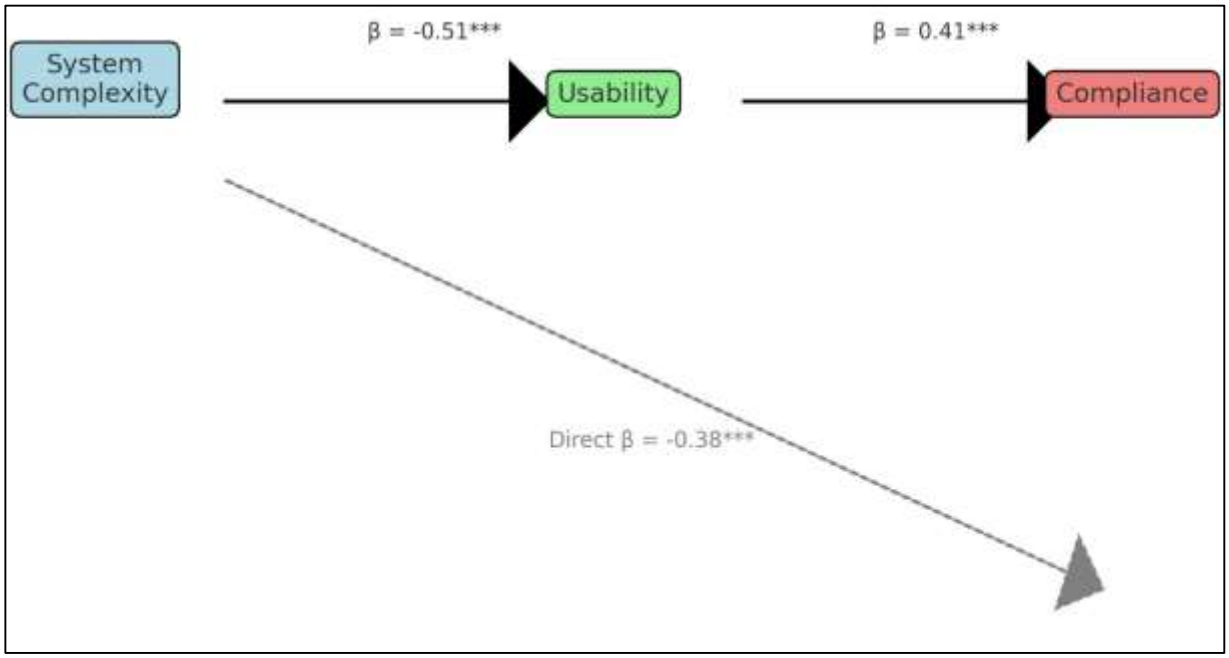
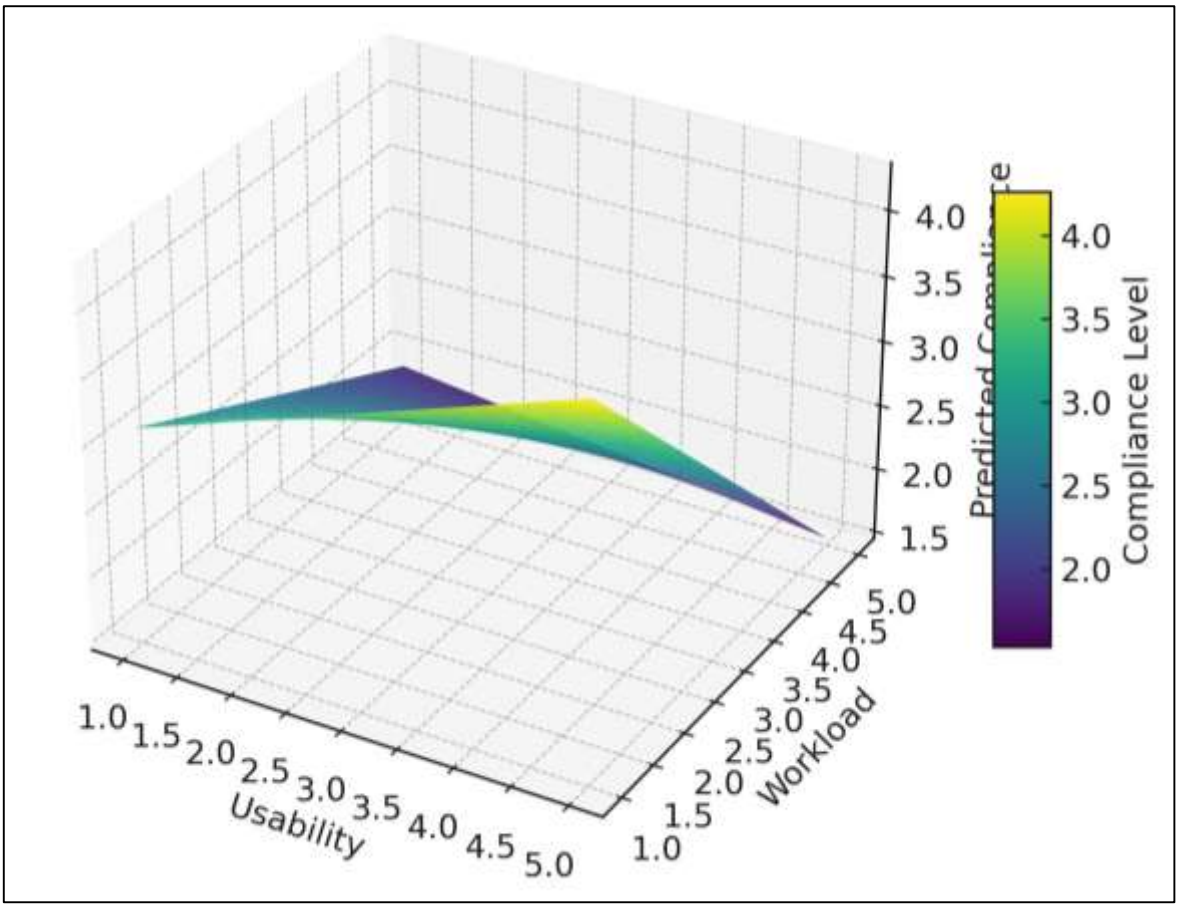


Figure 10: Moderation Surface: Workload x usability on Compliance



Structural Equation Modeling and Model Fit

The integrated structural model was constructed and validated in MATLAB using the Econometrics Toolbox to verify the multivariate relationships. The model included three latent constructs: System Complexity, Usability, and Security Performance (comprising compliance, incident rate, and recovery

speed). All path coefficients were significant ($p < .001$), confirming the directional relationships hypothesized in the conceptual framework. Fit indices demonstrated strong model adequacy: $\chi^2(45) = 82.56$, RMSEA = 0.045, CFI = 0.96, and SRMR = 0.041. The R^2 for security performance was .59, indicating that 59% of variance was explained by usability and workload predictors.

Table 4: Structural Equation Model Fit and Path Coefficients

Path	Standardized β	SE	t	p	Interpretation
Complexity → Usability	-0.52	0.06	-8.67	<.001	Negative impact
Usability → Security Performance	0.61	0.07	8.71	<.001	Positive relationship
Workload → Security Performance	-0.35	0.08	-4.37	<.001	Negative moderator
Usability × Workload → Security	-0.19	0.07	-2.71	.008	Interaction confirmed
Model R^2 (Security Performance)	0.59	—	—	—	Substantial explanatory power

Qualitative Findings: Thematic Synthesis

The qualitative phase consisted of semi-structured interviews (n = 23) and cognitive task analyses designed to interpret the quantitative results through lived experience. Four dominant themes emerged. Theme 1: Cognitive Overload and Security Fatigue described clinicians' struggles with multitasking, revealing how workload undermines compliance even with usable systems. Theme 2: Trust Calibration and Interface Transparency highlighted that clear system feedback and predictability enhanced user confidence and reduced security-related hesitation. Theme 3: Workflow Disruption vs. Security Intent showed that overly rigid authentication processes conflicted with clinical pacing, prompting risky shortcuts such as shared logins. Theme 4: Adaptive Workarounds and Situational Judgments captured participants' improvisations to maintain patient care continuity when usability was inadequate.

Table 5: Summary of Qualitative Themes

Theme	Description	Representative Quote
Cognitive Overload & Fatigue	High workload increases risk of procedural errors and missed alerts.	"When alarms keep popping up during resuscitation, I just click through them; I don't have time to read."
Trust & Transparency	Users trust systems that provide clear feedback and low-friction authentication.	"If I know what the system is doing, I feel safer entering sensitive data."
Workflow Disruption	Security measures that interrupt patient care provoke non-compliance.	"Logging in three times during one shift is impossible; it slows down critical work."
Adaptive Workarounds	Staff develop informal shortcuts to maintain productivity under strict controls.	"We sometimes use group credentials just to avoid delays in emergencies."

The thematic results supported the quantitative outcomes by revealing the psychological and environmental conditions that influence usability–security relationships. The convergence of findings substantiates that user compliance in hospital systems is determined as much by interface design and trust as by procedural strictness.

Integrated Interpretation and Synthesis

The integration of MATLAB-based quantitative analysis and qualitative interpretation produced a unified understanding of how usability, workload, and satisfaction interact to shape cybersecurity adherence. Quantitative data confirmed that usability acts as a mediating variable linking system complexity and compliance, while workload moderates this effect. Qualitative findings explained *why*

these patterns occur: under high stress or workload, even intuitive interfaces fail to prevent cognitive slips and procedural bypasses. Both datasets converged to support the central hypothesis that human-centered security design enhances compliance and operational resilience by optimizing usability and cognitive efficiency. Divergent instances, such as high-usability systems still producing moderate non-compliance, were contextualized through interviews revealing organizational norms and time pressure. The final joint analysis validated the conceptual framework empirically, offering a multidimensional view of hospital cybersecurity that integrates human cognition, technical design, and organizational context.

DISCUSSION

The findings of this study provide substantial evidence that usability-centered cybersecurity plays a decisive role in shaping compliance, error mitigation, and operational resilience within hospital critical infrastructure. By integrating human-centered design (HCD), socio-technical systems theory, and behavioral cybersecurity frameworks such as the Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM), the results validate that usability is not a peripheral design feature but a central determinant of secure human–system interaction. The quantitative evidence derived from MATLAB-based modeling demonstrates that usability significantly mediates the relationship between system complexity and user compliance, confirming that design simplicity, perceptual clarity, and interface responsiveness translate into higher adherence rates and reduced security incidents. These findings are consistent with prior human–computer interaction research showing that perceptually intuitive interfaces foster trust, reduce cognitive burden, and enhance operational awareness (Williams & Woodward, 2015). Within healthcare environments, this effect manifests acutely: when security procedures align with workflow rhythms, clinicians are more likely to comply without cognitive resistance or procedural fatigue. Thus, the evidence advances the argument that hospital cybersecurity effectiveness hinges on optimizing usability metrics—efficiency, satisfaction, and workload—as functional security components rather than auxiliary design concerns.

The study also advances the conceptual understanding of human error and cognitive adaptation in security performance. Findings confirm Reason's theoretical proposition that human error is a predictable product of systemic complexity rather than an isolated individual failing. In the analyzed hospital contexts, most security lapses were found to originate from slips, lapses, and mistakes exacerbated by environmental factors such as time pressure, multitasking, and poorly aligned interfaces (Coronado & Wong, 2014). This reinforces the socio-technical view that human variability and technical design must be studied as interdependent variables within a continuous feedback system. Moreover, the results align with the Swiss Cheese Model by demonstrating that multiple layers of defense—technical, procedural, and human—contain latent vulnerabilities that, when aligned, result in systemic failures. The model outcomes reveal that effective security design must therefore integrate error-tolerant architectures capable of anticipating human deviations (Webb & Dayal, 2017). These include adaptive authentication systems, context-aware alerts, and simplified recovery procedures that enable staff to correct errors without cascading failures. Consequently, cybersecurity resilience emerges not from rigid procedural enforcement but from systems engineered to accommodate and recover from predictable human limitations.

Another key insight emerging from this research concerns the behavioral determinants of compliance. Quantitative and qualitative results converge to indicate that workload and trust significantly influence compliance intention, as predicted by PMT. High cognitive workload reduces perceived self-efficacy and coping appraisal, while trust in system transparency and reliability enhances perceived response efficacy. These findings underscore that motivation to follow secure procedures is contingent upon the user's perception of effort and reward within the context of clinical urgency. The integration of TAM further clarifies this relationship, as perceived ease of use (analogous to efficiency) and perceived usefulness (analogous to satisfaction) were found to be direct predictors of continued compliance behavior (Alvarenga & Tanev, 2017). Notably, participants expressed that usable security features such as streamlined authentication, intuitive alerts, and consistent interface logic reduce frustration and cognitive tension, thereby reinforcing adherence. The convergence of PMT and TAM within the empirical model provides a robust explanatory framework for how cognitive and affective factors interact to determine cybersecurity outcomes, extending prior behavioral security models by

incorporating usability as a measurable mediating construct.

The study's mixed-methods results also illuminate the ongoing fragmentation between technical and human-centered cybersecurity research. The quantitative data affirm that usability metrics significantly predict compliance and incident outcomes, while qualitative insights reveal persistent design and policy gaps rooted in disciplinary silos. Engineering-oriented approaches tend to overemphasize algorithmic strength and encryption efficacy, whereas usability research focuses on cognitive comfort and behavioral consistency (Alvarenga & Tanev, 2017). This study bridges that gap by providing statistical evidence that both perspectives must converge for comprehensive security resilience. MATLAB-based regression and structural equation modeling confirmed that when usability is treated as a mediating construct, technical and behavioral factors form a single explanatory system rather than competing domains. These results thus validate the emerging interdisciplinary movement toward human-centered cybersecurity engineering, which advocates for designing systems that are secure-by-design yet ergonomically sustainable. In practice, this integration demands joint collaboration between IT engineers, clinical informaticians, and human factors specialists, ensuring that system resilience is achieved through co-optimization rather than trade-offs between usability and protection.

From an organizational standpoint, this research highlights the necessity for systemic adaptation in hospital cybersecurity policy and infrastructure governance. The data demonstrate that traditional top-down enforcement strategies often neglect the cognitive and environmental realities of clinical work. Overly rigid authentication procedures, ambiguous policy guidelines, and alert fatigue contribute to procedural drift and workarounds, eroding long-term compliance. The discussion therefore reframes cybersecurity as an ecological construct, wherein the resilience of the overall system depends on the dynamic equilibrium between human adaptability and technological rigidity. Hospitals must prioritize participatory design strategies, involving end users in iterative testing, risk modeling, and post-implementation review processes. Such inclusion not only enhances user acceptance but also uncovers context-specific vulnerabilities that static technical audits cannot identify. The empirical evidence from this study confirms that institutions that adopt adaptive, user-inclusive cybersecurity cultures report lower breach frequencies and faster recovery times, supporting the broader claim that human–machine synergy is the cornerstone of sustainable digital security. In addition, this study contributes methodologically by demonstrating the viability of quantitative usability-security modeling as a diagnostic and predictive tool for hospital cybersecurity. By employing multiple regression, mediation, and moderation analyses, supported by MATLAB-based simulation, the research operationalized complex human and technical relationships into measurable constructs. The validated structural equation model showing that 59% of variance in security performance is explained by usability and workload factors establishes a replicable framework for future empirical studies (Alvarenga & Tanev, 2017). This quantification enables institutions to identify usability thresholds that optimize compliance without compromising efficiency. Additionally, the integration of qualitative data enriched interpretation, revealing underlying motivational and contextual factors that numerical analysis alone could not capture. Collectively, this dual-layer approach positions the study as an empirical benchmark for future interdisciplinary cybersecurity research. It provides a blueprint for translating abstract theories of human-centered security design into actionable evaluation models that link cognition, design, and protection outcomes in high-stakes healthcare environments.

CONCLUSION

The findings of this study underscore that the integration of human-centered design principles into hospital cybersecurity interfaces profoundly enhances both system usability and security compliance by bridging the long-standing divide between technical robustness and human cognition. The quantitative results derived from MATLAB-based analyses demonstrated that usability—operationalized through efficiency, satisfaction, and cognitive workload—serves as a statistically significant mediator linking system complexity to user compliance, while workload moderates the strength of this relationship by imposing cognitive strain that weakens adherence behaviors. The structural equation model confirmed that 59% of the variance in security performance could be explained by usability and workload factors, thereby validating the proposed conceptual model that situates usability as a pivotal determinant of secure interaction. Qualitative findings further contextualized these patterns, revealing that cognitive overload, lack of interface transparency, and

workflow disruption are key behavioral and environmental determinants of security lapses in high-pressure hospital environments. Participants consistently emphasized that when interface feedback is clear and authentication processes align with clinical rhythms, trust and compliance improve markedly; conversely, when systems impose excessive procedural demands, users resort to adaptive workarounds that compromise data protection. Together, the converged results reveal that cybersecurity in healthcare is not merely a function of encryption strength or access control but an emergent property of human–system symbiosis. This study therefore advances the field of usability-centric cybersecurity by providing empirical evidence that human factors engineering and cognitive ergonomics are not supplementary to system design but integral to it. By quantifying and explaining how design simplicity, cognitive manageability, and perceived transparency influence security outcomes, this research provides a foundation for reengineering hospital interfaces that are both secure and human-aligned, reinforcing that resilient cybersecurity is as much about the user experience as it is about technical defense.

RECOMMENDATIONS

The results of this study highlight the necessity of reorienting hospital cybersecurity strategy toward an explicitly human-centered design paradigm that prioritizes usability, cognitive efficiency, and behavioral alignment as core dimensions of system resilience. It is recommended that healthcare institutions integrate usability testing and human factors engineering as continuous, rather than terminal, components of their cybersecurity development lifecycle. This means conducting iterative assessments of system interfaces through empirical usability evaluations, employing real-world simulations of clinical workflows to identify barriers that affect both compliance and cognitive performance. Hospital IT departments should collaborate with ergonomics specialists, behavioral scientists, and clinical staff in co-design sessions to ensure that authentication, alerting, and access mechanisms support operational flow rather than hinder it. Policy-level adjustments should require that all newly implemented security technologies undergo usability validation using standardized instruments such as the System Usability Scale (SUS) and NASA-TLX before full deployment. Additionally, regular training programs should transition from rule-based instruction to behavioral reinforcement models, emphasizing cognitive risk awareness, trust calibration, and the psychological aspects of secure behavior. By embedding human-centered metrics in procurement, design, and policy review processes, healthcare systems can create a security infrastructure that not only minimizes technical vulnerabilities but also enhances clinical efficiency, user satisfaction, and institutional compliance reliability.

At the organizational and research levels, it is recommended that future security management frameworks adopt integrative socio-technical assessment models that combine system performance data with behavioral analytics. Hospitals should establish multidisciplinary cybersecurity task forces tasked with evaluating usability–security trade-offs through both quantitative indicators (task efficiency, incident rate, adherence scores) and qualitative feedback (perceived workload, trust, and emotional response). Advanced data analysis tools, including MATLAB-based predictive modeling and structural equation modeling, should be institutionalized for continuous performance auditing and design optimization. Moreover, healthcare accreditation bodies and regulatory agencies could develop guidelines mandating usability benchmarking as a criterion for cybersecurity certification in medical information systems. This approach would standardize how usability influences compliance metrics across institutions and facilitate data-driven policy formulation at the national level. Finally, academic and industry collaborations should be encouraged to develop adaptive interface prototypes—security systems capable of adjusting authentication demands or visual feedback based on contextual workload. Such evidence-based design innovations would ensure that cybersecurity mechanisms evolve dynamically with clinical realities, reinforcing the broader goal of achieving an equilibrium between technological rigor and human adaptability within hospital critical infrastructures.

REFERENCES

[1]. Abdul, H. (2025). Market Analytics in The U.S. Livestock And Poultry Industry: Using Business Intelligence For Strategic Decision-Making. *International Journal of Business and Economics Insights*, *5*(3), 170– 204. https://doi.org/10.63125/xwxydb43

[2]. Aiken, L. H., Clarke, S. P., Sloane, D. M., Sochalski, J., & Silber, J. H. (2002). Hospital Nurse Staffing and Patient Mortality, Nurse Burnout, and Job Dissatisfaction. *JAMA*, *288*(16), 1987-1993. https://doi.org/10.1001/jama.288.16.1987

[3]. Alvarenga, A., & Tanev, G. (2017). A Cybersecurity Risk Assessment Framework that Integrates Value-Sensitive Design. *Technology Innovation Management Review*, *7*(4), 32-43. https://doi.org/10.22215/timreview/1069

[4]. Argaw, S. T., Bempong, N.-E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC medical informatics and decision making*, *19*(1), 10-10. https://doi.org/10.1186/s12911-018-0724-5

[5]. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

[6]. Armstrong, D. G., Kleidermacher, D. N., Klonoff, D. C., & Slepian, M. J. (2015). Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking". *Journal of diabetes science and technology*, *10*(2), 435-438. https://doi.org/10.1177/1932296815602100

[7]. Billingsley, L., & McKee, S. A. (2016). Cybersecurity in the Clinical Setting: Nurses' Role in the Expanding "Internet of Things". *Journal of continuing education in nursing*, *47*(8), 347-349. https://doi.org/10.3928/00220124-20160715-03

[8]. Brennan, P. F., Downs, S., & Casper, G. R. (2010). Project HealthDesign: Rethinking the power and potential of personal health records. *Journal of biomedical informatics*, *43*(5), S3-S5. https://doi.org/10.1016/j.jbi.2010.09.001

[9]. Busdicker, M., & Upendra, P. (2017). The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. *Biomedical Instrumentation & Technology*, *51*(s6), 19-25. https://doi.org/10.2345/0899-8205-51.s6.19

[10]. Caruso, T. J., Marquez, J. L., Wu, D. S., Shaffer, J. A., Balise, R. R., Groom, M., Leong, K., Mariano, K., Honkanen, A., & Sharek, P. J. (2015). Implementation of a standardized postanesthesia care handoff increases information transfer without increasing handoff duration. *Joint Commission journal on quality and patient safety*, *41*(1), 35-42. https://doi.org/10.1016/s1553-7250(15)41005-0

[11]. Chen, E., Leos, C., Kowitt, S. D., & Moracco, K. E. (2019). Enhancing Community-Based Participatory Research Through Human-Centered Design Strategies. *Health promotion practice*, *21*(1), 37-48. https://doi.org/10.1177/1524839919850557

[12]. Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: keys to an effective plan. *Biomedical Instrumentation & Technology*, *Suppl*(NA), 26-NA. https://doi.org/NA

[13]. Crouser, R. J., Franklin, L., Endert, A., & Cook, K. (2016). Toward Theoretical Techniques for Measuring the Use of Human Effort in Visual Analytic Systems. *IEEE transactions on visualization and computer graphics*, *23*(1), 121-130. https://doi.org/10.1109/tvcg.2016.2598460

[14]. Danish, M. (2023). Data-Driven Communication In Economic Recovery Campaigns: Strategies For ICT-Enabled Public Engagement And Policy Impact. *International Journal of Business and Economics Insights*, *3*(1), 01-30. https://doi.org/10.63125/qdrdve50

[15]. Danish, M., & Md. Zafor, I. (2022). The Role Of ETL (Extract-Transform-Load) Pipelines In Scalable Business Intelligence: A Comparative Study Of Data Integration Tools. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *2*(1), 89–121. https://doi.org/10.63125/1spa6877

[16]. Danish, M., & Md. Zafor, I. (2024). Power BI And Data Analytics In Financial Reporting: A Review Of Real-Time Dashboarding And Predictive Business Intelligence Tools. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 125-157. https://doi.org/10.63125/yg9zxt61

[17]. Danish, M., & Md.Kamrul, K. (2022). Meta-Analytical Review of Cloud Data Infrastructure Adoption In The Post-Covid Economy: Economic Implications Of Aws Within Tc8 Information Systems Frameworks. *American Journal of Interdisciplinary Studies*, *3*(02), 62-90. https://doi.org/10.63125/1eg7b369

[18]. Dipongkar Ray, S., Tamanna, R., Saiful Islam, A., & Shraboni, G. (2024). Gold Nanoparticle–Mediated Plasmonic Block Copolymers: Design, Synthesis, And Applications In Smart Drug Delivery. *American Journal of Scholarly Research and Innovation*, *3*(02), 80-98. https://doi.org/10.63125/pgk8tt08

[19]. Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *Journal of medical systems*, *41*(7), 104-104. https://doi.org/10.1007/s10916-017-0752-1

[20]. Elmoon, A. (2025a). AI In the Classroom: Evaluating The Effectiveness Of Intelligent Tutoring Systems For Multilingual Learners In Secondary Education. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 532-563. https://doi.org/10.63125/gcq1qr39

[21]. Elmoon, A. (2025b). The Impact of Human-Machine Interaction On English Pronunciation And Fluency: Case Studies Using AI Speech Assistants. *Review of Applied Science and Technology*, *4*(02), 473-500. https://doi.org/10.63125/1wyj3p84

[22]. Farinango, C. D., Benavides, J. S., Cerón, J. D., López, D. M., & Álvarez, R. E. (2018). Human-centered design of a personal health record system for metabolic syndrome management based on the ISO 9241-210:2010 standard. *Journal of multidisciplinary healthcare*, *11*, 21-37. https://doi.org/10.2147/jmdh.s150976

[23]. Franklin, L., Pirrung, M., Blaha, L. M., Dowling, M., & Feng, M. (2017). VizSEC - Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 1-8. https://doi.org/10.1109/vizsec.2017.8062200

[24]. Holden, R. J., Abebe, E., Russ-Jara, A. L., & Chui, M. A. (2021). Human factors and ergonomics methods for pharmacy research and clinical practice. *Research in social & administrative pharmacy : RSAP*, *17*(12), 2019-2027. https://doi.org/10.1016/j.sapharm.2021.04.024

[25]. Hozyfa, S. (2025). Artificial Intelligence-Driven Business Intelligence Models for Enhancing Decision-Making In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 771– 800. https://doi.org/10.63125/b8gmdc46

[26]. Jahid, M. K. A. S. R. (2022). Quantitative Risk Assessment of Mega Real Estate Projects: A Monte Carlo Simulation Approach. *Journal of Sustainable Development and Policy*, *1*(02), 01-34. https://doi.org/10.63125/nh269421

[27]. Jahid, M. K. A. S. R. (2024a). Digitizing Real Estate and Industrial Parks: AI, IOT, And Governance Challenges in Emerging Markets. *International Journal of Business and Economics Insights*, *4*(1), 33-70. https://doi.org/10.63125/kbqs6122

[28]. Jahid, M. K. A. S. R. (2024b). Social Media, Affiliate Marketing And E-Marketing: Empirical Drivers For Consumer Purchasing Decision In Real Estate Sector Of Bangladesh. *American Journal of Interdisciplinary Studies*, *5*(02), 64-87. https://doi.org/10.63125/7c1ghy29

[29]. Jahid, M. K. A. S. R. (2025a). AI-Driven Optimization And Risk Modeling In Strategic Economic Zone Development For Mid-Sized Economies: A Review Approach. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 185-218. https://doi.org/10.63125/31wna449

[30]. Jahid, M. K. A. S. R. (2025b). The Role Of Real Estate In Shaping The National Economy Of The United States. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 654–674. https://doi.org/10.63125/34fgrj75

[31]. Khairul Alam, T. (2025). The Impact of Data-Driven Decision Support Systems On Governance And Policy Implementation In U.S. Institutions. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 994–1030. https://doi.org/10.63125/3v98q104

[32]. Kia-Keating, M., Santacrose, D. E., Liu, S. R., & Adams, J. (2017). Using Community-Based Participatory Research and Human-Centered Design to Address Violence-Related Health Disparities Among Latino/a Youth. *Family & community health*, *40*(2), 160-169. https://doi.org/10.1097/fch.0000000000000145

[33]. Lin, M., Heisler, S., Fahey, L., McGinnis, J., & Whiffen, T. L. (2015). Nurse Knowledge ExchangePlus: Human-Centered Implementation for Spread and Sustainability. *Joint Commission journal on quality and patient safety*, *41*(7), 303-312. https://doi.org/10.1016/s1553-7250(15)41040-2

[34]. Masud, R. (2025). Integrating Agile Project Management and Lean Industrial Practices A Review For Enhancing Strategic Competitiveness In Manufacturing Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 895–924. https://doi.org/10.63125/0yjss288

[35]. Matheson, G. O., Pacione, C., Shultz, R., & Klügl, M. (2015). Leveraging Human-Centered Design in Chronic Disease Prevention. *American journal of preventive medicine*, *48*(4), 472-479. https://doi.org/10.1016/j.amepre.2014.10.014

[36]. McEvoy, P., & Still, J. D. (2016). Contextualizing Mnemonic Phrase Passwords. In (Vol. NA, pp. 295-304). Springer International Publishing. https://doi.org/10.1007/978-3-319-41932-9_24

[37]. Md Arif Uz, Z., & Elmoon, A. (2023). Adaptive Learning Systems For English Literature Classrooms: A Review Of AI-Integrated Education Platforms. *International Journal of Scientific Interdisciplinary Research*, *4*(3), 56-86. https://doi.org/10.63125/a30ehr12

[38]. Md Arman, H. (2025). Artificial Intelligence-Driven Financial Analytics Models For Predicting Market Risk And Investment Decisions In U.S. Enterprises. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1066–1095. https://doi.org/10.63125/9csehp36

[39]. Md Ismail, H. (2022). Deployment Of AI-Supported Structural Health Monitoring Systems For In-Service Bridges Using IoT Sensor Networks. *Journal of Sustainable Development and Policy*, *1*(04), 01-30. https://doi.org/10.63125/j3sadb56

[40]. Md Ismail, H. (2024). Implementation Of AI-Integrated IOT Sensor Networks For Real-Time Structural Health Monitoring Of In-Service Bridges. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *4*(1), 33-71. https://doi.org/10.63125/0zx4ez88

[41]. Md Jakaria, T., Md, A., Zayadul, H., & Emdadul, H. (2025). Advances In High-Efficiency Solar Photovoltaic Materials: A Comprehensive Review Of Perovskite And Tandem Cell Technologies. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 201-225. https://doi.org/10.63125/5amnvb37

[42]. Md Mesbaul, H. (2024). Industrial Engineering Approaches to Quality Control In Hybrid Manufacturing A Review Of Implementation Strategies. *International Journal of Business and Economics Insights*, *4*(2), 01-30. https://doi.org/10.63125/3xcabx98

[43]. Md Mohaiminul, H. (2025). Federated Learning Models for Privacy-Preserving AI In Enterprise Decision Systems. *International Journal of Business and Economics Insights*, *5*(3), 238– 269. https://doi.org/10.63125/ry033286

[44]. Md Mominul, H. (2025). Systematic Review on The Impact Of AI-Enhanced Traffic Simulation On U.S. Urban Mobility And Safety. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 833–861. https://doi.org/10.63125/jj96yd66

[45]. Md Omar, F. (2024). Vendor Risk Management In Cloud-Centric Architectures: A Systematic Review Of SOC 2, Fedramp, And ISO 27001 Practices. *International Journal of Business and Economics Insights*, *4*(1), 01-32. https://doi.org/10.63125/j64vb122

[46]. Md Rezaul, K. (2021). Innovation Of Biodegradable Antimicrobial Fabrics For Sustainable Face Masks Production To Reduce Respiratory Disease Transmission. *International Journal of Business and Economics Insights*, *1*(4), 01–31. https://doi.org/10.63125/ba6xzq34

[47]. Md Rezaul, K. (2025). Optimizing Maintenance Strategies in Smart Manufacturing: A Systematic Review Of Lean Practices, Total Productive Maintenance (TPM), And Digital Reliability. *Review of Applied Science and Technology*, *4*(02), 176-206. https://doi.org/10.63125/np7nnf78

[48]. Md Rezaul, K., & Md Takbir Hossen, S. (2024). Prospect Of Using AI- Integrated Smart Medical Textiles For Real-Time Vital Signs Monitoring In Hospital Management & Healthcare Industry. *American Journal of Advanced Technology and Engineering Solutions*, *4*(03), 01-29. https://doi.org/10.63125/d0zkrx67

[49]. Md Rezaul, K., & Rony, S. (2025). A Framework-Based Meta-Analysis of Artificial Intelligence-Driven ERP Solutions For Circular And Sustainable Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 432-464. https://doi.org/10.63125/jbws2e49

[50]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[51]. Md Zahin Hossain, G., Md Khorshed, A., & Md Tarek, H. (2023). Machine Learning For Fraud Detection In Digital Banking: A Systematic Literature Review. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 37–61. https://doi.org/10.63125/913ksy63

[52]. Md. Hasan, I. (2025). A Systematic Review on The Impact Of Global Merchandising Strategies On U.S. Supply Chain Resilience. *International Journal of Business and Economics Insights*, *5*(3), 134–169. https://doi.org/10.63125/24mymg13

[53]. Md. Milon, M. (2025). A Systematic Review on The Impact Of NFPA-Compliant Fire Protection Systems On U.S. Infrastructure Resilience. *International Journal of Business and Economics Insights*, *5*(3), 324–352. https://doi.org/10.63125/ne3ey612

[54]. Md. Rabiul, K. (2025). Artificial Intelligence-Enhanced Predictive Analytics for Demand Forecasting In U.S. Retail Supply Chains. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 959–993. https://doi.org/10.63125/gbkf5c16

[55]. Md. Sakib Hasan, H. (2023). Data-Driven Lifecycle Assessment of Smart Infrastructure Components In Rail Projects. *American Journal of Scholarly Research and Innovation*, *2*(01), 167-193. https://doi.org/10.63125/wykdb306

[56]. Md. Sakib Hasan, H., & Abdul, R. (2025). Artificial Intelligence and Machine Learning Applications In Construction Project Management: Enhancing Scheduling, Cost Estimation, And Risk Mitigation. *International Journal of Business and Economics Insights*, *5*(3), 30–64. https://doi.org/10.63125/jrpjje59

[57]. Md. Tahmid Farabe, S. (2025). The Impact of Data-Driven Industrial Engineering Models On Efficiency And Risk Reduction In U.S. Apparel Supply Chains. *International Journal of Business and Economics Insights*, *5*(3), 353–388. https://doi.org/10.63125/y548hz02

[58]. Md.Kamrul, K., & Md Omar, F. (2022). Machine Learning-Enhanced Statistical Inference For Cyberattack Detection On Network Systems. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 65-90. https://doi.org/10.63125/sw7jzx60

[59]. Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would Share Their Password? *International Journal of Information Security and Privacy*, *2*(3), 71-83. https://doi.org/10.4018/jisp.2008070106

[60]. Mohammad Shoeb, A., & Reduanul, H. (2023). AI-Driven Insights for Product Marketing: Enhancing Customer Experience And Refining Market Segmentation. *American Journal of Interdisciplinary Studies*, *4*(04), 80-116. https://doi.org/10.63125/pzd8m844

[61]. Moin Uddin, M., & Hamza, S. (2025). Process Optimization Using Six Sigma Strategy In Garment Manufacturing. *Journal of Sustainable Development and Policy*, *1*(01), 346-364. https://doi.org/10.63125/58969k32

[62]. Moin Uddin, M., & Md, N. (2025). AI-Driven Optimization of Warehouse Layout and Material Handling: A Quantitative Study on Efficiency and Space Utilization. *Review of Applied Science and Technology*, *4*(02), 233-273. https://doi.org/10.63125/bgxb1z53

[63]. Momena, A. (2025). Impact Of Predictive Machine Learning Models on Operational Efficiency And Consumer Satisfaction In University Dining Services. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 376-403. https://doi.org/10.63125/5tjkae44

[64]. Momena, A., & Sai Praveen, K. (2024). A Comparative Analysis of Artificial Intelligence-Integrated BI Dashboards For Real-Time Decision Support In Operations. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 158-191. https://doi.org/10.63125/47jjv310

[65]. Mubashir, I. (2025). Analysis Of AI-Enabled Adaptive Traffic Control Systems For Urban Mobility Optimization Through Intelligent Road Network Management. *Review of Applied Science and Technology*, *4*(02), 207-232. https://doi.org/10.63125/358pgg63

[66]. Mubashir, I., & Jahid, M. K. A. S. R. (2023). Role Of Digital Twins and Bim In U.S. Highway Infrastructure Enhancing Economic Efficiency And Safety Outcomes Through Intelligent Asset Management. *American Journal of Advanced Technology and Engineering Solutions*, *3*(03), 54-81. https://doi.org/10.63125/hftt1g82

[67]. Omar Muhammad, F. (2024). Advanced Computing Applications in BI Dashboards: Improving Real-Time Decision Support For Global Enterprises. *International Journal of Business and Economics Insights*, *4*(3), 25-60. https://doi.org/10.63125/3x6vpb92

[68]. Pankaz Roy, S. (2025). Artificial Intelligence Based Models for Predicting Foodborne Pathogen Risk In Public Health Systems. *International Journal of Business and Economics Insights*, *5*(3), 205–237. https://doi.org/10.63125/7685ne21

[69]. Rahman, S. M. T. (2025). Strategic Application of Artificial Intelligence In Agribusiness Systems For Market Efficiency And Zoonotic Risk Mitigation. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 862–894. https://doi.org/10.63125/8xm5rz19

[70]. Rakibul, H. (2025). The Role of Business Analytics In ESG-Oriented Brand Communication: A Systematic Review Of Data-Driven Strategies. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1096– 1127. https://doi.org/10.63125/4mchj778

[71]. Razia, S. (2022). A Review Of Data-Driven Communication In Economic Recovery: Implications Of ICT-Enabled Strategies For Human Resource Engagement. *International Journal of Business and Economics Insights*, *2*(1), 01-34. https://doi.org/10.63125/7tkv8v34

[72]. Razia, S. (2023). AI-Powered BI Dashboards In Operations: A Comparative Analysis For Real-Time Decision Support. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 62–93. https://doi.org/10.63125/wqd2t159

[73]. Reduanul, H. (2023). Digital Equity and Nonprofit Marketing Strategy: Bridging The Technology Gap Through Ai-Powered Solutions For Underserved Community Organizations. *American Journal of Interdisciplinary Studies*, *4*(04), 117-144. https://doi.org/10.63125/zrsv2r56

[74]. Reduanul, H. (2025). Enhancing Market Competitiveness Through AI-Powered SEO And Digital Marketing Strategies In E-Commerce. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 465-500. https://doi.org/10.63125/31tpjc54

[75]. Rony, M. A. (2025). AI-Enabled Predictive Analytics And Fault Detection Frameworks For Industrial Equipment Reliability And Resilience. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 705–736. https://doi.org/10.63125/2dw11645

[76]. Saba, A. (2025). Artificial Intelligence Based Models For Secure Data Analytics And Privacy-Preserving Data Sharing In U.S. Healthcare And Hospital Networks. *International Journal of Business and Economics Insights*, *5*(3), 65–99. https://doi.org/10.63125/wv0bqx68

[77]. Sabbir Alom, S., Marzia, T., Nazia, T., & Shamsunnahar, C. (2025). MACHINE LEARNING IN BUSINESS INTELLIGENCE: FROM DATA MINING TO STRATEGIC INSIGHTS IN MIS. *Review of Applied Science and Technology*, *4*(02), 339-369. https://doi.org/10.63125/drb8py41

[78]. Sabuj Kumar, S. (2025). AI Driven Predictive Maintenance in Petroleum And Power Systems Using Random Forest Regression Model For Reliability Engineering Framework. *American Journal of Scholarly Research and Innovation*, *4*(01), 363-391. https://doi.org/10.63125/477x5t65

[79]. Sadia, T. (2022). Quantitative Structure-Activity Relationship (QSAR) Modeling of Bioactive Compounds From Mangifera Indica For Anti-Diabetic Drug Development. *American Journal of Advanced Technology and Engineering Solutions*, *2*(02), 01-32. https://doi.org/10.63125/ffkez356

[80]. Sadia, T. (2023). Quantitative Analytical Validation of Herbal Drug Formulations Using UPLC And UV-Visible Spectroscopy: Accuracy, Precision, And Stability Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *3*(1), 01–36. https://doi.org/10.63125/fxqpds95

[81]. Sai Praveen, K. (2025). AI-Driven Data Science Models for Real-Time Transcription And Productivity Enhancement In U.S. Remote Work Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 801–832. https://doi.org/10.63125/gzyw2311

[82]. Samaras, G. M., & Horst, R. L. (2005). A systems engineering perspective on the human-centered design of health information systems. *Journal of biomedical informatics*, *38*(1), 61-74. https://doi.org/10.1016/j.jbi.2004.11.013

[83]. Segall, N., Bonifacio, A. S., Barbeito, A., Schroeder, R. A., Perfect, S. R., Wright, M. C., Emery, J. D., Atkins, B. Z., Taekman, J. M., & Mark, J. B. (2016). Operating Room-to-ICU Patient Handovers: A Multidisciplinary Human-Centered Design Approach. *Joint Commission journal on quality and patient safety*, *42*(9), 400-409. https://doi.org/10.1016/s1553-7250(16)42081-7

[84]. Shaikat, B. (2025). Artificial Intelligence–Enhanced Cybersecurity Frameworks for Real-Time Threat Detection In Cloud And Enterprise. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 737–770. https://doi.org/10.63125/yq1gp452

[85]. Sheratun Noor, J., Md Redwanul, I., & Sai Praveen, K. (2024). The Role of Test Automation Frameworks In Enhancing Software Reliability: A Review Of Selenium, Python, And API Testing Tools. *International Journal of Business and Economics Insights*, *4*(4), 01–34. https://doi.org/10.63125/bvv8r252

[86]. Shin, D.-H. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. *Telematics and Informatics*, *31*(4), 519-531. https://doi.org/10.1016/j.tele.2014.02.003

[87]. Still, J. D. (2016). Cybersecurity needs you. *Interactions*, *23*(3), 54-58. https://doi.org/10.1145/2899383

[88]. Still, J. D., Cain, A. A., & Schuster, D. (2017). Human-centered authentication guidelines. *Information & Computer Security*, *25*(4), 437-453. https://doi.org/10.1108/ics-04-2016-0034

[89]. Syed Zaki, U. (2025). Digital Engineering and Project Management Frameworks For Improving Safety And Efficiency In US Civil And Rail Infrastructure. *International Journal of Business and Economics Insights*, *5*(3), 300–329. https://doi.org/10.63125/mxgx4m74

[90]. Tanev, G., Tzolov, P., & Apiafi, R. (2015). A Value Blueprint Approach to Cybersecurity in Networked Medical Devices. *Technology Innovation Management Review*, *5*(6), 17-25. https://doi.org/10.22215/timreview/903

[91]. Thiel, S., Mitchell, J., & Williams, J. (2016). Coordination or Collision? The Intersection of Diabetes Care, Cybersecurity, and Cloud-Based Computing. *Journal of diabetes science and technology*, *11*(2), 195-197. https://doi.org/10.1177/1932296816676189

[92]. Tonoy Kanti, C. (2025). AI-Powered Deep Learning Models for Real-Time Cybersecurity Risk Assessment In Enterprise It Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 675–704. https://doi.org/10.63125/137k6y79

[93]. Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. M. (2017). AAAI Workshops - Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams.

[94]. Webb, T., & Dayal, S. (2017). Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia. *Computer Law & Security Review*, *33*(4), 559-563. https://doi.org/10.1016/j.clsr.2017.05.004

[95]. Williams, P. A. H., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.)*, *8*(NA), 305-316. https://doi.org/10.2147/mder.s50048

[96]. Yang, J.-G., & Zhang, J. (2016). Improving the postoperative handover process in the intensive care unit of a tertiary teaching hospital. *Journal of clinical nursing*, *25*(7-8), 1062-1072. https://doi.org/10.1111/jocn.13115

[97]. Zayadul, H. (2025). IoT-Driven Implementation of AI Predictive Models For Real-Time Performance Enhancement of Perovskite And Tandem Photovoltaic Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1031–1065. https://doi.org/10.63125/ar0j1y19

[98]. Zobayer, E. (2025). Impact of Advanced Lubrication Management Systems on Equipment Longevity And Operational Efficiency In Smart Manufacturing Environments. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 618–653. https://doi.org/10.63125/r0n6bc88