

DOI: https://doi.org/10.48009/1_iis_2026_131

Socio-technical determinants of lightweight cryptography adoption and key management strategies for securing smart home IoT networks: An information systems perspective

Oluwatosin Olaore, *Dakota State University* James.olaore@trojans.dsu.edu

Ahmed Alghamdi, *Dakota State University*, ahmed.alghamdi@trojans.dsu.edu

Abeer Alkhwaldi, *Dakota State University*, Abeer.Alkhwaldi@dsu.edu

Abstract

Smart home environments depend on interconnected devices that handle sensitive personal data under strict computational and energy limits. Lightweight cryptography offers an efficient security solution for these devices, yet its adoption relies on more than technical performance. This review systematically synthesizes forty-six peer-reviewed studies across information systems, cybersecurity, and smart home research to provide a comprehensive explanation of how lightweight cryptography and key management are adopted in consumer smart home ecosystems. The evidence shows that adoption is driven by user perceptions of usefulness, ease of use, trust, and risk; vendor practices involving transparency, update integrity, and security governance; environmental expectations shaped by regulation, industry norms, and interoperability requirements; and technical qualities such as algorithmic efficiency, computational overhead, energy consumption, and practical key management under device-level constraints. The review develops a socio-technical model that specifies how these determinants interact to shape user confidence, vendor implementation decisions, and long-term security outcomes. This model offers a clear conceptual foundation for vendors, policymakers, standards bodies, and researchers seeking to strengthen the security, reliability, and governance of smart home IoT networks.

Keywords: Lightweight cryptography; Key management strategies; Smart home IoT security; Socio technical determinants; Technology adoption; Security governance.

Introduction

Smart home environments depend on interconnected Internet of Things devices that continuously collect and process sensitive personal information while operating under strict computational and energy constraints. These systems generate behavioral, contextual, and household level data that intensify privacy concerns and perceived risk in digital ecosystems (Bélanger & Crossler, 2011). Users cannot inspect the cryptographic protections embedded in these devices and instead form judgments from observable indicators such as performance, reliability, interface clarity, vendor communication, and institutional assurances. Empirical research demonstrates that individuals evaluate privacy and security through visible signals rather than through technical examination of underlying mechanisms (Featherman & Pavlou, 2003; McKnight et al., 2002). This reality makes lightweight cryptography a socio technical adoption challenge rather than a technical engineering problem, because user confidence is shaped by interpretation, trust, and perceived reliability rather than by direct assessment of algorithmic strength. Lightweight cryptography

comprises cryptographic mechanisms engineered to function effectively under severe constraints on processing power, memory, and energy, which makes adoption dependent on both human perception and technical feasibility.

Lightweight cryptography delivers efficient protection for resource constrained devices, yet its adoption is governed by behavioral, organizational, environmental, and technical conditions. Information systems research establishes that perceived usefulness, perceived ease of use, trust, and perceived risk determine acceptance when users cannot directly evaluate underlying mechanisms (Davis, 1989; Featherman & Pavlou, 2003; McKnight et al., 2002). Vendor practices including transparency, update integrity, and security governance shape user confidence and implementation feasibility by signaling competence and commitment to protection (Johnston & Warkentin, 2010; Lau et al., 2018). Regulatory expectations and industry norms define standards for acceptable protection, accountability, and interoperability and structure both vendor strategies and user expectations (Bélanger & Crossler, 2011; Wang et al., 2020). Technical feasibility exerts a decisive influence on perceived usefulness and trust because performance constraints determine whether security mechanisms appear reliable, unobtrusive, and aligned with user expectations. Key management processes such as key generation, distribution, storage, rotation, and revocation reinforce these perceptions by determining whether protection is maintained consistently over time. Recent work confirms that practical key management is essential for sustaining security in constrained Internet of Things environments (Bettayeb et al., 2023; Dhakare et al., 2024).

Despite substantial research on Internet of Things security, lightweight cryptography, and smart home adoption, the literature remains fragmented. Prior studies typically examine behavioral, organizational, environmental, or technical determinants in isolation rather than analyzing how these forces interact to shape adoption outcomes (Bélanger & Crossler, 2011; Davis, 1989; Johnston & Warkentin, 2010). This separation obstructs theoretical progress because it conceals the ways in which user perceptions, vendor practices, regulatory pressures, and device level constraints jointly influence adoption and implementation. Existing frameworks do not integrate governance practices, regulatory expectations, and resource limitations with user interpretations of embedded cryptographic mechanisms, nor do they incorporate the practical challenges of key management in constrained environments. Recent systematic reviews reinforce this diagnosis and call for integrated socio technical explanations that connect technical mechanisms with behavioral and organizational determinants (Ansari & Ali, 2025; Haider et al., 2026; Rana et al., 2022). The socio technical model advanced in this review addresses these limitations by unifying behavioral, organizational, environmental, and technical determinants into a single explanatory structure. Its originality lies in specifying how contextual forces and vendor practices shape user perceptions and how technical feasibility conditions the influence of those perceptions on adoption, relationships that prior information systems and cybersecurity research has not articulated.

This review synthesizes forty-six studies across information systems, cybersecurity, and smart home research to develop this integrated model. It makes three concrete contributions. First, it provides a unified socio technical explanation of lightweight cryptography and key management adoption in consumer smart home ecosystems. Second, it clarifies how contextual and technical conditions structure user perceptions and implementation feasibility in resource constrained environments. Third, it offers targeted guidance for vendors, policymakers, and researchers who seek to strengthen security, reliability, and governance in smart home deployments. Although prior research has examined behavioral, organizational, environmental, or technical factors in isolation, no existing review integrates these determinants into a unified socio-technical explanation of lightweight cryptography and key-management adoption in smart home ecosystems. This review is the first to synthesize forty-six studies across information systems, cybersecurity, and smart home research to show how these determinants interact, why they jointly shape user confidence and vendor implementation decisions, and how technical feasibility mediates the influence of organizational and

environmental conditions on user perceptions. By connecting cryptographic performance, key-management practicality, vendor governance, regulatory expectations, and user-level interpretations into a single explanatory model, this review provides a level of conceptual integration not present in prior frameworks.

Research Question

This review addresses the following research question:

RQ1: How do behavioral, organizational, environmental, and technical determinants interact to shape the adoption and implementation of lightweight cryptography and key management in smart home environments?

The contribution of this review lies in integrating these determinants into a single socio-technical explanation of adoption, extending prior work that has typically examined these factors independently (Bélanger & Crossler, 2011; Davis, 1989; McKnight et al., 2002). This integration provides a unified account of how human perceptions, institutional practices, contextual pressures, and device level constraints jointly shape adoption outcomes, a relationship that earlier research has not defined with precision.

Theoretical Background

Technology adoption research explains how individuals evaluate security mechanisms they cannot directly observe. Although users do not select cryptographic algorithms directly, they do adopt devices whose embedded protections they evaluate through perceived usefulness, ease of use, trust, and risk (Davis, 1989; Featherman & Pavlou, 2003). Thus, adoption occurs at the device level, but perceptions of cryptographic adequacy shape device acceptance and continued use. Perceived usefulness and perceived ease of use remain central predictors of intention and use (Davis, 1989). In smart home environments, these perceptions arise not from direct inspection of cryptographic strength but from observable cues such as device responsiveness, reliability, interface clarity, and vendor communication. Prior work shows that trust in vendor competence and integrity becomes essential when users lack the expertise or access needed to evaluate algorithms or key lifecycle processes (McKnight et al., 2002). Perceived risk and privacy concern further shape whether security features are interpreted as protective or intrusive (Bélanger & Crossler, 2011; Featherman & Pavlou, 2003; Y. Liu et al., 2021). These behavioral constructs form the foundation for understanding how users interpret embedded security mechanisms in smart home ecosystems. These behavioral constructs form the interpretive framework through which users judge the adequacy of embedded security mechanisms, even when the underlying cryptographic processes remain inaccessible.

Organizational and environmental perspectives extend this behavioral foundation by explaining how institutional practices and contextual pressures shape user confidence. Vendor transparency, update integrity, and security governance influence perceptions of data handling, cryptographic protections, and long-term reliability (Chan et al., 2005; J. M. Haney & Furman, 2023; Johnston & Warkentin, 2010; Lau et al., 2018). Regulatory frameworks and industry norms define expectations for privacy, accountability, interoperability, and baseline security quality. These expectations shape vendor strategies and influence how users interpret assurances of protection and redress (Bélanger & Crossler, 2011; Wang et al., 2020; Y. Yang et al., 2023). Together, these organizational and environmental conditions establish the institutional setting within which lightweight cryptography and key management are evaluated, adopted, and maintained.

Technical determinants ground the socio technical dynamics of lightweight cryptography and key management in the material limits of smart home devices. These devices operate under strict constraints on processing power, memory, energy, and bandwidth, which requires cryptographic mechanisms that can deliver credible protection without impairing responsiveness or stability (Gu et al., 2019; H. Liu et al., 2017). The practicality of key management is equally decisive because key generation, distribution, storage, rotation, and revocation must remain secure and unobtrusive while still being manageable for vendors and service providers. Key revocation presents a particular challenge because revocation information must propagate across heterogeneous and intermittently connected devices that cannot support continuous communication or computationally intensive rekeying. System quality theory links performance, reliability, and service continuity to satisfaction and continued use ("The DeLone and McLean Model of Information Systems Success," 2003), which positions cryptographic design choices and key lifecycle processes as integral components of overall system behavior. Algorithmic efficiency, computational overhead, energy consumption, and interoperability directly shape whether security mechanisms can operate without degrading device performance. These technical determinants influence how users interpret usefulness, ease of use, trustworthiness, and risk, which makes technical feasibility a central driver of adoption in resource constrained smart home ecosystems.

Collectively, these interdependent socio-technical factors provide a coherent theoretical foundation for understanding the adoption of lightweight cryptography and key management in smart home environments. They also demonstrate the necessity of an integrated socio technical model that explains how these determinants interact to shape adoption and implementation success, a perspective that prior research has not fully articulated.

Systematic Review Method

This review followed a structured protocol designed to ensure rigor, transparency, and reproducibility. The procedure consisted of database selection, search strategy development, screening, quality appraisal, and thematic synthesis. Each stage applied explicit criteria that support the validity of the final socio technical model. This protocol aligns with established practices in information systems and cybersecurity research and ensures that the resulting synthesis rests on a defensible evidentiary base.

Database Selection

Four databases were selected to capture the breadth of research across information systems, cybersecurity, and human computer interaction. Scopus and Web of Science provided comprehensive coverage of peer reviewed work in information systems. IEEE Xplore and the ACM Digital Library ensured inclusion of technical studies on cryptography, key management, and smart home security. This combination secured representation of both behavioral and technical perspectives. It also ensured that studies addressing privacy, trust, risk, and system quality were captured alongside research on cryptographic mechanisms and device level constraints (Ammar et al., 2018; Conti et al., 2018; Sookhak et al., 2019).

Search Strategy

Search strings combined terms related to smart home security, Internet of Things adoption, lightweight cryptography, key management, technology acceptance, trust, perceived risk, vendor transparency, update integrity, interoperability, and system quality. Boolean operators linked these concepts to balance recall and precision. The search was limited to peer reviewed journal articles and conference papers published in English, with no restriction on publication year to capture the evolution of the field. This approach ensured that foundational work on privacy, trust, and security perceptions (Barth & De Jong, 2017; Zheng et al.,

2018) was included alongside recent advances in lightweight cryptography and key management (Bettayeb et al., 2023; Dhakare et al., 2024).

Search Strings and Search Dates

Searches were conducted across all four databases in February 2026. Search strings combined terms such as “smart home security,” “Internet of Things adoption,” “lightweight cryptography,” “key management,” “perceived risk,” “trust,” “vendor transparency,” and “system quality,” consistent with the constructs identified in prior IS and cybersecurity research (Davis, 1989; Johnston & Warkentin, 2010; McKnight et al., 2002). Additional terms captured emerging concerns related to device reliability, update behavior, and privacy preserving analytics (Chakravorty et al., 2013; J. Haney et al., 2025; He et al., 2019).

Inclusion and Exclusion Criteria

Studies were included if they examined smart home environments or Internet of Things security and addressed cryptographic mechanisms, key management, or behavioral, organizational, environmental, or technical determinants of adoption. Studies were excluded if they focused solely on cryptographic design without socio technical relevance, addressed unrelated Internet of Things domains, lacked methodological detail, or were not peer reviewed. These criteria ensured that each study contributed directly to the development of the socio technical model. This approach also prevented the inclusion of work that addressed industrial, vehicular, or medical Internet of Things contexts without relevance to consumer smart homes (Harvey et al., 2020; Hossain et al., 2015).

Screening Process

The search produced one thousand two hundred forty-seven records. After removing three hundred twelve duplicates, nine hundred thirty-five titles and abstracts were screened. One hundred forty-two full texts were assessed, and forty-six studies met all criteria, as illustrated in Figure 1. This process ensured that the final corpus reflected both methodological rigor and substantive relevance. The screening also incorporated studies addressing vulnerabilities, risks, and countermeasures in smart homes (Bugeja et al., 2016; Hammi et al., 2022), as well as research on user perceptions of device trustworthiness and privacy (Y. Liu et al., 2021; Nemec Zlatolas et al., 2022).

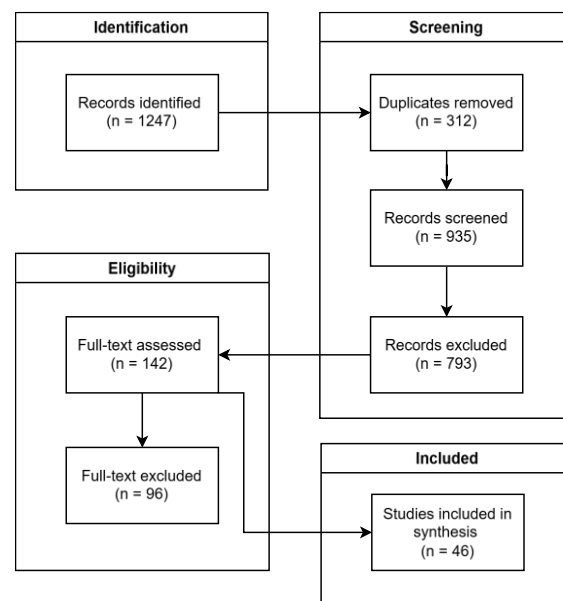


Figure 1. PRISMA 2020 flow diagram illustrating the identification, screening, exclusion, and final inclusion of studies

Quality Appraisal

Quality appraisal evaluated methodological clarity, empirical grounding, and relevance to the socio technical determinants of lightweight cryptography and key management. Studies lacking sufficient methodological detail, empirical evidence, or conceptual alignment were excluded. Disagreements were resolved through discussion until consensus was reached. This appraisal ensured that the synthesis rested on studies that were both credible and directly aligned with the review objectives. This process also ensured that studies addressing update integrity, vendor behavior, and user experience were appropriately weighted (J. M. Haney & Furman, 2023; H. Liu et al., 2017).

Coding and Synthesis

A thematic synthesis approach was used. Each study was coded into behavioral, organizational, environmental, and technical determinant categories. Three researchers independently coded all studies. Disagreements were resolved through discussion until consensus was reached, consistent with qualitative synthesis practices in information systems research (Bélanger & Crossler, 2011; Lau et al., 2018). Codes were refined as patterns emerged and were grouped into higher order themes within each category. These themes were integrated across information systems, cybersecurity, and smart home research to construct the socio technical model that links determinants to adoption and implementation success. This synthesis incorporated insights from studies on user acceptance (H. Yang et al., 2017; Y. Yang et al., 2023), device level vulnerabilities (H. Liu et al., 2017), context aware security (Khanpara et al., 2023), and hybrid cryptographic approaches (Haider et al., 2026; Rana et al., 2022).

Finding

The review identified four categories of determinants that shape adoption of lightweight cryptography and key management in smart home environments. These categories are behavioral, organizational, environmental, and technical, as summarized in Table 1. Together they explain how user perceptions, vendor practices, contextual expectations, and technical constraints influence adoption and implementation. The findings also reveal that these determinants operate across multiple layers of the smart home ecosystem, from device level interactions to institutional and regulatory structures, confirming the socio technical nature of embedded security adoption (Ammar et al., 2018; Sicari et al., 2015).

Behavioral determinants reflect how users interpret security mechanisms they cannot directly observe. Perceived usefulness, perceived ease of use, trust, and perceived risk consistently emerged as central influences on adoption. Users rely on device performance, interface clarity, and vendor communication to form judgments about security, which aligns with established information systems research on technology acceptance and privacy concern (Bélanger & Crossler, 2011; Davis, 1989; Featherman & Pavlou, 2003; McKnight et al., 2002). Users' interpretations of privacy and control also influence perceived risk, consistent with research showing that smart home privacy decisions depend heavily on perceived agency and contextual cues (Keshavarz & Anwar, 2018). Studies on smart speaker privacy, user perceptions of device intelligence, and the privacy paradox reinforce that users routinely depend on observable cues rather than technical inspection when evaluating embedded protections (Barth & De Jong, 2017; Lau et al., 2018; Zheng et al., 2018). These findings confirm that adoption of embedded security mechanisms is shaped by cognitive and affective evaluations rather than by direct assessment of cryptographic strength.

Organizational determinants capture the role of vendor practices in shaping user confidence and implementation feasibility. Transparency about data handling and cryptographic protections, the integrity and reliability of update processes, and the presence of coherent security governance structures influence whether users view lightweight cryptography and key management as credible and trustworthy. Studies

show that disruptions during updates, opaque communication, or inconsistent governance practices undermine confidence even when technical protections are strong (J. M. Haney & Furman, 2023; Johnston & Warkentin, 2010; Lau et al., 2018). Research on smart home user experiences, vendor communication failures, and device update behavior further demonstrates that organizational practices shape trust more strongly than technical specifications (Bringhenti et al., 2022; He et al., 2019; Marghalani et al., 2025).

Environmental determinants reflect the broader institutional context in which smart home security decisions occur. Regulatory expectations, industry norms, and interoperability requirements shape both vendor strategies and user perceptions of accountability, privacy protection, and ecosystem reliability. Early conceptual models of smart home privacy and security highlight that environmental expectations shape both vendor strategies and user interpretations of acceptable protection (Jacobsson & Davidsson, 2015). These contextual forces influence what users consider acceptable security and what vendors consider feasible or necessary to implement (Bélanger & Crossler, 2011; Wang et al., 2020; Y. Yang et al., 2023). Studies on smart home vulnerabilities, risk communication, and privacy preserving analytics show that environmental pressures often determine whether lightweight cryptography and key management are prioritized in product design (Bugeja et al., 2016; Chakravorty et al., 2013; Hammi et al., 2022). Broader analyses of smart home security challenges emphasize that ecosystem-level vulnerabilities and inconsistent vendor practices shape both regulatory expectations and user assumptions about risk (Khawla & Tomader, 2018). The findings show that environmental pressures often determine whether lightweight cryptography and key management are prioritized in product design.

Technical determinants define the feasibility of deploying lightweight cryptography and key management in resource constrained devices. Algorithmic efficiency, computational overhead, energy consumption, and interoperability determine whether security mechanisms can operate without degrading performance or reliability. These constraints are amplified in distributed smart home environments where computation is increasingly offloaded to edge devices, introducing new attack surfaces and performance security tradeoffs (Garg et al., 2021). Key management practicality emerged as a particularly influential factor, since key generation, distribution, rotation, and revocation must be secure, efficient, and largely invisible to users while remaining manageable for vendors (Gu et al., 2019; H. Liu et al., 2017). In this review, key management practicality refers to the feasibility of performing key generation, distribution, storage, rotation, and revocation under device-level constraints such as limited processing power, intermittent connectivity, and energy restrictions (Gu et al., 2019; H. Liu et al., 2017). Device-level security research further shows that anomaly detection and intelligent monitoring systems play an increasingly important role in maintaining trust and perceived reliability in smart home environments (Rahim et al., 2023). Recent evaluations of lightweight and hybrid cryptographic algorithms confirm that performance constraints directly shape adoption feasibility in smart home environments (Haider et al., 2026; Radhakrishnan et al., 2024; Rana et al., 2022). These constraints determine whether key lifecycle processes can operate reliably and unobtrusively in smart home environments. These findings confirm that technical feasibility is not merely a background condition but a central determinant of adoption and implementation success.

Collectively, these four determinant categories provide a comprehensive explanation of how lightweight cryptography and key management are evaluated, adopted, and implemented in smart home environments. They also align with broader analyses of Internet of Things security challenges, including device heterogeneity, inconsistent vendor practices, and the difficulty of maintaining secure communication across distributed ecosystems (Anwar et al., 2020; Hossain et al., 2015; Hwang, 2015). These findings establish the empirical foundation for the integrated socio technical model developed in the next section.

Table 1. Determinant Categories, Associated Constructs, and Key Supporting Literature

Determinant Category	Core Constructs	Representative Studies
Behavioral	Perceived usefulness, perceived ease of use, trust, perceived risk	Davis (1989). McKnight et al. (2002). Featherman and Pavlou (2003).
Organizational	Vendor transparency, update integrity, security governance	Lau et al. (2018). Haney and Furman (2023). Johnston and Warkentin (2010).
Environmental	Regulatory expectations, industry norms, interoperability expectations.	Bélanger and Crossler (2011). Wang et al. (2020).
Technical	Algorithmic efficiency, computational overhead, energy consumption, interoperability, key management practicality.	Liu et al. (2017); Gu et al. (2019); Radhakrishnan et al. (2024); Haider et al. (2026); Rana et al. (2022)

Integrated Socio-Technical Model

The integrated socio technical model explains adoption of lightweight cryptography and key management as the result of four determinant categories that operate in continuous interaction, as shown in Figure 2. Behavioral determinants remain the most immediate pathway to adoption because users rely on perceived usefulness, perceived ease of use, trust, and perceived risk when evaluating security mechanisms, they cannot directly inspect (Davis, 1989; Featherman & Pavlou, 2003; McKnight et al., 2002). These perceptions are shaped by the technical, organizational, and environmental conditions that define how security mechanisms behave in practice. Studies on smart home user experience, privacy judgments, and device trustworthiness confirm that users interpret security through observable performance rather than through technical analysis (Barth & De Jong, 2017; Bringhenti et al., 2022; Zheng et al., 2018).

Organizational determinants consist of vendor transparency, update integrity, and security governance. These practices influence confidence in protection, reliability, and the credibility of key lifecycle processes (Johnston & Warkentin, 2010; Lau et al., 2018). Research on vendor communication, device update failures, and governance inconsistencies shows that organizational practices often determine whether users interpret embedded protections as competent or unreliable (J. M. Haney & Furman, 2023; He et al., 2019; Marghalani et al., 2025). Environmental determinants include regulatory expectations and industry norms that define acceptable security, accountability, and privacy protection. Regulatory expectations shape vendor strategies and user assumptions about acceptable protection, accountability, and interoperability, reinforcing the institutional pressures identified in prior IS research (Bélanger & Crossler, 2011; Wang et al., 2020). These contextual forces shape vendor strategies and influence user expectations (Bélanger & Crossler, 2011; Wang et al., 2020). Environmental pressures also reflect broader concerns about smart home vulnerabilities, data misuse, and ecosystem reliability (Bugeja et al., 2016; Hammi et al., 2022; Sicari et al., 2015).

Technical determinants establish feasibility. Algorithmic efficiency, computational overhead, energy consumption, interoperability, and the practicality of key generation, distribution, rotation, and revocation determine whether lightweight cryptography and key management can operate without impairing performance (Gu et al., 2019; H. Liu et al., 2017). Recent evaluations of lightweight and hybrid cryptographic algorithms demonstrate that performance constraints directly shape adoption feasibility in smart home environments (Haider et al., 2026; Radhakrishnan et al., 2024; Rana et al., 2022). These technical conditions directly influence behavioral constructs. When computational overhead slows device responsiveness, users interpret the delay as reduced usefulness. When energy intensive key processes shorten battery life, users perceive the device as less easy to use. When interoperability limitations cause device errors, users experience heightened perceived risk and diminished trust in vendor competence. These

interactions demonstrate that technical feasibility mediates the influence of organizational practices on behavioral perceptions. Studies on device heterogeneity, context aware security, and resource constrained communication confirm that technical limitations shape user experience and trust formation (Hossain et al., 2015; Hwang, 2015; Khanpara et al., 2023).

The model positions adoption as the central driver of implementation success and advances information systems theory by specifying how organizational and environmental conditions shape behavioral evaluations and how technical feasibility transmits the influence of vendor practices into user perceptions. This model also aligns with broader analyses of smart home security ecosystems, which emphasize that adoption outcomes depend on the alignment of human interpretation, institutional structures, and material constraints (Anwar et al., 2020; Harvey et al., 2020; Ortega, 2024). The model therefore provides a coherent explanation of how lightweight cryptography and key management succeed or fail in consumer smart home environments.

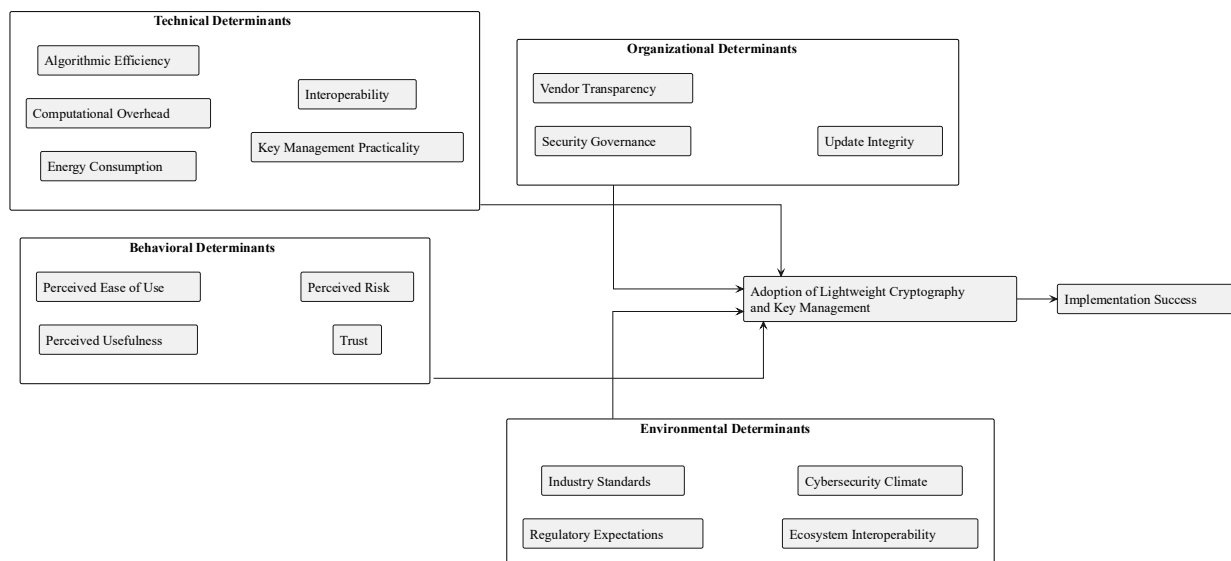


Figure 2. Socio-Technical Model of Lightweight Cryptography and Key Management Adoption and Implementation Success

Discussion

The findings demonstrate that adoption of lightweight cryptography and key management in smart home environments is a socio-technical process shaped by continuous interaction among behavioral, organizational, environmental, and technical determinants. Users rely on perceived usefulness, perceived ease of use, trust, and perceived risk when evaluating security mechanisms they cannot directly observe (Davis, 1989; Featherman & Pavlou, 2003; McKnight et al., 2002). These perceptions are formed through the technical behavior of devices, the clarity of vendor communication, and the institutional expectations that define acceptable protection. Studies on smart home privacy judgments, device trustworthiness, and user experience confirm that individuals interpret embedded protections through observable performance and communication cues rather than through technical inspection (Barth & De Jong, 2017; Bringhenti et al., 2022; Zheng et al., 2018).

While IoT adoption research explains device-level acceptance, these frameworks do not account for embedded cryptographic mechanisms or key lifecycle processes. This review extends that work by showing how perceptions of invisible security functions are shaped by vendor transparency, update integrity, and technical feasibility (J. M. Haney & Furman, 2023; Lau et al., 2018). Research on device update failures, inconsistent governance, and opaque communication further demonstrates that organizational practices strongly influence whether users interpret embedded protections as credible or unreliable (He et al., 2019; Marghalani et al., 2025).

Organizational determinants shape these perceptions by influencing how users interpret security assurances. Transparency, update integrity, and governance determine whether lightweight cryptography and key management are viewed as credible protections or as uncertain mechanisms that may fail in practice (J. M. Haney & Furman, 2023; Johnston & Warkentin, 2010; Lau et al., 2018). Environmental expectations reinforce these interpretations by establishing regulatory and normative boundaries that guide vendor decisions and shape user assumptions about privacy, accountability, and interoperability (Bélanger & Crossler, 2011; Wang et al., 2020). Environmental pressures also reflect broader concerns about smart home vulnerabilities, data misuse, and ecosystem reliability, which influence both vendor strategies and user expectations (Bugeja et al., 2016; Hammi et al., 2022; Sicari et al., 2015).

Technical determinants anchor these socio-technical dynamics. Algorithmic efficiency, computational overhead, energy consumption, and interoperability determine whether security mechanisms operate without degrading performance (Gu et al., 2019; H. Liu et al., 2017). These constraints directly reshape behavioral constructs. When computational overhead slows responsiveness, users perceive reduced usefulness. When key management processes shorten battery life, users perceive reduced ease of use. When interoperability failures occur, users experience heightened risk and diminished trust. Technical feasibility therefore mediates the influence of organizational practices on behavioral evaluations. Evaluations of lightweight and hybrid cryptographic algorithms confirm that performance constraints directly shape adoption feasibility in smart home environments (Haider et al., 2026; Radhakrishnan et al., 2024; Rana et al., 2022). Studies on device heterogeneity, context-aware security, and resource constrained communication further demonstrate that technical limitations shape user experience and trust formation (Hossain et al., 2015; Hwang, 2015; Khanpara et al., 2023).

Taken together, these interactions show that adoption depends on the alignment of technical performance, credible vendor practices, and the broader institutional context that shapes user interpretation. Misalignment between technical feasibility, vendor governance, and environmental expectations creates contradictory signals that elevate perceived risk even when cryptographic strength is high (Featherman & Pavlou, 2003; Johnston & Warkentin, 2010). Conversely, when efficient performance aligns with transparent communication and institutional assurances, users interpret embedded protections as credible despite lacking direct visibility into algorithmic processes. This socio-technical perspective aligns with broader analyses of smart home security ecosystems, which emphasize that adoption outcomes emerge from the interplay between user cognition, governance structures, and device-level constraints (Anwar et al., 2020; Harvey et al., 2020; Ortega, 2024). The findings therefore clarify that embedded security mechanisms must be understood as components of a broader system shaped by user cognition, vendor behavior, regulatory expectations, and device level limitations.

Theoretical Implications

This review advances information systems theory by demonstrating that lightweight cryptography and key management function as socio-technical constructs whose adoption depends on how users interpret system

behavior within the constraints set by vendor practices, regulatory expectations, and device capabilities. This extends technology acceptance research by demonstrating that user judgments depend on observable system behavior and vendor communication when the underlying technology is inaccessible to direct evaluation (Davis, 1989). It also clarifies that performance indicators such as latency, responsiveness, and battery impact serve as proxies for cryptographic adequacy in user decision making (Bringhenti et al., 2022; Zheng et al., 2018). It strengthens trust theory by showing that trust in vendor competence and integrity becomes essential when users cannot assess algorithmic strength or key lifecycle processes (Y. Liu et al., 2021; McKnight et al., 2002). It advances information systems security research by demonstrating that transparency, update integrity, and governance shape adoption of embedded security mechanisms (Chan et al., 2005; Johnston & Warkentin, 2010; Lau et al., 2018). It extends environmental perspectives by showing how regulatory expectations and industry norms shape vendor governance choices and the boundaries of what users consider acceptable protection (Bélanger & Crossler, 2011; Wang et al., 2020). Finally, it advances system quality theory by demonstrating that technical feasibility mediates the influence of organizational practices on behavioral perceptions, positioning algorithmic efficiency, computational overhead, energy consumption, and interoperability as central determinants of adoption in resource constrained environments (Hossain et al., 2015; Hwang, 2015).

Practical Implications

The findings have clear implications for vendors, policymakers, standards bodies, and security practitioners. Vendors must recognize that users evaluate lightweight cryptography and key management through perceptions shaped by technical performance and communication rather than through direct inspection of cryptographic strength. Clear explanations of security features, consistent update processes, and visible governance practices strengthen trust and reduce uncertainty (J. M. Haney & Furman, 2023; Lau et al., 2018). Vendors should also address performance indicators such as latency, battery consumption, and interoperability, since these shape user judgments of usefulness and reliability (Bringhenti et al., 2022; He et al., 2019). Policymakers influence adoption by defining expectations for privacy, accountability, and baseline security. Regulatory requirements shape vendor strategies and user assumptions about acceptable protection (Bélanger & Crossler, 2011). Standards bodies should develop guidelines that balance security, performance, and interoperability in resource constrained environments. Security practitioners must design systems that integrate protection, performance, and usability. Algorithmic efficiency, computational overhead, energy consumption, and key management practicality must be evaluated together to ensure that security mechanisms do not degrade user experience or system reliability (Gu et al., 2019; H. Liu et al., 2017). The socio technical model provides a framework for aligning technical decisions with behavioral, organizational, and environmental realities in smart home ecosystems, ensuring that embedded protections remain credible, efficient, and usable (Hammi et al., 2022; Sicari et al., 2015).

Research Implications

The integrated socio-technical model suggests a focused agenda for future research. Behavioral research should examine how users interpret performance indicators such as latency, battery impact, and reliability, and how these interpretations shape perceived usefulness, ease of use, trust, and risk in the context of embedded cryptography. Organizational research should investigate how transparency, update design, and governance practices influence trust and perceived risk over time through experimental and longitudinal designs. Comparative research should analyze how differences in regulatory environments shape vendor governance, technical implementation choices, and user confidence in smart home security (Bélanger & Crossler, 2011; Wang et al., 2020). Technical and design-oriented research should develop operational

measures of key management practicality that link algorithmic and protocol level properties to user level perceptions and adoption decisions. Future work should also examine how users conceptualize security mechanisms that operate outside their direct awareness, since these mental models likely mediate the influence of vendor communication and environmental cues on adoption (Barth & De Jong, 2017; Zheng et al., 2018). Research on context aware security, device heterogeneity, and resource constrained communication can further clarify how technical limitations shape user experience and trust formation (Hossain et al., 2015; Khanpara et al., 2023).

Conclusion

This review demonstrates that adoption of lightweight cryptography and key management in smart home environments is shaped by the interaction of behavioral, organizational, environmental, and technical determinants. Users rely on perceptions of usefulness, ease of use, trust, and risk to evaluate security mechanisms they cannot directly observe. Organizational practices shape how users interpret security assurances, while environmental expectations define the broader context of acceptable protection. Technical feasibility remains essential, since algorithmic efficiency, computational overhead, energy consumption, interoperability, and key management practicality determine whether security mechanisms can operate without degrading performance. The findings confirm that adoption outcomes depend on the alignment of human interpretation, vendor governance, regulatory expectations, and device level constraints, reinforcing the socio technical nature of embedded security mechanisms (Anwar et al., 2020; Harvey et al., 2020; Ortega, 2024). The integrated socio-technical model provides a comprehensive explanation of how these determinants jointly influence adoption and implementation success and offers a foundation for future research and practical efforts aimed at improving the security and reliability of smart home ecosystems. By integrating behavioral, organizational, environmental, and technical determinants, this review provides a socio-technical foundation for understanding adoption of embedded security mechanisms in smart home ecosystems (Bélanger & Crossler, 2011; Davis, 1989).

Acknowledgement

Generative AI was used only to polish writing. All analysis and conclusions are the authors' own. The tool did not contribute to the development of ideas or the synthesis of evidence.

References

- Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8–27. <https://doi.org/10.1016/j.jisa.2017.11.002>
- Ansari, S. A., & Ali, S. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing*, 28(1), 266. <https://doi.org/10.1007/s10791-025-09755-3>
- Anwar, R. W., Zainal, A., Abdullah, T., & Iqbal, S. (2020). Security Threats and Challenges to IoT and its Applications: A Review. *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, 301–305. <https://doi.org/10.1109/FMEC49853.2020.9144832>
- Barth, S., & De Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>

- Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems1. *MIS Quarterly*, 35(4), 1017-A36. <https://doi.org/10.2307/41409971>
- Bettayeb, S., Messai, M.-L., & Hemam, S. M. (2023). A robust and efficient vector-based key management scheme for IoT networks. *Ad Hoc Networks*, 149, 103250. <https://doi.org/10.1016/j.adhoc.2023.103250>
- Bringhenti, D., Valenza, F., & Basile, C. (2022). Toward Cybersecurity Personalization in Smart Homes. *IEEE Security & Privacy*, 20(1), 45–53. <https://doi.org/10.1109/MSEC.2021.3117471>
- Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On Privacy and Security Challenges in Smart Connected Homes. *2016 European Intelligence and Security Informatics Conference (EISIC)*, 172–175. <https://doi.org/10.1109/EISIC.2016.044>
- Chakravorty, A., Wlodarczyk, T., & Chunming Rong. (2013). Privacy Preserving Data Analytics for Smart Homes. *2013 IEEE Security and Privacy Workshops*, 23–27. <https://doi.org/10.1109/SPW.2013.22>
- Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 1(3), 18–41. <https://doi.org/10.1080/15536548.2005.10855772>
- Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546. <https://doi.org/10.1016/j.future.2017.07.060>
- Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- Dhakare, S., Chippalkatti, S. S., & Misbahuddin, M. (2024). Securing the IoT Device Network with Lightweight Cryptography. *2024 27th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 1–5. <https://doi.org/10.1109/WPMC63271.2024.10863558>
- Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies*, 59(4), 451–474. [https://doi.org/10.1016/S1071-5819\(03\)00111-3](https://doi.org/10.1016/S1071-5819(03)00111-3)
- Garg, S., Kaur, K., Kaddoum, G., Garigipati, P., & Aujla, G. S. (2021). Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities. *IEEE Network*, 35(5), 298–305. <https://doi.org/10.1109/MNET.211.2000526>
- Gu, W., Bao, P., Hao, W., & Kim, J. (2019). Empirical Examination of Intention to Continue to Use Smart Home Services. *Sustainability*, 11(19), 5213. <https://doi.org/10.3390/su11195213>
- Haider, Z. A., Zeb, A., Islam, A. K. M. M., Rahman, T., Arishi, A., & Ullah, I. (2026). Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms. *Computer Science Review*, 59, 100861. <https://doi.org/10.1016/j.cosrev.2025.100861>
- Hammi, B., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security*, 117, 102677. <https://doi.org/10.1016/j.cose.2022.102677>
- Haney, J., Acar, Y., Li, A., & Haney, F. (2025). *Survey on smart home users' security and privacy perceptions and actions: A device category perspective* (NIST SP 1343; p. NIST SP 1343). National Institute of Standards and Technology (U.S.). <https://doi.org/10.6028/NIST.SP.1343>
- Haney, J. M., & Furman, S. M. (2023). User Perceptions and Experiences with Smart Home Updates. *2023 IEEE Symposium on Security and Privacy (SP)*, 2867–2884. <https://doi.org/10.1109/SP46215.2023.10179459>

- Harvey, P., Toutsoy, O., Kornegay, K., Alale, E., & Reaves, D. (2020). Security and Privacy of Medical Internet of Things Devices for Smart Homes. *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 1–6. <https://doi.org/10.1109/IOTSMS52051.2020.9340231>
- He, W., Martinez, J., Padhi, R., Zhang, L., & Ur, B. (2019). When Smart Devices Are Stupid: Negative Experiences Using Home Smart Devices. *2019 IEEE Security and Privacy Workshops (SPW)*, 150–155. <https://doi.org/10.1109/SPW.2019.00036>
- Hossain, Md. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services*, 21–28. <https://doi.org/10.1109/SERVICES.2015.12>
- Hwang, Y. H. (2015). IoT Security & Privacy: Threats and Challenges. *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*, 1–1. <https://doi.org/10.1145/2732209.2732216>
- Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 727–732. <https://doi.org/10.1109/WF-IoT.2015.7389144>
- Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34(3), 549–566. <https://doi.org/10.2307/25750691>
- Keshavarz, M., & Anwar, M. (2018). Towards Improving Privacy Control for Smart Homes: A Privacy Decision Framework. *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 1–3. <https://doi.org/10.1109/PST.2018.8514198>
- Khanpara, P., Lavingia, K., Trivedi, R., Tanwar, S., Verma, A., & Sharma, R. (2023). A context-aware internet of things-driven security scheme for smart homes. *SECURITY AND PRIVACY*, 6(1), e269. <https://doi.org/10.1002/spy2.269>
- Khawla, M., & Tomader, M. (2018). A Survey on the Security of Smart Homes: Issues and Solutions. *Proceedings of the 2nd International Conference on Smart Digital Environment*, 81–87. <https://doi.org/10.1145/3289100.3289114>
- Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–31. <https://doi.org/10.1145/3274371>
- Liu, H., Li, C., Jin, X., Li, J., Zhang, Y., & Gu, D. (2017). Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 13–18. <https://doi.org/10.1145/3139937.3139948>
- Liu, Y., Gan, Y., Song, Y., & Liu, J. (2021). What Influences the Perceived Trust of a Voice-Enabled Smart Home System: An Empirical Study. *Sensors*, 21(6), 2037. <https://doi.org/10.3390/s21062037>
- Marghalani, L., Aljoby, W., & Asadullah, A. (2025). The Illusion of Control in Smart Homes: How IoT App Privacy Statement and Device Interaction Complexity Impact User Security Practices. *2025 European Symposium on Usable Security (EuroUSEC)*, 191–203. <https://doi.org/10.1109/EuroUSEC69254.2025.00027>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Nemec Zlatolas, L., Feher, N., & Hölbl, M. (2022). Security Perception of IoT Devices in Smart Homes. *Journal of Cybersecurity and Privacy*, 2(1), 65–73. <https://doi.org/10.3390/jcp2010005>

- Ortega, A. G. (Ed.). (2024). Session details: Privacy and Smart Homes. In *Designing Interactive Systems Conference*. ACM. <https://doi.org/10.1145/3676265>
- Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors*, 24(12), 4008. <https://doi.org/10.3390/s24124008>
- Rahim, A., Zhong, Y., Ahmad, T., Ahmad, S., Pławiak, P., & Hammad, M. (2023). Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models. *Sensors*, 23(15), 6979. <https://doi.org/10.3390/s23156979>
- Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, 129, 77–89. <https://doi.org/10.1016/j.future.2021.11.011>
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>
- Sookhak, M., Tang, H., He, Y., & Yu, F. R. (2019). Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, 21(2), 1718–1743. <https://doi.org/10.1109/COMST.2018.2867288>
- The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. (2003). *Journal of Management Information Systems*, 19(4), 9–30. <https://doi.org/10.1080/07421222.2003.11045748>
- Wang, X., McGill, T. J., & Klobas, J. E. (2020). I Want It Anyway: Consumer Perceptions of Smart Home Devices. *Journal of Computer Information Systems*, 60(5), 437–447. <https://doi.org/10.1080/08874417.2018.1528486>
- Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management & Data Systems*, 117(1), 68–89. <https://doi.org/10.1108/IMDS-01-2016-0017>
- Yang, Y., Yu, X., Zhang, Z., & Gan, L. (2023). Integrating Technology Acceptance Model With Maslow's Hierarchy Needs Theory to Investigate Smart Homes Adoption. *IEEE Access*, 11, 80726–80740. <https://doi.org/10.1109/ACCESS.2023.3300724>
- Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–20. <https://doi.org/10.1145/3274469>