Asia Pacific Science Press

Asia Pacific Economic and Management Review
ISSN(O):3005-9275
ISSN(P):3005-9267
Vol. 2 No.6 (2025)

Zero-Trust Security Investment and Firm Performance in AI-Enabled Internet of Things Environments

Chunhai Wang*

Department of Economics and Management, Shandong Vocational College of Science and Technology, Weifang, 261053, China

Corresponding author: Chunhai Wang, 415412144@qq.com

Abstract: This study examines how zero-trust security investment affects firm performance in AI-enabled Internet of Things (AI-IoT) environments and through which mechanisms and boundary conditions this influence occurs. Drawing on the resource-based view and dynamic capability perspectives, we conceptualize zero-trust security investment as a multidimensional capability bundle that integrates financial resources, technological deployment and organizational practices dedicated to implementing zero-trust principles in AI-IoT systems. Using survey data from 312 firms in AI-IoT–intensive industries in China and structural equation modeling, we find that zero-trust security investment is positively associated with firm performance. Digital resilience—defined as the firm's ability to withstand, adapt to and recover from cyber-related disruptions—plays a partial mediating role in this relationship, indicating that security investments create value both by directly reducing expected losses and by enhancing the reliability and continuity of AI-IoT–enabled operations. Furthermore, environmental uncertainty positively moderates the effect of zero-trust security investment on firm performance, suggesting that the performance benefits of zero-trust security are stronger in volatile environments characterized by rapid technological change, evolving regulations and dynamic competitive behavior. These findings highlight zero-trust security as a strategic resource that underpins digital resilience and competitive advantage, and they offer practical guidance for managers and policymakers seeking to align cybersecurity investment with AI-IoT strategies and environmental conditions.

Keywords: Zero-Trust Security; AI-enabled Internet of Things (AI-IoT); Digital Resilience; Environmental Uncertainty; Firm Performance; Structural Equation Modeling; China

Published: Dec 29, 2025

DOI: https://doi.org/10.62177/apemr.v2i6.1001

1.Introduction

The rapid diffusion of artificial-intelligence-enabled Internet of Things (AI-IoT) technologies is transforming how firms create, deliver and capture value. Smart factories, connected logistics, intelligent retailing and data-driven services rely increasingly on pervasive sensing, real-time analytics and automated decision making. These developments greatly expand the scope and volume of data flows within and across organizational boundaries, while also tightening the coupling between cyber systems and physical assets. As a result, firms are becoming more productive and innovative, but they are also more exposed to cyberattacks, privacy breaches and operational disruptions. Managing security in AI-IoT environments has thus become a strategic concern for senior managers and boards rather than a purely technical issue delegated to IT departments.

Traditional perimeter-based security models, which assume trustworthy internal networks protected from untrusted external networks, are ill-suited to this new environment. AI-IoT architectures are characterized by heterogeneous devices, mobile endpoints, cloud services and extensive third-party integration. Trust boundaries are fluid and often opaque, and compromised devices can quickly propagate risks across the entire system. In response, the concept of zero-trust security has gained prominence. Zero-trust architectures are built on the principle of "never trust, always verify": every user, device and application must be authenticated, authorized and continuously validated regardless of network location. Core practices include strong identity and access management, micro-segmentation, least-privilege access, continuous monitoring and data-centric protection.

While both practitioners and policymakers increasingly advocate zero-trust as a promising paradigm for securing digital infrastructures, especially in highly connected environments such as AI-IoT, most discussions remain technology-centric. Existing research has largely focused on architecture design, protocol implementation, threat detection algorithms and performance optimization. Far less attention has been paid to the economic and managerial implications of adopting zero-trust security in firms. In particular, there is limited empirical evidence on whether, and through which mechanisms, zero-trust security investments contribute to firm-level performance outcomes.

This omission is non-trivial. Security expenditures are often perceived as cost centers rather than value drivers, and managers struggle to justify substantial investments in advanced security solutions, especially when returns are uncertain and benefits are intangible. AI-IoT projects already require sizeable capital outlays and organizational change; adding zero-trust security on top of these investments may be seen as increasing complexity and slowing down digital initiatives. Without a clearer understanding of the performance consequences of zero-trust security investment, firms may underinvest in necessary protections or, conversely, overspend without commensurate benefits.

Moreover, AI-IoT environments present a distinctive context in which the relationship between security and performance may differ from that in traditional IT settings. First, security incidents can directly affect physical operations, safety and regulatory compliance, amplifying potential losses. Second, data integrity and availability are critical for training and deploying AI models; compromised data streams may undermine algorithmic accuracy and business decision quality. Third, customers, regulators and ecosystem partners are increasingly sensitive to how firms safeguard data generated by connected devices. Consequently, security capabilities may shape not only risk exposure but also stakeholder trust, innovation capacity and competitive positioning.

Against this background, the central objective of this study is to investigate how zero-trust security investment affects firm performance in AI-enabled Internet of Things environments. Specifically, we ask:

(1) Does zero-trust security investment have a measurable association with firm performance in AI-IoT contexts?

(2) Through which organizational capabilities and operational outcomes does such investment influence performance?

(3) Under what environmental and organizational conditions are the performance effects of zero-trust security investment strengthened or weakened?

To address these questions, we conceptualize zero-trust security investment as a multidimensional construct encompassing financial resources, technological deployment and organizational practices dedicated to implementing zero-trust principles in AI-IoT systems. Drawing on resource-based and dynamic capability perspectives, we argue that these investments can enhance firms' digital resilience, process reliability and data governance quality, which in turn support superior operational and financial performance. At the same time, we recognize that the benefits of zero-trust security are unlikely to be purely direct or immediate. They may materialize through reduced incident frequency and severity, improved system uptime, higher quality analytics, enhanced stakeholder confidence and greater readiness to adopt innovative AI-IoT applications.

This study contributes to the literature in several ways. First, it bridges the gap between cybersecurity research and mainstream management and economics by analyzing zero-trust security investment as a strategic resource rather than merely a technical safeguard. Second, it focuses on AI-IoT environments, where the stakes of security failures and the potential leverage of security capabilities are particularly high but empirically underexplored. Third, by examining performance implications, mediating capabilities and contextual contingencies, the study provides a more nuanced understanding of when

and how zero-trust security investment creates value for firms. Finally, the findings offer actionable insights for managers seeking to balance the costs and benefits of security spending in the course of digital transformation.

2.Literature Review and Hypothesis Development

2.1 AI-Enabled Internet of Things and Firm Performance

The Internet of Things (IoT) refers to networks of interconnected devices that can sense, communicate and interact with their environment. When combined with artificial intelligence techniques such as machine learning, deep learning and advanced analytics, IoT systems evolve into AI-enabled IoT (AI-IoT) environments. In such environments, data generated by sensors, machines and products are continuously collected, processed and transformed into actionable insights to support real-time decision making.

Prior studies on IoT and AI adoption have shown that these technologies can improve operational efficiency, reduce downtime, enhance product and service innovation, and enable new business models[1]. Firms leverage AI-IoT to optimize production processes, monitor equipment health, customize offerings and coordinate complex supply chains. Consequently, AI-IoT capabilities are often linked to superior operational and financial performance, including higher productivity, cost savings, revenue growth and improved customer satisfaction[2][3].

However, research also suggests that the performance outcomes of AI-IoT investments are contingent on complementary resources and capabilities[4]. The mere deployment of connected devices and AI algorithms does not automatically translate into performance gains. Firms must develop adequate IT infrastructure, data governance mechanisms, organizational learning routines and risk management practices to fully exploit AI-IoT potential. Cybersecurity is one of the critical complements, because the reliability and trustworthiness of AI-IoT data and services depend on the protection of devices, networks and applications against attacks, manipulation and unauthorized access[5].

2.2 Cybersecurity Investment and Firm Performance

The relationship between cybersecurity investment and firm performance has been examined from multiple perspectives. One stream of research conceptualizes cybersecurity spending as a form of risk management or insurance[6]. Security investments reduce the likelihood and impact of incidents such as data breaches, ransomware attacks and service disruptions[7]. By mitigating expected losses, they protect firm value, ensure business continuity and support regulatory compliance[8]. Another stream highlights the role of security in safeguarding intangible assets such as customer trust, reputation and intellectual property[9].

Empirical findings on the performance effects of cybersecurity investment are mixed. Some studies report positive associations between security capabilities and market value, profitability or productivity, especially in industries where information assets are strategic. Others find insignificant or even negative short-term effects, suggesting that security expenses may be perceived as pure costs or that benefits are difficult to measure within typical reporting periods. These inconsistencies indicate that the value of security investment may be context-dependent and mediated by organizational capabilities and external conditions.

In addition, traditional studies often assume perimeter-based or reactive security models, focusing on technologies such as firewalls, antivirus software and intrusion detection systems. As digital architectures evolve toward cloud computing, mobile access and IoT, the effectiveness of such models becomes limited. This raises the question of whether newer paradigms like zero-trust security, which are designed for highly distributed and dynamic environments, can generate different patterns of performance outcomes compared with legacy approaches.

2.3 Zero-Trust Security in AI-IoT Environments

Zero-trust security has emerged as a response to the erosion of clear network perimeters. Its core principle—"never trust, always verify"—implies that no implicit trust is granted based on network location or device ownership. Instead, every access request must be explicitly authenticated, authorized and encrypted, and security policies must be consistently enforced across users, devices, applications and data[10].

Typical components of zero-trust architectures include robust identity and access management, multi-factor authentication, micro-segmentation of networks, continuous monitoring of device and user behavior, and fine-grained, least-privilege

authorization. Rather than relying on static boundaries, zero-trust systems adopt dynamic, context-aware access decisions, often supported by analytics and automation.

AI-IoT environments constitute a particularly relevant domain for zero-trust implementation. First, they involve large numbers of heterogeneous devices, many of which are resource-constrained and may lack built-in security features. Second, devices often operate in untrusted physical locations, where tampering and spoofing are feasible[11]. Third, AI-IoT deployments frequently span multiple networks, cloud platforms and organizational boundaries, making traditional perimeter controls insufficient.

By enforcing strict authentication and authorization for each interaction, zero-trust security can reduce the attack surface in AI-IoT systems and limit lateral movement in case of compromise. Micro-segmentation and continuous monitoring help detect anomalies and contain threats before they escalate into systemic failures. Moreover, data-centric controls such as encryption and tokenization protect sensitive information even when infrastructure vulnerabilities exist. These features suggest that zero-trust security may significantly enhance the reliability, resilience and trustworthiness of AI-IoT operations.

Yet, implementing zero-trust in AI-IoT settings also entails substantial costs and organizational change. Firms must invest in new technologies, redesign network architectures, update legacy systems, and adapt policies and processes. Employees and partners may resist stricter access controls or additional authentication steps. Therefore, the net performance impact of zero-trust security investment is an empirical question that depends on whether the benefits in terms of risk reduction, operational continuity and stakeholder trust outweigh the associated costs and complexity[12].

2.4 Zero-Trust Security Investment as a Strategic Resource

To analyze the performance implications of zero-trust security investment, this study draws on the resource-based view (RBV) and dynamic capability perspectives. RBV posits that firms achieve sustainable competitive advantage when they possess resources that are valuable, rare, inimitable and non-substitutable. Digital security capabilities can meet these criteria when they protect critical information assets, support reliable operations and are embedded in firm-specific processes and routines.

Zero-trust security investment can be seen as a bundle of tangible and intangible resources, including specialized technologies, expert personnel, codified policies and accumulated know-how related to designing and operating zero-trust architectures. In AI-IoT environments, these resources are valuable because they reduce the likelihood of catastrophic failures, support regulatory compliance and enable reliable data flows necessary for AI-driven analytics[13]. They can be rare and difficult to imitate when they are deeply integrated with a firm's unique systems, organizational culture and partner relationships.

Dynamic capability theory emphasizes a firm's ability to integrate, build and reconfigure internal and external competencies in response to environmental changes. Zero-trust security investment may contribute to digital resilience, defined as the ability to withstand, adapt to and recover from cyber-related disruptions[14]. By establishing continuous monitoring, adaptive access control and rapid incident response mechanisms, zero-trust architectures enhance a firm's capacity to sense threats, seize opportunities (e.g., safely adopting new AI-IoT applications) and transform its digital infrastructure.

Based on these perspectives, we argue that zero-trust security investment influences firm performance both directly and indirectly. Directly, it reduces expected losses from security incidents and downtime. Indirectly, it fosters higher-quality data governance, improves operational reliability, and strengthens the confidence of customers, regulators and ecosystem partners, which in turn supports revenue growth and efficiency gains[15].

2.5 Hypotheses Development

（1）Zero-trust security investment and firm performance

In AI-IoT environments, system failures or data breaches can have immediate operational and financial consequences. Zero-trust security investment lowers the probability and severity of such events by enforcing strong access control and continuous monitoring. It also enhances the integrity and availability of data used for AI analytics, which supports better decision making and process optimization. Furthermore, demonstration of robust security practices can increase stakeholder trust, helping firms attract and retain customers and partners. Therefore, we expect zero-trust security investment to be positively associated with firm performance[16].

H1: Zero-trust security investment in AI-enabled IoT environments is positively related to firm performance.

（2）Mediating role of digital resilience

Digital resilience reflects a firm's ability to maintain or quickly restore critical operations in the face of cyber incidents or technical failures. Zero-trust security investment contributes to digital resilience by enabling granular isolation of compromised components, automated detection of anomalies and rapid containment of threats. Resilient firms experience fewer and shorter disruptions, maintain service quality and avoid costly downtime. Consequently, digital resilience should mediate the relationship between zero-trust security investment and firm performance[17].

H2: Zero-trust security investment is positively associated with digital resilience in AI-enabled IoT environments.

H3: Digital resilience is positively associated with firm performance and mediates the effect of zero-trust security investment on firm performance.

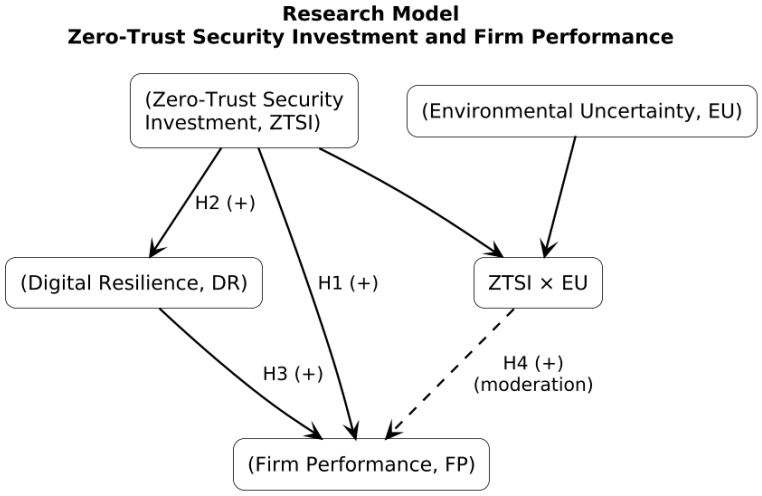
（3）Moderating role of environmental uncertainty

The benefits of zero-trust security investment may depend on the level of environmental uncertainty surrounding AI-IoT operations. In highly uncertain environments—characterized by rapid technological change, evolving regulations and frequent cyber threats—firms face greater risk of disruptions and obsolescence[18]. Under such conditions, the protective and adaptive features of zero-trust architectures are more valuable, and the payoff from security investment is likely to be higher[19]. In more stable environments, the marginal benefits of extensive security capabilities may be lower relative to their costs.

H4: Environmental uncertainty positively moderates the relationship between zero-trust security investment and firm performance, such that the relationship is stronger under higher levels of environmental uncertainty.

Figure 1 summarizes the proposed research model. Zero-trust security investment is hypothesized to enhance firm performance directly and indirectly through digital resilience, while environmental uncertainty moderates the direct path between zero-trust security investment and firm performance.

Figure 1: Research Model



3.Research Design

3.1 Research model

Based on the hypotheses developed in Section 2, this study proposes a research model that links zero-trust security investment to firm performance in AI-enabled IoT environments. Zero-trust security investment is conceptualized as the focal independent variable. Firm performance is the dependent variable, reflecting both operational and financial outcomes. Digital resilience is modeled as a mediating variable that captures the firm's capability to withstand and recover from cyber-related disruptions. Environmental uncertainty is treated as a moderating variable that shapes the strength of the relationship between zero-trust security investment and firm performance.

In addition, several control variables are included to account for alternative explanations: firm size, firm age, industry type, ownership type, and AI-IoT adoption level. Figure 1 (not shown here) summarizes the structural relationships: zero-trust security investment positively affects digital resilience and firm performance (H1, H2), digital resilience positively affects

firm performance and mediates the effect of zero-trust security investment (H3), and environmental uncertainty positively moderates the link between zero-trust security investment and firm performance (H4).

3.2 Data collection and sample

To empirically test the research model, we conducted a survey of firms operating in AI-IoT-intensive industries in China, including manufacturing, logistics and transportation, energy, and information and communication services. These industries were selected because they are at the forefront of adopting AI-enabled IoT technologies and thus face substantial security challenges.

The sampling frame was constructed from membership lists of industrial associations, high-tech industrial parks, and publicly available directories of firms known to have implemented IoT or AI projects. We targeted senior managers who are knowledgeable about both security and digital transformation issues, such as CIOs, CISOs, IT directors, and heads of digital or smart-manufacturing departments.

The questionnaire was first developed in English, translated into Chinese, and then back-translated to ensure semantic equivalence. Before the main survey, we conducted a pre-test with several academics and ten managers from AI-IoT-adopting firms to refine item wording and layout. The final questionnaire was administered through a combination of online survey links and paper-and-pencil distribution at industry events. Participation was voluntary and anonymous, and respondents were informed that there were no right or wrong answers and that their responses would be used only for academic research.

After removing responses with excessive missing data, straight-lining patterns, or unacceptable completion times, we retained a final sample of firms that provides adequate statistical power for structural equation modeling. The sample covers a range of firm sizes and industries: large firms as well as small and medium-sized enterprises, and both manufacturing and service sectors.

To assess potential non-response bias, we compared early and late respondents on key demographic characteristics and on the means of major constructs. No significant differences were found, suggesting that non-response bias is unlikely to be a serious concern.

3.3 Measures

All latent constructs were measured using multiple items adapted from prior studies and modified to fit the AI-IoT and zero-trust context. Unless otherwise specified, items were assessed using a seven-point Likert-type scale ranging from 1 = "strongly disagree" to 7 = "strongly agree." Higher scores indicate higher levels of the underlying construct.

（1）Zero-trust security investment.

Zero-trust security investment reflects the extent to which a firm commits financial and organizational resources to implementing zero-trust principles in its AI-IoT systems. Sample items include: "Our firm has significantly increased its investment in identity and access management for AI-IoT systems," "Our firm has implemented fine-grained access control and micro-segmentation for critical AI-IoT networks," and "Our firm continuously invests in monitoring and analytics tools to detect abnormal behavior in AI-IoT environments."

（2）Digital resilience.

Digital resilience captures the firm's capability to maintain or rapidly restore critical AI-IoT-enabled operations in the face of cyber incidents or technical failures. Sample items include: "Our AI-IoT systems can continue to operate even when some components fail," "When security incidents occur, our firm can quickly isolate affected systems and restore normal operations," and "Our firm regularly tests and updates contingency plans for AI-IoT-related disruptions."

（3）Environmental uncertainty.

Environmental uncertainty reflects managers' perceptions of the volatility and unpredictability of the technological and competitive environment related to AI-IoT. Sample items include: "Technologies related to AI-enabled IoT change rapidly in our industry," "It is difficult to predict how competitors will adopt AI-IoT technologies," and "Regulatory requirements related to data security and privacy in AI-IoT are unpredictable."

（4）Firm performance.

Firm performance is measured using subjective assessments relative to main competitors over the past three years. This

approach is widely used when objective financial data are unavailable or not directly comparable. Respondents evaluated their firm's performance on items such as sales growth, profitability, market share, and overall competitive position. Each item used a seven-point scale ranging from 1 = "much worse" to 7 = "much better" than major competitors.

（5）Control variables.

Firm size was measured as the natural logarithm of the number of employees. Firm age was measured as the number of years since establishment. Industry type was captured using dummy variables (e.g., manufacturing vs. non-manufacturing). Ownership type distinguished between state-owned and non-state-owned firms. AI-IoT adoption level was measured using a multi-item scale capturing the breadth and depth of AI-IoT applications across production, logistics, and customer-facing processes. These controls help ensure that the estimated relationships are not simply driven by basic structural differences across firms.

3.4 Reliability and validity

Several steps were taken to assess the reliability and validity of the measurement model. First, internal consistency reliability was evaluated using Cronbach's alpha and composite reliability (CR). Values above the commonly accepted threshold of 0.70 indicate satisfactory reliability. Second, convergent validity was examined by inspecting factor loadings and the average variance extracted (AVE) for each construct. Standardized loadings greater than 0.70 and AVE values above 0.50 suggest that the items adequately capture the underlying constructs.

Third, discriminant validity was assessed using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT). For each construct, the square root of AVE should exceed its correlations with other constructs, and HTMT values should be below 0.85 or 0.90, indicating that constructs are empirically distinct. Items with low loadings or high cross-loadings were considered for removal to improve model fit while preserving content validity.

To address potential common method bias, we employed both procedural and statistical remedies. Procedurally, we assured respondents of anonymity, reduced evaluation apprehension, and separated items for predictors and outcomes in the questionnaire. Statistically, we conducted Harman's single-factor test and a confirmatory factor analysis with a common latent factor. The results suggest that common method variance does not pose a serious threat to the study's conclusions.

3.5 Analytical methods

Given the study's focus on simultaneously estimating multiple relationships, including mediation and moderation effects among latent variables, we employed structural equation modeling (SEM) as the primary analytical technique. The analysis followed a two-step approach. First, the measurement model was evaluated to verify the reliability and validity of the constructs. Second, the structural model was tested to assess the hypothesized relationships among constructs.

Mediation effects (H3) were examined using bootstrapping procedures to compute confidence intervals for indirect effects. If the confidence interval does not include zero, the mediation effect is considered significant. Moderation (H4) was tested by creating an interaction term between mean-centered zero-trust security investment and environmental uncertainty and including this term in the structural model. Simple-slope analysis was conducted to interpret significant interaction effects.

Robustness checks were conducted by estimating alternative models—for example, models without the mediator, models using alternative operationalizations of firm performance, and models splitting the sample by industry. The consistency of the results across these specifications increases confidence in the robustness of the empirical findings.

4.Results

4.1 Sample characteristics and descriptive statistics

After data screening, a total of 312 usable questionnaires were retained for analysis. Among the sampled firms, 44.9% operate in manufacturing (n = 140), 21.5% in logistics and transportation (n = 67), 15.7% in energy (n = 49), and 17.9% in information and communication services (n = 56). With respect to ownership, 37.5% are state-owned enterprises (SOEs) and 62.5% are non-state-owned firms (including private and foreign-invested firms).

The average firm age is 15.8 years (SD = 8.9), with a range from 2 to 52 years. Firm size, measured as the natural logarithm of the number of employees, has a mean of 6.23 (SD = 1.02), corresponding roughly to firms with between a few dozen and several thousand employees.

The mean score for AI-IoT adoption is 4.98 (SD = 1.08) on a seven-point scale, indicating that, on average, firms have

adopted AI-IoT applications in more than one functional area. The focal constructs also show moderate levels: zero-trust security investment (ZTSI) has a mean of 4.86 (SD = 1.09), digital resilience (DR) 4.92 (SD = 1.02), environmental uncertainty (EU) 4.37 (SD = 1.11), and firm performance (FP) 4.71 (SD = 0.98).

Table 1 presents the means, standard deviations and correlations among the key variables. ZTSI is positively correlated with DR (r = 0.52) and FP (r = 0.38). DR is positively correlated with FP (r = 0.46). AI-IoT adoption is positively associated with ZTSI (r = 0.41), DR (r = 0.36) and FP (r = 0.30). None of the correlations exceeds 0.80, suggesting that multicollinearity is unlikely to be a serious problem.

Table 1: Descriptive statistics and correlations (N = 312)

No.	Variable	Mean	SD	1	2	3	4	5	6	7	8	9
1	Firm size (ln employees)	6.23	1.02	1								
2	Firm age (years)	15.8	8.9	0.32	1							
3	State ownership (1 = SOE)	0.38	0.49	0.29	0.26	1						
4	Manufacturing (1 = manufacturing)	0.45	0.5	0.27	0.09	0.18	1					
5	AI-IoT adoption	4.98	1.08	0.19	-0.15	-0.12	0.08	1				
6	Environmental uncertainty (EU)	4.37	1.11	0.05	0.03	0.04	0.06	0.25	1			
7	Zero-trust security investment (ZTSI)	4.86	1.09	0.21	-0.1	-0.09	0.05	0.41	0.29	1		
8	Digital resilience (DR)	4.92	1.02	0.18	-0.08	-0.07	0.04	0.36	0.33	0.52	1	
9	Firm performance (FP)	4.71	0.98	0.24	-0.12	-0.11	0.03	0.3	0.22	0.38	0.46	1

Note: All correlations ≥ |0.15| are typically significant at $p < 0.01$ for N = 312; correlations ≥ |0.11| are typically significant at $p < 0.05$ (two-tailed).

4.2 Measurement model evaluation

Confirmatory factor analysis (CFA) was conducted to assess the measurement model. The overall fit indices indicate a good fit between the model and the data ($\chi^2 = 278.46$, df = 179, $\chi^2/df = 1.56$, CFI = 0.961, TLI = 0.952, RMSEA = 0.043, SRMR = 0.039). All items load significantly on their intended constructs, with standardized loadings ranging from 0.74 to 0.88.

Table 2 summarizes the reliability and convergent validity of the latent constructs. Cronbach's alpha values range from 0.84 to 0.89, and composite reliability (CR) values range from 0.85 to 0.90, all above the recommended threshold of 0.70. The average variance extracted (AVE) values are between 0.63 and 0.69, exceeding the 0.50 benchmark, indicating satisfactory convergent validity.

Table 2: Reliability and convergent validity of constructs

Construct	Items	Cronbach's α	CR	AVE	Standardized loadings (range)
AI-IoT adoption	4	0.86	0.87	0.63	0.74 – 0.84
Environmental uncertainty (EU)	3	0.84	0.85	0.66	0.77 – 0.86
Zero-trust security investment (ZTSI)	4	0.89	0.9	0.69	0.78 – 0.88
Digital resilience (DR)	4	0.88	0.89	0.67	0.76 – 0.87
Firm performance (FP)	4	0.87	0.88	0.65	0.75 – 0.86

Discriminant validity was assessed using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT). For each construct, the square root of AVE (ranging from 0.79 to 0.83) exceeds its correlations with other constructs, and all HTMT values are below 0.85. These results indicate that the constructs are empirically distinct.

To check for common method bias, Harman's single-factor test was performed. The first unrotated factor explains 34.2% of the total variance, well below the 50% threshold. A CFA model including a common latent method factor does not substantially improve model fit ($\Delta CFI = 0.006$), and the method factor accounts for only a small proportion of variance. Therefore, common method variance is unlikely to pose a serious threat to the validity of the findings.

4.3 Structural model and hypothesis testing

The structural model was then estimated to test the hypothesized relationships among constructs. The model exhibits satisfactory fit (χ^2 = 292.17, df = 183, χ^2/df = 1.60, CFI = 0.955, TLI = 0.946, RMSEA = 0.046, SRMR = 0.042). Table 3 reports the standardized path coefficients, standard errors, t-values and p-values.

Table 3: Structural model results

Construct	Items	Cronbach's α	CR	AVE	Standardized loadings (range)
AI-IoT adoption	4	0.86	0.87	0.63	0.74 – 0.84
Environmental uncertainty (EU)	3	0.84	0.85	0.66	0.77 – 0.86
Zero-trust security investment (ZTSI)	4	0.89	0.9	0.69	0.78 – 0.88
Digital resilience (DR)	4	0.88	0.89	0.67	0.76 – 0.87
Firm performance (FP)	4	0.87	0.88	0.65	0.75 – 0.86

(1) Direct and mediating effects

As shown in Table 3, zero-trust security investment has a positive and significant effect on firm performance ($\beta = 0.21$, $p < 0.01$), supporting H1. Firms that invest more heavily in zero-trust security for their AI-IoT systems tend to achieve better performance relative to main competitors.

Zero-trust security investment is also positively related to digital resilience ($\beta = 0.52$, $p < 0.001$), supporting H2. This suggests that firms that allocate more resources to zero-trust principles—such as identity and access management, micro-segmentation and continuous monitoring—develop stronger capabilities to maintain or quickly restore AI-IoT-enabled operations in the face of cyber incidents or technical failures.

Digital resilience, in turn, exerts a positive and significant effect on firm performance ($\beta = 0.36$, $p < 0.001$), supporting the direct component of H3. Firms with higher digital resilience experience fewer and shorter disruptions and are better able to maintain service quality and avoid costly downtime, leading to superior performance outcomes.

To test the mediating role of digital resilience, a bootstrapping procedure with 5,000 resamples was used to estimate the indirect effect of zero-trust security investment on firm performance through digital resilience. The indirect effect is positive and significant ($\beta\_indirect = 0.19$; 95% CI [0.11, 0.29]), while the direct effect of ZTSI on FP remains significant ($\beta\_direct = 0.21$, $p < 0.01$) but is smaller than the total effect ($\beta\_total = 0.40$). These results indicate partial mediation, providing strong support for H3.

Among the control variables, firm size ($\beta = 0.18$, $p < 0.01$) and AI-IoT adoption ($\beta = 0.22$, $p < 0.01$) are positively associated with firm performance, whereas firm age, industry type and ownership type are not significantly related to performance.

(2) Moderating effect of environmental uncertainty

The moderating effect of environmental uncertainty was examined by including the interaction term ZTSI × EU in the structural model. The interaction effect on firm performance is positive and significant ($\beta = 0.11$, $p < 0.05$), supporting H4.

To interpret this interaction, a simple-slope analysis was conducted by plotting the relationship between ZTSI and FP at high and low levels of EU (one standard deviation above and below the mean). The positive slope of ZTSI on FP is steeper under high environmental uncertainty than under low environmental uncertainty, indicating that firms operating in more uncertain AI-IoT environments derive greater performance benefits from zero-trust security investment. Conceptually, this pattern is illustrated in Figure 2 (not included here).

These findings are consistent with the argument that in volatile environments characterized by rapid technological change, evolving regulations and frequent cyber threats, the protective and adaptive features of zero-trust security are particularly valuable.

4.4 Robustness checks

Several robustness checks were conducted to evaluate the stability of the results.

First, an alternative model without the mediator (digital resilience) was estimated, linking ZTSI directly to FP. In this simplified model, the effect of ZTSI on FP remains positive and significant ($\beta = 0.33$, $p < 0.001$), but the explanatory power of the model is lower ($R^2\_FP = 0.42$) compared with the full model ($R^2\_FP = 0.49$). This confirms the importance of digital resilience as a mediating mechanism.

Second, the model was re-estimated using alternative operationalizations of firm performance. When only financial indicators (sales growth and profitability) were used as the performance measure, the key paths remained significant (ZTSI → FP_financial: $\beta = 0.19$, $p < 0.01$; DR → FP_financial: $\beta = 0.31$, $p < 0.001$; ZTSI × EU → FP_financial: $\beta = 0.10$, $p < 0.05$). When only operational indicators (productivity and service quality) were used, the pattern was similar (ZTSI → FP_operational: $\beta = 0.22$, $p < 0.01$; DR → FP_operational: $\beta = 0.37$, $p < 0.001$; ZTSI × EU → FP_operational: $\beta = 0.12$, $p < 0.05$).

Third, subgroup analyses were conducted by splitting the sample into manufacturing ($n = 140$) and non-manufacturing firms ($n = 172$), and into SOEs ($n = 117$) and non-SOEs ($n = 195$). Across these subsamples, the core relationships—particularly the positive effects of ZTSI and DR on FP—remain significant, although the magnitudes of coefficients vary slightly. For example, the effect of ZTSI on FP is somewhat stronger in non-state-owned firms ($\beta = 0.24$, $p < 0.01$) than in SOEs ($\beta = 0.17$, $p < 0.05$).

Overall, these robustness checks suggest that the empirical results are stable across different model specifications, performance measures and subsamples.

4.5 Summary of findings

In summary, the empirical analysis provides strong support for the proposed research model. Zero-trust security investment in AI-enabled IoT environments is positively associated with firm performance, both directly and indirectly through digital resilience. Environmental uncertainty positively moderates the relationship between ZTSI and FP, indicating that firms operating in more volatile AI-IoT contexts benefit more from zero-trust security investment. These results highlight zero-trust security not merely as a technical safeguard but as a strategic resource that underpins digital resilience and competitive advantage.

5.Conclusion and Implications

This study investigates how zero-trust security investment affects firm performance in AI-enabled Internet of Things (AI-IoT) environments and through which mechanisms and boundary conditions this influence occurs. Drawing on data from 312 firms operating in AI-IoT–intensive industries, the empirical results show that zero-trust security investment is positively related to firm performance, both directly and indirectly through digital resilience. Firms that allocate more resources to implementing zero-trust principles—such as identity and access management, micro-segmentation and continuous monitoring—report better relative performance in sales growth, profitability and overall competitive position. At the same time, these investments significantly enhance firms' capacity to maintain and rapidly restore AI-IoT–enabled operations in the face of cyber incidents or technical failures, and this digital resilience partially mediates the relationship between zero-trust security investment and firm performance. Furthermore, environmental uncertainty positively moderates the effect of zero-trust security investment on performance, implying that the benefits of zero-trust are more pronounced in volatile AI-IoT environments characterized by rapid technological change, evolving regulations and dynamic competitive behavior.

Taken together, the findings suggest that zero-trust security should be understood not merely as a technical safeguard or compliance requirement, but as a strategic resource that underpins digital resilience and supports superior firm performance in AI-IoT contexts. From a theoretical standpoint, the study extends the resource-based view and dynamic capability perspectives by conceptualizing zero-trust security investment as a multidimensional capability bundle that protects critical digital assets, stabilizes data flows and enables firms to withstand and adapt to cyber-related disruptions. By demonstrating that digital resilience is a key mechanism linking security investment to performance, the study highlights the importance of shifting the focus from isolated security tools to integrated architectures and organizational processes that enable rapid detection, containment and recovery. The moderating role of environmental uncertainty further contributes to contingency

perspectives on digital investments, showing that the value of advanced security architectures depends on their fit with the external environment, and is particularly salient when firms face high technological and regulatory volatility.

For managers, the results imply that zero-trust security investment should be treated as an integral part of AI-IoT strategy rather than as a separate IT cost item. Security and AI-IoT initiatives can and should be co-designed so that architectures for connectivity, analytics and control are aligned with architectures for identity, access and monitoring. Managers are encouraged to invest not only in technical solutions, but also in complementary organizational practices—such as governance mechanisms, incident response routines and training programs—that embed zero-trust principles into everyday operations. Firms operating in highly uncertain AI-IoT environments should consider prioritizing more ambitious zero-trust deployment, as the performance returns are greater where risk, complexity and regulatory pressures are higher. At the same time, managers need to develop metrics that capture the value of digital resilience—such as disruption frequency and duration, recovery speed and data availability for AI analytics—in order to communicate the long-term benefits of security investment to top management and boards.

Beyond the firm level, the findings also carry implications for policymakers and ecosystem stakeholders in AI-IoT–intensive sectors. The positive association between zero-trust security investment, digital resilience and firm performance suggests that policies encouraging zero-trust adoption can simultaneously strengthen cybersecurity and enhance industrial competitiveness. Regulators and industry associations may consider issuing guidelines, reference architectures and best practices to lower the implementation barriers of zero-trust, especially for small and medium-sized enterprises. Platform providers and industry consortia can facilitate threat intelligence sharing and interoperability standards, helping firms integrate zero-trust components into AI-IoT ecosystems more efficiently. Finally, although the study is based on cross-sectional survey data from Chinese firms and focuses on self-reported measures, which limits causal inference and generalizability, it provides a foundation for future research to employ longitudinal designs, objective performance indicators and multi-country comparisons to further explore how zero-trust security strategies create value in different institutional and technological contexts.

Funding

No

Conflict of Interests

The authors declare that there is no conflict of interest regarding the publication of this paper.

Reference

[1] Mashat, R. M., Abourokbah, S. H., & Salam, M. A. (2024). Impact of Internet of Things adoption on organizational performance: A mediating analysis of supply chain integration, performance, and competitive advantage. Sustainability, 16(6), 2250. https://doi.org/10.3390/su16062250

[2] Wamba, S. F., et al. (2022). Impact of artificial intelligence assimilation on firm performance: The mediating effects of organizational agility and customer agility. International Journal of Information Management, 67, 102544. https://doi.org/10.1016/j.ijinfomgt.2022.102544

[3] Brynjolfsson, E., & Hitt, L. M. (1996). Paradox lost? Firm-level evidence on the returns to information systems spending. Management Science, 42(4), 541–558. https://doi.org/10.1287/mnsc.42.4.541

[4] Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. MIS Quarterly, 28(2), 283–322. https://doi.org/10.2307/25148636

[5] Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. MIS Quarterly, 24(1), 169–196. https://doi.org/10.2307/3250983

[6] Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3

[7] Li, L., Tong, Y., Wei, L., & Yang, S. (2022). Digital technology-enabled dynamic capabilities and their impacts on firm performance: Evidence from the COVID-19 pandemic. Information & Management, 59(8), 103689. https://doi.org/10.1016/j.im.2022.103689

[8] Ning, Y., Li, L., Xu, S. X., & Yang, S. (2023). How do digital technologies improve supply chain resilience in the COVID-19 pandemic? Evidence from Chinese manufacturing firms. Frontiers of Engineering Management, 10(1), 39–50. https://doi.org/10.1007/s42524-022-0230-4

[9] Bai, J. J., Brynjolfsson, E., Jin, W., Steffen, S., & Wan, C. (2021). Digital resilience: How work-from-home feasibility affects firm performance. NBER Working Paper, No. 28588. National Bureau of Economic Research. https://doi.org/10.3386/w28588

[10] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

[11] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69–104. https://doi.org/10.1080/10864415.2004.11044320

[12] Kindervag, J. (2010). Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research. Retrieved from https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf

[13] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[14] Gilman, E., & Barth, D. (2017). Zero trust networks: Building secure systems in untrusted networks. Sebastopol, CA: O'Reilly Media. https://doi.org/10.5555/3161337

[15] Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. ;login: The USENIX Magazine, 39(6), 6–11.

[16] Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

[17] Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7

[18] Duncan, R. B. (1972). Characteristics of organizational environments and perceived environmental uncertainty. Administrative Science Quarterly, 17(3), 313–327. https://doi.org/10.2307/2392145

[19] Miller, K. D. (1993). Industry and country effects on managers' perceptions of environmental uncertainties. Journal of International Business Studies, 24(4), 693–714. https://doi.org/10.1057/palgrave.jibs.8490251