Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.083568

ARTICLE

An Integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) for Developing Economies

Davis Matovu[1], **Ali Mwase**[2] **and Gilbert Gilibrays Ocen**[1,*]

[1]Department of Computer Engineering and Informatics, Faculty of Engineering, Busitema University, Tororo, Uganda
[2]Department of Marketing and Management, Makerere University Business School, Kampala, Uganda

*Corresponding Author: Gilbert Gilibrays Ocen. Email: gilbertocen@gmail.com

Received: 06 April 2026; Accepted: 04 June 2026; Published: 13 November 2026

ABSTRACT: The rapid expansion of the Internet of Things (IoT) across critical sectors has significantly increased the scale, heterogeneity, and complexity of modern digital ecosystems, making cybersecurity assessment and management increasingly challenging. Although existing cybersecurity assessment models provide general evaluation frameworks, they often fail to adequately capture the unique characteristics of IoT environments, particularly in developing economies where infrastructural, regulatory, and human capacity constraints persist. This limitation stems from the reliance on static and generalized assessment approaches that overlook context-specific factors such as resource constraints, policy maturity, and adoption dynamics. To address this gap, this study proposes an integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) structured around three core domains: Readiness, Intensity, and Adoption. In the first stage, key constructs including human resource capacity, policy frameworks, regulatory support, technological effectiveness, and facilitating conditions are identified and operationalized into measurable indicators. In the second stage, a weighted composite model is developed, incorporating statistically derived coefficients to compute domain-specific sub-indices and an overall cybersecurity maturity score. The proposed model is empirically evaluated using data collected from 127 respondents and analyzed using statistical techniques in SPSS, including regression analysis, factor analysis, and ANOVA. Results indicate that human resource capacity ($\beta = 0.62$, $p < 0.05$) and policy frameworks ($\beta = 0.58$, $p < 0.05$) are significant predictors of the Readiness domain of IoT cybersecurity. In addition, within the Intensity domain, Effectiveness (EIS) emerged as the strongest predictor ($\beta = 0.728$, $p = 0.001$), highlighting the importance of effective implementation in strengthening IoT cybersecurity maturity. Furthermore, the integrated IoT-CSAM model demonstrates strong explanatory power and robustness across the Intensity, Readiness, and Adoption domains, enabling a comprehensive assessment of national IoT cybersecurity posture. Overall, this study advances IoT cybersecurity assessment by moving beyond static evaluation frameworks toward a dynamic, multi-dimensional model that incorporates contextual and structural factors. The IoT-CSAM model provides a practical and scalable tool for policymakers, regulators, and organizations in developing economies to evaluate, benchmark, and enhance their IoT cybersecurity capabilities.

KEYWORDS: Internet of Things (IoT); cybersecurity assessment; IoT-CSAM; developing economies; cybersecurity readiness; technology adoption

1 Introduction

The rapid proliferation of the Internet of Things (IoT) has fundamentally transformed digital ecosystems by enabling seamless interconnectivity among physical devices, systems, and services across diverse sectors. From smart cities and healthcare to agriculture and industrial automation, IoT technologies have introduced

Copyright © 2026 The Authors. Published by Tech Science Press. This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

unprecedented levels of efficiency, automation, and data-driven decision-making. However, this rapid expansion has simultaneously increased the scale, heterogeneity, and complexity of modern networks, significantly expanding the associated cybersecurity threat landscape. One of the most critical challenges emerging from this transformation is the growing vulnerability of IoT environments to cyber threats, largely due to their distributed architecture, resource constraints, and reliance on wireless communication channels.

Globally, the number of connected IoT devices has grown exponentially, increasing from approximately 15 billion devices in 2015 to over 30 billion devices by 2023, with projections exceeding 75 billion devices by 2030 [1]. This surge in connectivity has been accompanied by a corresponding increase in cyberattacks targeting IoT systems, including distributed denial-of-service (DDoS) attacks, data breaches, and unauthorized device access [2]. Reports indicate that IoT-related cyber incidents have risen by over 300% in recent years, with critical infrastructure sectors such as healthcare and energy being among the most affected [3]. These trends underscore the urgent need for robust, scalable, and context-aware cybersecurity assessment mechanisms capable of addressing the unique vulnerabilities inherent in IoT ecosystems.

Despite the increasing importance of IoT cybersecurity, existing assessment frameworks remain largely generalized and are often derived from traditional information systems security models that do not adequately capture the distinctive characteristics of IoT environments. Specifically, IoT systems are characterized by unattended operation, heterogeneous device architectures, limited computational capabilities, and dynamic network topologies [4], all of which introduce unique security challenges that conventional models fail to address effectively and that have prompted dedicated IoT-specific mechanisms rather than traditional IT security approaches [4,5]. Furthermore, many existing cybersecurity assessment models emphasize compliance, risk management, and return on investment metrics, while overlooking critical dimensions such as technological intensity, adoption dynamics, and contextual readiness, particularly in developing economies [6].

The situation is further compounded in developing countries, where limitations in policy frameworks, regulatory enforcement, technical expertise, and infrastructure significantly constrain the effective implementation of IoT cybersecurity measures. While baseline frameworks for IoT security in critical infrastructures have been proposed [7], their translation into national assessment practices in developing economies remains uneven, and disparities in digital maturity and institutional capacity further increase susceptibility to cyber threats. In such contexts, the absence of tailored assessment models that incorporate socio-technical and regulatory dimensions poses a significant barrier to the effective evaluation and enhancement of national IoT cybersecurity posture.

In response to these challenges, a growing body of research has explored various approaches to IoT cybersecurity, including intrusion detection systems, machine learning-based threat detection, and risk assessment frameworks, as reflected in recent surveys of IoT framework security and open security/privacy/trust challenges [8,9]. While these approaches have demonstrated promising results, significant gaps remain in terms of systematic organization, standardized evaluation metrics, and integration of contextual factors relevant to developing economies. Moreover, many of these approaches focus primarily on technical solutions without providing a comprehensive, multi-dimensional framework that integrates policy, human capacity, and adoption dynamics into a unified assessment model.

In contrast, this study proposes an integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) that is specifically designed to address the unique challenges of IoT environments in developing economies. The proposed model adopts a domain-based approach, incorporating three critical dimensions: Readiness, Intensity, and Adoption. It: (i) synthesizes key constructs from existing literature into a structured, multi-dimensional framework tailored to IoT cybersecurity assessment; (ii) develops measurable indicators and composite indices to evaluate cybersecurity maturity across the three domains; (iii) integrates statistical

validation techniques, including regression analysis and factor analysis, to ensure robustness and reliability; and (iv) provides a scalable and adaptable tool for policymakers and practitioners to assess and enhance IoT cybersecurity capabilities.

The model helps policymakers and organizations identify weaknesses and strengths, benchmark maturity, and create strategies to improve IoT ecosystem resilience.

2 Related Work

2.1 IoT Cybersecurity Landscape

IoT technologies have enabled the integration of physical and digital systems across sectors such as healthcare, energy, transportation, and smart cities. However, this integration has also expanded the cyber threat landscape, exposing critical infrastructure to vulnerabilities that were previously non-existent. IoT devices often interact with sensitive systems and data, making them attractive targets for cybercriminals. Studies have shown that the increasing adoption of IoT devices has led to a corresponding rise in cyber threats, including distributed denial-of-service (DDoS) attacks, data breaches, and unauthorized system access [2,8].

Furthermore, the interconnected nature of IoT systems implies that a single compromised device can have cascading effects across the entire network. This interconnectedness, coupled with the lack of standardized security protocols, creates significant challenges in ensuring end-to-end security. As a result, there is a growing need for comprehensive cybersecurity frameworks that can effectively address the complexity and scale of IoT ecosystems [9].

2.2 Unique Characteristics of IoT Security

IoT environments possess distinct characteristics that differentiate them from traditional information systems and make them more susceptible to cyber threats. One of the primary characteristics is unattended operation, where devices often function without direct human supervision, making them vulnerable to physical and remote attacks. Additionally, IoT devices typically rely on wireless communication, which increases the risk of eavesdropping and data interception [5].

Another critical characteristic is the limited computational and power capacity of many IoT devices. Due to these constraints, implementing complex security mechanisms such as advanced encryption and intrusion detection systems becomes challenging. This limitation often results in weak security implementations, making IoT devices easy targets for attackers. Moreover, IoT systems generate and process large volumes of data, raising concerns about data privacy, integrity, and secure storage [4,8].

2.3 IoT Security Principles and Frameworks

The foundation of IoT cybersecurity is largely guided by the Confidentiality, Integrity, and Availability (CIA) triad, which remains a fundamental model for designing secure systems. Confidentiality ensures that sensitive data is accessible only to authorized entities, integrity guarantees that data remains accurate and unaltered, and availability ensures that systems and services are accessible when needed. In addition to the CIA triad, authentication and authorization mechanisms are critical in ensuring that only legitimate devices and users can access IoT networks.

Several frameworks and standards have been proposed to enhance IoT security, including guidelines from organizations such as the European Union Agency for Cybersecurity [7]. These frameworks emphasize secure device design, data protection, risk management, and regulatory compliance. However, many of these frameworks remain generalized and are not tailored to specific contextual conditions [7,8], and

their applicability to developing economies—where infrastructure, cybersecurity awareness, and regulatory enforcement are often limited—remains insufficiently addressed.

2.4 Limitations of Existing IoT Cybersecurity Models

Despite the availability of various cybersecurity frameworks, significant gaps remain in their applicability to IoT environments, particularly in developing countries. Most existing models are designed for traditional IT systems and focus heavily on compliance, risk assessment, and return on investment metrics. These approaches often overlook critical dimensions such as technological intensity, adoption levels, and readiness of institutions and human resources [9].

Additionally, many existing approaches emphasize technical solutions, such as intrusion detection systems and machine learning-based threat detection. However, as arguments for adaptive, socio-technical cybersecurity policy models in critical infrastructure organizations make clear [10], factors such as policy frameworks, user awareness, and institutional capacity play a crucial role in cybersecurity outcomes, and a narrow technical focus limits effectiveness in real-world deployments.

Another key limitation is the lack of standardized evaluation metrics for assessing IoT cybersecurity maturity. Many studies rely on accuracy-based metrics or isolated performance indicators [11], which do not provide a comprehensive view of cybersecurity readiness and effectiveness, creating a gap in the development of holistic assessment models that can guide policymakers and organizations in improving their cybersecurity posture.

2.5 Comparative IoT Cybersecurity Landscape: Developed vs. Developing Economies

The rapid evolution of the Internet of Things (IoT) has significantly reshaped the global cybersecurity landscape, making IoT security an increasingly important research domain. This is driven by the exponential growth in connected devices, the expansion of attack surfaces, and the highly distributed and interconnected nature of IoT ecosystems [12]. Unlike traditional computing environments, IoT systems consist of heterogeneous, resource-constrained, and geographically dispersed devices, which introduce complex and continuously evolving security challenges. Consequently, securing IoT environments requires specialized cybersecurity frameworks that extend beyond conventional information security models and are specifically designed to address IoT's operational, architectural, and resource limitations [13].

Although IoT cybersecurity risks are global, there are clear and measurable disparities in how these risks manifest across developed and developing economies. In developed countries, IoT ecosystems are supported by advanced digital infrastructure, high broadband penetration, stable electricity supply, mature cybersecurity governance frameworks, standardized security practices, and a well-trained cybersecurity workforce. For example, internet penetration in many high-income countries exceeds 90%, and broadband speeds frequently surpass 100 Mbps, enabling real-time threat monitoring and automated security updates [14,15]. These environments also benefit from well-established incident response systems, widespread adoption of security-by-design principles, and continuous investment in cybersecurity innovation. As a result, IoT systems in these settings are more likely to implement advanced protections such as automated patch management, zero-trust architectures, and AI-driven threat detection systems [16].

In contrast, developing economies face persistent and multidimensional infrastructural limitations that significantly weaken IoT cybersecurity resilience. These include unreliable electricity supply, limited broadband coverage, low internet speeds, weak cybersecurity governance, and insufficient investment in digital security infrastructure. For instance, in several Sub-Saharan African countries, internet penetration remains below 50%, and rural connectivity can fall below 20%, creating uneven exposure to IoT-enabled

services [17,18]. Frequent power interruptions further disrupt IoT system availability and hinder continuous security monitoring, while limited access to secure data centers and cloud infrastructure increases reliance on poorly protected local deployments.

In addition, many organizations in developing economies operate with outdated hardware, unpatched systems, and minimal cybersecurity controls due to cost constraints and limited technical expertise. Cybersecurity workforce shortages are also significant; global reports estimate a shortage of millions of cybersecurity professionals, with the gap being most severe in low- and middle-income countries [19]. Furthermore, weak enforcement of data protection regulations and low levels of cybersecurity awareness among users exacerbate vulnerabilities, increasing exposure to threats such as ransomware, device hijacking, and distributed denial-of-service (DDoS) attacks.

These infrastructural and institutional weaknesses create a fundamentally different cybersecurity context compared to developed economies. While developed regions focus on optimization of advanced security systems, developing economies often struggle with foundational issues such as connectivity stability, system availability, and basic security implementation. This disparity highlights why many existing IoT cybersecurity frameworks designed under assumptions of stable infrastructure and high technological maturity fail to adequately represent conditions in resource-constrained environments [20].

Therefore, the observed infrastructural gaps provide a strong justification for the IoT-CSAM model, particularly its emphasis on domains such as Readiness, Intensity, and Adoption. These dimensions are essential for capturing infrastructural preparedness, the extent of IoT deployment, and the level of cybersecurity integration in environments where foundational digital infrastructure remains uneven and evolving.

2.6 Cybersecurity Assessment Models and Positioning of the IoT-CSAM Framework

Cybersecurity assessment models provide structured mechanisms for evaluating the security posture, maturity, and resilience of information systems within a defined environment. According to [21], a cybersecurity model constitutes a predefined set of policies, procedures, and controls designed to enhance security practices within an organization or system context. Similarly, the U.S. Department of Energy Cybersecurity Capability Maturity Model [22] defines an assessment model as a benchmark framework used to evaluate an entity's cybersecurity capability, including its processes, practices, and technological safeguards, while also supporting the establishment of improvement targets and priorities. These models are often tailored to specific sectors, industries, or national contexts and are primarily intended to reduce unknown vulnerabilities and misconfigurations within targeted environments [23].

From a systems perspective, IoT cybersecurity assessment requires both macro-level and micro-level analysis. At the macro level, the assessment encompasses the entire IoT ecosystem, including interconnected devices, communication protocols, software platforms, and supporting infrastructure. At the micro level, attention is given to individual components such as hardware configurations, firmware integrity, communication interfaces, programming environments, and third-party integrations, all of which may introduce unique vulnerabilities. This dual-level analysis is essential because IoT environments exhibit high heterogeneity and interdependence, where weaknesses in a single component can propagate across the entire system.

Despite the existence of multiple cybersecurity frameworks, a critical limitation in the literature is the fragmented nature of existing assessment approaches, which often focus on isolated dimensions such as technical controls, risk management, or compliance requirements. To address this gap, this study positions the proposed IoT-CSAM model within existing cybersecurity maturity and assessment frameworks by drawing conceptual alignment while highlighting key distinctions. Specifically, the IoT-CSAM integrates three core

domains; Readiness, Intensity, and Adoption which are synthesized from established models but restructured into a unified and context-sensitive framework tailored for IoT environments in developing economies.

To further justify the development of IoT-CSAM, a comparative synthesis of foundational cybersecurity models is presented below, demonstrating how existing frameworks inform but do not fully capture the multidimensional requirements of IoT cybersecurity assessment.

2.6.1 Holistic Digital Forensic Readiness (DFR) Model

The holistic Digital Forensic Readiness (DFR) model, grounded in ISO/IEC 27001 and ISO/IEC 27043 standards, emphasizes preparedness for digital investigations through structured planning, implementation, and evidence management processes [24]. It integrates organizational readiness, forensic data management, and IoT security layers to ensure that potential digital evidence is identified, preserved, and protected across the data lifecycle.

While this model significantly contributes to the concept of organizational readiness, its primary focus is forensic preparedness rather than continuous cybersecurity maturity assessment. It does not explicitly incorporate IoT adoption levels or operational intensity of IoT deployments, thereby limiting its applicability as a comprehensive IoT cybersecurity assessment framework.

2.6.2 Generic Threat Matrix Model

The Generic Threat Matrix provides a structured approach for characterizing cyber threats based on attributes such as intensity, technical capability, resources, and stealth [25]. It supports operational threat assessment by enabling analysts to evaluate attacker capabilities and identify potential attack paths.

Although this model significantly informs threat characterization, it is primarily attacker-centric and does not incorporate organizational readiness or technology adoption dimensions. In this study, the concept of intensity is adapted from this model to measure the level of cyber threat exposure within IoT environments.

2.6.3 Security Diffusion Model

The Security Diffusion Model explains cybersecurity adoption behavior by focusing on adopter characteristics, innovation attributes, communication channels, and decision processes [26]. It emphasizes how perceived usefulness, complexity, and effectiveness influence the adoption of security innovations [27].

However, this model is largely behavioral and does not account for infrastructural readiness or the technical intensity of IoT systems. In IoT-CSAM, the adoption domain is conceptually informed by this model but extended to include organizational and technological adoption within IoT environments.

2.6.4 ISO/IEC 27001 Information Security Management System (ISMS)

ISO/IEC 27001 [28] provides a globally recognized framework for establishing, implementing, maintaining, and continuously improving information security management systems. It adopts a risk-based approach and defines extensive controls across multiple domains to manage organizational security risks.

Despite its comprehensiveness, ISO/IEC 27001 is a general-purpose and not specifically designed for IoT ecosystems. It assumes relatively stable IT environments and does not explicitly address IoT heterogeneity, device constraints, or adoption variability across different economic contexts.

2.6.5 NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides five core functions: Identify, Protect, Detect, Respond, and Recover to guide cybersecurity risk management [29]. It is widely adopted across industries for improving cyber resilience.

However, while highly effective, the framework lacks a formal quantitative mechanism for measuring cybersecurity maturity levels and does not provide a structured assessment model for IoT-specific environments.

2.6.6 COBIT Framework

COBIT integrates governance and management of enterprise IT, focusing on aligning IT objectives with business goals [30]. It emphasizes control objectives, performance measurement, and stakeholder value creation.

Although COBIT provides strong governance structures, it is primarily enterprise-oriented and not specifically designed for IoT ecosystems or resource-constrained environments, limiting its direct applicability to IoT cybersecurity maturity assessment.

2.6.7 COSO Framework

The COSO framework focuses on enterprise risk management through control environments, risk assessment, control activities, monitoring, and communication [31]. It supports organizational risk governance and compliance assurance.

However, COSO is broad and financial-risk oriented and does not explicitly incorporate technological intensity or IoT adoption dynamics, making it insufficient as a standalone IoT cybersecurity assessment model.

2.6.8 General Cybersecurity Process Model

General cybersecurity process models typically comprise the Identify, Protect, Detect, Respond, and Recover lifecycle [32]. These processes provide a foundational structure for cybersecurity operations and incident management.

While useful for operational security, this model does not provide a maturity-based assessment structure or incorporate contextual factors such as infrastructure readiness or technology adoption, which are essential for evaluating IoT ecosystems.

2.6.9 Positioning and Justification of the IoT-CSAM Model

A review of existing cybersecurity frameworks reveals that although each contributes valuable constructs such as readiness, intensity, and adoption, none provides an integrated, IoT-specific, and context-aware assessment model. Existing frameworks remain largely incremental, focusing on isolated dimensions such as compliance, governance, or technical controls without integrating them into a unified maturity assessment structure.

To address this gap, the proposed IoT-CSAM framework integrates Readiness, Intensity, and Adoption into a single structured model tailored for IoT environments in developing economies. This integration enables a more comprehensive evaluation of cybersecurity maturity by explicitly incorporating infrastructural constraints, technological deployment levels, and organizational cybersecurity capability within a unified assessment framework.

2.7 Research Gap and Contribution

From the foregoing analysis, it is evident that while significant progress has been made in IoT cybersecurity research, there remains a lack of integrated, context-aware assessment models that address the unique challenges of IoT environments in developing economies. Existing frameworks fail to provide a multi-dimensional perspective that combines technical, regulatory, and socio-economic factors into a unified evaluation model.

This study addresses this gap by proposing an Integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) that incorporates three key domains: Readiness, Intensity, and Adoption. By integrating these dimensions, the model provides a comprehensive framework for evaluating IoT cybersecurity maturity and supports informed decision-making for policymakers and practitioners.

3 Methodology

This study adopts a Design Science Research (DSR) methodology to develop and validate an integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM). The DSR approach is particularly suitable for this study as it focuses on the creation and evaluation of artefacts designed to solve identified real-world problems, in this case, the lack of a comprehensive and context-aware IoT cybersecurity assessment framework for developing economies [33]. The methodology follows established DSR guidelines, including problem identification, objective definition, artefact design and development, demonstration, evaluation, and communication of results [33].

3.1 Research Design

A mixed-methods research design was employed, combining both quantitative and qualitative approaches to ensure a comprehensive understanding of IoT cybersecurity practices. The quantitative component involved the collection of structured data through questionnaires, while the qualitative component involved semi-structured interviews with domain experts to provide contextual insights and validate the model constructs.

The study targeted stakeholders involved in IoT deployment, cybersecurity management, and policy formulation, including IT professionals, system administrators, regulatory authorities, and academic experts. This ensured that the data captured reflected both technical and institutional perspectives relevant to IoT cybersecurity.

3.2 Sampling Technique and Sample Size

A combination of simple random sampling and purposive sampling techniques was employed. Simple random sampling was used to select respondents from a broader population of ICT practitioners to ensure representativeness, while purposive sampling was used to identify key informants with specialized knowledge in IoT and cybersecurity.

The study involved a target population of 190 respondents from selected organisations, including ICT administrators, security analysts, IT specialists, information systems managers and heads, IT security administrators and managers, IT experts, administrators, and information systems end-users. These respondents were selected based on their knowledge and experience in ICT and cybersecurity. 127 questionnaires were distributed, of which 80 valid responses were obtained, representing a 63% response rate. The sample size of 127 was determined using the Krejcie and Morgan (1970) [34] sample size determination table. In addition, the sample was considered adequate for the planned statistical analyses and model development, consistent with sample sizes used in similar cybersecurity studies and sufficient for multivariate analyses, including

regression and factor analysis [15]. A post-hoc power consideration further indicated that, given the number of predictors and observed effect sizes, the study achieved acceptable statistical power (≥0.80) for detecting medium-to-large effects at the 5% significance level, supporting the statistical validity of the regression estimates. Selected IoT and cybersecurity experts were purposively sampled to validate the developed Cybersecurity Assessment Model (IoT-CSAM) in terms of its functionality, usability, reliability and validity.

3.3 Data Collection Methods

Data were collected using two primary instruments:

Structured Questionnaires: Data were collected using a structured questionnaire comprising Likert-scale items measuring key IoT cybersecurity constructs, including human resource capacity, policy frameworks, regulatory support, technological effectiveness, and adoption-related factors. The items were adapted from relevant literature and refined to suit the study context. The questionnaire was pre-tested to ensure clarity, reliability, and validity before full deployment, and feedback from the pre-test was used to revise and improve the instrument. Construct scores were obtained by aggregating the corresponding item responses using consistent scoring procedures. Internal consistency was assessed using Cronbach's alpha, with results showing high reliability for Readiness (15 items, $\alpha = 0.934$), Intensity (27 items, $\alpha = 0.968$), and Adoption (20 items, $\alpha = 0.922$). These coefficients exceeded the acceptable threshold, confirming the internal consistency and reliability of the questionnaire.

Semi-Structured Interviews: These were conducted with selected experts to validate the constructs and provide deeper insights into the contextual challenges of IoT cybersecurity in developing economies.

3.4 Data Analysis Techniques

The collected data were analyzed using the Statistical Package for the Social Sciences (SPSS) V26. Descriptive statistics, including means, standard deviations, and frequency distributions, were used to summarize respondent characteristics and assess general trends in IoT cybersecurity practices.

For the Exploratory Factor Analysis (EFA), Principal Component Analysis (PCA) was used as the extraction method, with Varimax rotation applied to facilitate interpretation of the factor structure. Sampling adequacy was assessed using the Kaiser-Meyer-Olkin (KMO) test (value = 0.842) and Bartlett's Test of Sphericity ($\chi^2 = 1486.37$, df = 276, $p < 0.001$). Factors were retained based on eigenvalues greater than 1.0, inspection of the scree plot, and theoretical interpretability. Items with factor loadings of 0.50 or higher were considered acceptable. The analysis resulted in three components representing Readiness (ICSR), Intensity (ICSI), and Adoption (ICSA), jointly explaining 68.4% of the total variance.

For the multiple regression analysis, composite scores were generated for the relevant constructs and entered into the respective regression models. The analysis reported unstandardized coefficients (B), standard errors, standardized beta coefficients (β), t-values, and *p*-values, with statistical significance assessed at $\alpha = 0.05$. Multicollinearity was assessed using tolerance and VIF statistics, with values ranging from 0.54–0.81 for tolerance and 1.23–1.85 for VIF. The Durbin-Watson statistic (value = 1.91) was used to assess independence of residuals. Linearity and homoscedasticity were examined using residual plots, while residual normality was assessed using standardized residuals and normal probability plots.

The regression models for Readiness (ICSR), Intensity (ICSI), and Adoption (ICSA) are subsequently represented and presented in the respective sections below.

4 Results and Discussion

This section presents the findings of the study based on the primary data. The results are organized into descriptive statistics, factor analysis, regression analysis, and model evaluation.

4.1 Awareness of IoT Technologies

Descriptive statistics were used to summarize the characteristics of the respondents and assess general trends in IoT cybersecurity practices. The results indicated that the majority of respondents had moderate to high awareness of IoT technologies, but relatively lower levels of cybersecurity preparedness.

- The mean score for IoT Cybersecurity Readiness (ICSR) was 3.12, indicating a moderate level of preparedness.
- The mean score for IoT Cybersecurity Intensity (ICSI) was 3.05, suggesting moderate implementation of cybersecurity measures.
- The mean score for IoT Cybersecurity Adoption (ICSA) was 3.28, indicating relatively higher acceptance and perceived usefulness of IoT cybersecurity practices.

These findings suggest that while adoption levels are increasing, readiness and implementation intensity remain areas of concern, particularly in developing economies.

4.2 Factor Analysis Results

Exploratory Factor Analysis (EFA) was conducted to validate the grouping of variables into the three domains of the IoT-CSAM model.

Three principal components were extracted, corresponding to: Readiness (ICSR), Intensity (ICSI) and Adoption (ICSA).

The total variance explained by the three components was 68.4%, indicating a strong model structure.

Factor loadings for all variables were above 0.60, confirming construct validity.

This validates the conceptual structure of the IoT-CSAM model and supports its multidimensional approach.

4.3 Metrics Mathematical Modeling

Having presented the three main sub-indices of the model, herein, the mathematical modelling of the three sub-indices is presented.

4.3.1 Readiness

Let Readiness, R, be expressed as a constituent of its significant constructs, such as:

Readiness {Policy, Regulation, Literacy, Human Resource}

To represent each of these constructs, Table 1 provides the assumed Mathematical representations for each of the constructs.

Table 1: Construct parameters of readiness.

Construct	Construct Parameters	Mathematical Representation
Readiness		***R***
	Policy (POL)	R_{pol}
	Regulation (HO)	R_{ho}
	Literacy (DL)	R_{dl}
	Human Resource (MBAD)	R_{mbad}

Having defined these, R can be defined as shown in Eq. (1):

$$R \rightarrow f(R_{pol}, R_{ho}, R_{dl}, R_{mbad}) \tag{1}$$

where f is a linear regression function.

Consequently, replacing f with the appropriate regression coefficients results in Eq. (2):

$$R = \beta_0 + \beta_1 R_{pol} + \beta_2 R_{ho} + \beta_3 R_{dl} + \beta_4 R_{mbad} \tag{2}$$

From the analysis, these coefficients were determined to be as indicated in Table 2.

Table 2: Coefficients of readiness.

Coefficients[a]						
Model		**Unstd. Coef**		**Std. Coef**	**T**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	−1.365	0.647		−2.108	0.042
	DL	0.222	0.090	0.205	2.463	0.018
	POL	0.324	0.103	0.259	3.138	0.003
	HO	0.171	0.081	0.127	2.103	0.042
	MBAD	0.405	0.125	0.379	3.225	0.003

Note: [a]Dependent Variable: ICSR.

From the results in Table 2, it follows that readiness can be defined as shown in Eq. (3).

$$R = -1.365 + 0.259 R_{pol} + 0.127 R_{ho} + 0.205 R_{dl} + 0.379 R_{mbad} \tag{3}$$

Table 2 presents the regression coefficients used to model IoT cybersecurity Readiness. The results indicate that all predictors (Policy, Regulation, Literacy, and Human Resource capacity) have a statistically significant influence on Readiness, as all p-values are below 0.05. Among the predictors, Human Resource (MBAD) has the strongest influence (β = 0.379), followed by Policy (β = 0.259), Literacy (β = 0.205), and Regulation (β = 0.127). This implies that human capacity development contributes most significantly to improving cybersecurity readiness within IoT environments.

4.3.2 Intensity

Let Intensity, I, be expressed as a constituent of its significant constructs, such as:

Intensity {Effectiveness, Implementation, applications}

To represent each of these constructs, Table 3 provides the assumed Mathematical representations for each of the Intensity constructs.

Table 3: Construct parameters of intensity.

Intensity	*I*
IoT cyber security applications (ICA)	I_{ica}
Effectiveness of IoT cyber security (EIS)	I_{eis}
Perceived implementation of IoT cyber security (ICS)	I_{ics}

Similarly, like the readiness above, the Intensity is defined as shown in Eq. (4):

$$I \rightarrow f(I_{eis}, I_{ics}, I_{ica}) \tag{4}$$

where f is a linear function.

Having defined these, I can be defined as shown in Eq. (5):

$$I = \beta_0 + \beta_1 I_{eis} + \beta_2 I_{ics} + \beta_3 I_{ica} \tag{5}$$

The coefficients were determined to be as indicated in Table 4:

Table 4: Coefficients of intensity.

Coefficients[a]						
Model		Unstd. Coef		Std. Coef	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.78	0.229		−0.08	0.018
	ICS	0.276	0.018	0.584	15.296	0.000
	ICA	0.227	0.033	0.267	6.898	0.000
	EIS	0.713	0.207	0.728	3.443	0.001

Note: [a]Dependent Variable: ICSI.

Consequently, replacing f with the appropriate regression coefficients results in Eq. (6):

$$I = 0.78 + 0.728 I_{eis} + 0.584 I_{ics} + 0.267 I_{ica} \tag{6}$$

Results from Table 4 above show that all intensity constructs significantly contribute to IoT cybersecurity Intensity. The most influential predictor is Effectiveness (EIS) with a beta value of 0.728, indicating that perceived effectiveness of cybersecurity measures strongly determines system intensity. Implementation (ICS) also shows a strong effect (β = 0.584), while Applications (ICA) contributes moderately (β = 0.267). The results confirm that intensity is largely driven by how effectively cybersecurity measures are perceived and implemented within IoT environments.

4.3.3 Adoption

Let Adoption, A be expressed as a constituent of its significant constructs, such as:

Adoption {Relative advantage, Facilitating Conditions}

To represent each of these constructs, Table 5 provides the assumed Mathematical representations for each of the Adoption constructs.

Table 5: Construct parameters of adoption.

Adoption	*A*
Relative Advantage (RA)	A_{ra}
Facilitating Conditions (FC)	A_{fc}

Similarly, like the other two metrics, the adoption can be defined as shown in Eq. (7):

$$A \rightarrow f(A_{ra}, A_{fc}) \tag{7}$$

where f is a linear function.

Further, this can be defined as in Eq. (8):

$$A = \beta_0 + \beta_1 A_{ra} + \beta_2 A_{fc} \tag{8}$$

Consequently, the beta coefficients for adoption are presented in Table 6.

Table 6: Beta coefficients of adoption.

Coefficients[a]					
Model	**Unstd. Coef**		**Std. Coef**	**T**	**Sig.**
	B	**Std. Error**	**Beta**		
(Constant)	0.82	0.273		2.385	0.018
FC	0.619	0.124	1.012	5.009	0.000
RA	0.715	0.112	1.008	5.850	0.000

Note: [a]Dependent Variable: ISCA.

Finally, A can be defined as Eq. (9):

$$A = 0.82 + 1.008A_{ra} + 1.012A_{fc} \tag{9}$$

Table 6 indicates that both Facilitating Conditions and Relative Advantage significantly influence IoT cybersecurity Adoption. Facilitating Conditions (β = 1.012) slightly outweigh Relative Advantage (β = 1.008), suggesting that organizational and infrastructural support systems play a marginally stronger role in driving adoption decisions. The results imply that adoption of IoT cybersecurity practices is highly dependent on the availability of enabling environments and perceived benefits of the security technologies.

4.3.4 IOTCSAM Mathematical Modeling

Having defined all metrics, the IOT Cyber Security Assessment Model (IOTCSAM) is hereby denoted consistently as M and defined as indicated in Eq. (10): The model integrates the three core components: Readiness (R), Intensity (I), and Adoption (A).

$$M \to f(f(R, I, A)) \tag{10}$$

where f is a linear function.

Since R, I, and A are already defined in Eqs. (1)–(9), then M is defined in (11):

$$M = R + I + A \tag{11}$$

Replacing each of the parameters R, I, and A, then we get:

$$\begin{aligned} M = {} & \left(-1.365 + 0.259R_{pol} + 0.127R_{ho} + 0.205R_{dl} + 0.379R_{mbad}\right) + \left(0.78 + 0.728I_{eis} + 0.584I_{ics}\right. \\ & \left. +0.267I_{ica}\right) + \left(0.82 + 1.008A_{ra} + 1.012A_{fc}\right) \end{aligned} \tag{12}$$

Combining constant terms:

$-1.365 + 0.78 + 0.82 = 0.235$

Therefore, the simplified final IoT-CSAM model becomes:

Resolving Eq. (12), then IOTCSAM *(M)*, becomes (13):

$$\begin{aligned} M = {} & 0.235 + 0.259R_{pol} + 0.127R_{ho} + 0.205R_{dl} + 0.379R_{mbad} + 0.728I_{eis} + 0.584I_{ics} \\ & +0.267I_{ica} + 1.008A_{ra} + 1.012A_{fc} \end{aligned} \tag{13}$$

Eq. (13) defines the final model, M, based on the various metric constructs. Since each of the components can have a maximum score of 5, the maximum score for the model would be 35. The following distribution of scores for the model thus determines the assessment levels of IoT cybersecurity in a country.

Table 7 presents the classification thresholds used to interpret the overall IoT-CSAM score. The model output ranges from 1 to 35, where higher scores indicate stronger cybersecurity maturity. Scores between 1 and 12 represent low cybersecurity maturity, indicating weak readiness, limited implementation intensity, and poor adoption levels. Scores between 13 and 24 indicate moderate maturity, reflecting partial implementation of cybersecurity practices. Scores between 25 and 35 represent high maturity, indicating strong readiness, high intensity of implementation, and advanced adoption of cybersecurity practices within IoT environments.

Table 7: Model assessment scores and interpretation.

Assessment Score	Interpretation
1–12	Low
13–24	Medium
25–35	High

4.4 Model Development (IoT-CSAM) and Validation

The IOTCSAM model seeks to establish a metric across the entire IoT Cyber Security ecosystem using three critical metrics of readiness, intensity, and adoption to measure the state of IoT Cyber Security in developing countries. The model is a composite metric drawn from the three independent sub-indices. For purposes of clarity, the defined sub-indices are hereby briefly presented as determined earlier in the thesis.

i. *IoT Cyber Security readiness (ICSR)*: The ENISA model for assessment of cyber security [7] identifies readiness in view of the technical, commercial, and physical infrastructures required to support IoT Cyber Security.
ii. *IoT Cyber Security intensity sub-index (ICSI)*: This is mainly concerned with the state of IoT Cyber Security implementation and effectiveness, respectively. Primarily, this means that IoT Cyber Security intensity metrics would give an indication of the use of IoT Cyber Security, and the demographics of the users, as well as the effectiveness of IoT Cyber Security deployments. For this study, significant metrics determined were the IoT Cyber Security applications (ICA), Effectiveness (EIS), and Implementation (ICS).
iii. *IoT Cyber Security adoption sub-index (ICSA)*: This is concerned with the attitudinal, normative, and control factors that influence intentions to adopt IoT Cyber Security. Two metrics, namely Relative Advantage (RA) and Facilitating Conditions (FC), were identified to be most significantly explaining the variation in IoT Cyber Security Adoption.

Consequently, it is postulated that the overall state of IoT Cybersecurity within a given country, measured using the IoT Cyber Security Assessment Metric (IoT-CSAM), is influenced by the three principal sub-indices: IoT Cyber Security Readiness (ICSR), IoT Cyber Security Intensity (ICSI), and IoT Cyber Security Adoption (ICSA). These sub-indices may contribute either equally or in varying proportions to the overall cybersecurity maturity level, depending on the contextual conditions of a given environment. Each sub-index is further composed of a set of underlying constructs that collectively define its structure and explanatory power.

To determine the most significant contributors within each sub-index, the study identified nine (9) key constructs that were statistically and theoretically significant in explaining variations in the dependent variables across the three domains. These constructs represent the most influential factors shaping IoT cybersecurity maturity and form the empirical basis for the development of the IoT-CSAM framework. Table 8 summarizes the significant constructs associated with each sub-index.

Table 8: Significant constructs for ICSR, ICSI, and ICSA.

Sub-Index	Significant Constructs
IoT Cyber Security Readiness (ICSR)	Digital Literacy (DL), Policy (POL), Human Resource (MBAD), and Regulatory (REG)
IoT Cyber Security Intensity (ICSI)	Education (ED) and Years of Experience (EX), Effectiveness of IoT Cyber Security (EIS), Perceived Implementation of IoT Cyber Security (ICS)
IoT Cyber Security Adoption (ICSA)	Relative Advantage (RA) and Facilitating Conditions (FC)

Table 8 presents the final set of constructs that significantly contribute to the three IoT cybersecurity sub-indices forming the IoT-CSAM model. For ICSR, Digital Literacy, Policy, Regulation, and Human

Resource Capacity were retained as significant predictors. This indicates that cybersecurity readiness is associated with both organizational and human-capability factors.

For ICSI, Education, Years of Experience, Effectiveness of IoT Cybersecurity, and Perceived Implementation of IoT Cybersecurity were identified as significant predictors. The inclusion of Education and Years of Experience reflects the human-capability dimension, while Effectiveness and Perceived Implementation represent the operational dimension of cybersecurity intensity.

For ICSA, adoption is primarily driven by Relative Advantage and Facilitating Conditions, indicating that organizations are more likely to adopt IoT cybersecurity measures when they perceive clear benefits and when enabling infrastructural and organizational support systems are in place.

Overall, Table 8 confirms that IoT cybersecurity maturity is a multi-dimensional construct shaped by a combination of governance, human, technical, and infrastructural factors, thereby justifying the integrated structure of the IoT-CSAM model. In line with this, Fig. 1 below presenting the IoT Cyber Security Assessment (IoT-CSAM) model and metric.

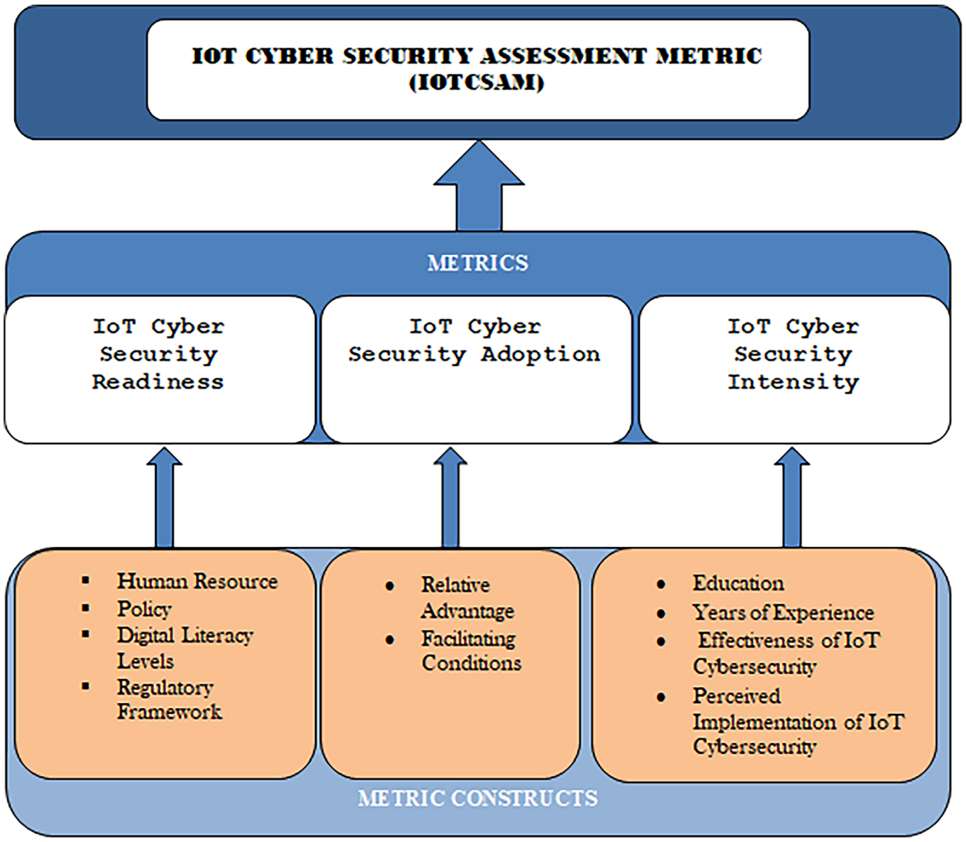


Figure 1: The IoT cyber security assessment (IOTCSAM) model and metric (Source: Researchers).

As seen in the model above, the IoT-CSAM model consists of three sub-indices: Readiness (ICSR), Intensity (ICSI), and Adoption (ICSA). The overall model is expressed as:

IoT-CSAM = w1(ICSR) + w2(ICSI) + w3(ICSA)

where weights (w1, w2, w3) are determined based on factor loadings derived from statistical analysis.

Fig. 1 above presents the conceptual structure and operational flow of the IoT Cyber Security Assessment Metric (IoT-CSAM), illustrating how individual cybersecurity indicators are systematically aggregated into progressively higher levels of assessment. At the base level, the model consists of metric constructs that represent measurable indicators of IoT cybersecurity performance, which are organized into three main categories.

The first category is Readiness constructs, which include Human Resource capacity, policy frameworks, digital literacy levels, and the regulatory environment, reflecting the foundational institutional and infrastructural preparedness for secure IoT deployment. The second category, Adoption constructs, comprises Relative Advantage and Facilitating Conditions, capturing the extent to which cybersecurity solutions are accepted and supported within an organization or broader environment. The third category, Intensity constructs, includes Education, Working Experience, Effectiveness of IoT Cybersecurity measures, and Perceived Implementation of IoT Cybersecurity practices, which collectively reflect the depth and operational strength of cybersecurity execution in IoT settings.

These constructs feed into the second level of the framework, which consists of three aggregated metrics: IoT Cyber Security Readiness, IoT Cyber Security Adoption, and IoT Cyber Security Intensity. Each metric is derived from its corresponding constructs, transforming raw indicators into structured sub-index scores that represent distinct dimensions of cybersecurity maturity.

At the highest level, the three metrics converge to form the overall IoT Cyber Security Assessment Metric (IoT-CSAM), which provides a composite measure of cybersecurity maturity for a given IoT environment or country. The directional flow in the framework reflects a hierarchical aggregation process in which lower-level constructs inform intermediate indices, which then collectively determine the final IoT-CSAM score, ensuring a multidimensional assessment that integrates technical, organizational, and contextual cybersecurity factors.

4.4.1 IOTCSAM Model Algorithm

The diagrammatic representation of the IoT Cyber Security Assessment model (IOTCSAM) is presented in Section 4.4 above, and the Mathematical model implementation algorithm is presented in the following section, as seen below (Algorithm 1).

Algorithm 1: Iot cyber security assessment model

Input: M{R, I, A};
R $\{R_{pol},\ R_{ho},\ R_{dl},\ R_{mbad}\}$
$I\ \{(I_{eis},\ I_{ics},\ I_{iex}, I_{ied},\}$
$A\ \{A_{ra},\ A_{fc}\}$
Output: M_{score}; Assessment_Score;
START:
STEP 1: Enter the specific scores:
IF (selected == R)
$R[] \leftarrow R_i\ where i\ \varepsilon\ R$
ELSE IF (selected == I)
$I[] \leftarrow I_i\ where i\ \varepsilon\ I$
ELSE (selected == A)
$A[] \leftarrow A_i\ where i\ \varepsilon\ A$
END IF

(Continued)

Algorithm 1 (continued)

STEP 2: Compute the constituent Scores of R, I, and A:

$R = -1.365 + 0.259R_{pol} + 0.127R_{ho} + 0.205R_{dl} + 0.379R_{mbad}$

$I = 0.78 + 0.728I_{eis} + 0.584I_{ics} + 0.267I_{ica}$

$A = 0.82 + 1.008A_{ra} + 1.012A_{fc}$

STEP 3: Compute Model Composite Score:

$M_{score} = R + I + A$

STEP 4: Cyber Security Assessment Score Interpretation:

IF ($M_{score} \leq 12$)

Assessment_Score = low;

ELSE IF ($M_{score} > 12$ && $M_{score} \leq 24$)

Assessment_Score = Medium;

ELSE IF ($M_{score} > 24$ && $M_{score} \leq 35$)

Assessment_Score = High;

ELSE

Output ("Error");

END IF

STOP!

4.4.2 IOTCSAM Model Validation

The developed IoT-CSAM model was validated using the Delphi method involving 26 purposively selected experts, chosen based on their expertise in Internet of Things (IoT), cybersecurity, information systems, and digital infrastructure. The selection was guided by their professional involvement in either academia, industry practice, or cybersecurity policy development, ensuring informed judgment in evaluating the model. The expert panel had a mix of experienced practitioners and researchers, with most having more than 5–15 years of experience in ICT and cybersecurity-related fields, across both public and private sector institutions.

The Delphi technique was adopted due to its suitability in situations with limited empirical IoT cybersecurity data and its ability to facilitate structured expert consensus among geographically dispersed participants through iterative questionnaire-based evaluation [35]. Experts assessed the model constructs and metrics using a five-point Likert scale. The results indicated strong validation, with 79.3% agreement on the model's suitability and 82.5% affirmation of the effectiveness of the proposed metrics for assessing IoT cybersecurity in developing countries.

The developed model was further evaluated using Design Science Research (DSR) evaluation criteria, including:

Functionality: Ability of the model to assess IoT cybersecurity maturity.

Usability: Ease of application by policymakers and practitioners.

Reliability: Consistency of results across different datasets.

Validity: Accuracy in representing real-world IoT cybersecurity conditions.

The evaluation results, supported by expert feedback and statistical outputs, confirm that the IoT-CSAM model is both practically applicable and methodologically robust for deployment in developing economies.

The composition of the expert panel is summarized in Table 9, showing a balanced representation from academia, industry, and government, as well as substantial experience in cybersecurity and IoT domains.

Table 9: Validation expert composition.

Category	Classification	Frequency (n)	Percentage (%)
Sector	Academia (Lecturers/Researchers)	11	42.3
	Industry (ICT/Cybersecurity Professionals)	10	38.5
	Government/Policy Experts	5	19.2
Experience in ICT/Cybersecurity	5–9 years	9	34.6
	10–14 years	12	46.2
	15+ years	5	19.2
Area of Expertise	Cybersecurity & Information Security	13	50.0
	Internet of Things (IoT) Systems	7	26.9
	Information Systems/ICT Governance	6	23.1
Highest Qualification	Master's Degree	10	38.5
	PhD	9	34.6
	Professional Certification (such as CISSP, CISM, CEH)	7	26.9

Model Fitness

The fitness of the developed IoT Cybersecurity Assessment Model (IoT-CSAM) was evaluated using the coefficient of determination (R^2), adjusted R^2, and Analysis of Variance (ANOVA). The results indicate that the model demonstrates strong explanatory and predictive capability.

The coefficient of determination (R^2) was 0.67, implying that 67% of the variation in IoT cybersecurity maturity can be explained by the independent variables included in the model. This suggests that the model provides substantial explanatory power in assessing IoT cybersecurity maturity within developing economies. Furthermore, the Adjusted R^2 value of 0.64 confirms the robustness and reliability of the model after adjusting for the number of predictors included in the regression analysis.

Analysis of Variance (ANOVA) was conducted to determine the overall statistical significance of the regression model. The results are presented in Table 10.

Table 10: Model fitness and ANOVA results for the IoT cybersecurity assessment model.

Source	Sum of Squares	df	Mean Square	F-Value	*p*-Value
Regression	245.36	4	61.34	12.45	0.000
Residual	121.78	122	0.99		

The ANOVA results show an F-value of 12.45 with a significance level of $p < 0.001$, indicating that the regression model is statistically significant. This demonstrates that the predictor variables collectively contribute to explaining variations in IoT cybersecurity maturity and confirms the suitability of the IoT-CSAM model for cybersecurity assessment and predictive analysis in developing economy contexts.

5 Discussion of Findings

The findings of this study provide empirical support for the growing body of literature emphasizing the multidimensional nature of IoT cybersecurity, particularly in developing economies. The significant influence of human resource capacity ($\beta = 0.62$, $p < 0.05$) on IoT cybersecurity readiness underscores the critical role of technical skills, awareness, and training in mitigating cyber risks. This aligns with prior studies, which identify the shortage of cybersecurity expertise as a major barrier to effective IoT security

implementation, especially in resource-constrained environments [9]. The increasing complexity of IoT ecosystems demands specialized knowledge, and without adequate human capacity, even well-designed security frameworks may fail in practice.

Similarly, the strong positive relationship between policy frameworks and cybersecurity readiness ($\beta = 0.58$, $p < 0.05$) reinforces the importance of governance structures in shaping cybersecurity outcomes. This finding is consistent with reports by international bodies such as the International Telecommunication Union (ITU), which emphasize that robust regulatory environments and national cybersecurity strategies are fundamental to strengthening digital resilience [19]. In the context of IoT, where devices and data flows often transcend organizational and national boundaries, well-defined policies are essential for ensuring accountability, standardization, and compliance.

The study also highlights the significant role of technological effectiveness ($\beta = 0.55$, $p < 0.05$), indicating that the deployment of appropriate security technologies contributes substantially to IoT cybersecurity maturity. However, the moderate levels observed in the intensity domain suggest that while technologies may be available, their implementation remains inconsistent. This observation corroborates earlier research, which notes that IoT devices often lack built-in security features due to resource constraints, leading to vulnerabilities that can be exploited by attackers [36]. Therefore, the effectiveness of technological solutions is not solely dependent on their availability but also on their proper integration and management within IoT ecosystems.

Another important finding is that adoption levels of IoT cybersecurity practices are relatively higher than readiness and intensity levels, suggesting a disparity between the willingness to adopt IoT technologies and the capacity to secure them. This phenomenon has been widely documented in the literature, where rapid technological adoption in developing economies often outpaces the development of supporting infrastructure and regulatory frameworks [2,7]. Such imbalances create significant security gaps, exposing systems to potential cyber threats.

Overall, the results validate the conceptual structure of the proposed IoT-CSAM model, demonstrating that IoT cybersecurity is influenced by a combination of human, technological, and institutional factors. This supports the argument that effective cybersecurity assessment frameworks must adopt a holistic and context-aware approach, rather than relying solely on technical metrics.

6 Conclusion and Future Work

6.1 Conclusion

This study set out to develop and validate an integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) tailored to the unique challenges of developing economies. Guided by a Design Science Research approach, the study successfully designed a multidimensional model comprising three core domains: Readiness, Intensity, and Adoption. Empirical evaluation using data from 127 respondents and statistical analysis through SPSS confirmed the robustness and validity of the model.

The findings reveal that IoT cybersecurity maturity is significantly influenced by human resource capacity, policy frameworks, and technological effectiveness. Among these, human capacity emerged as the most critical factor, highlighting the importance of skills development and awareness in enhancing cybersecurity readiness. The study also established that while IoT adoption is increasing, it is not adequately matched by corresponding improvements in cybersecurity readiness and implementation intensity, thereby creating potential vulnerabilities.

Overall, the IoT-CSAM model provides a comprehensive and context-aware framework for assessing IoT cybersecurity maturity. By integrating technical, organizational, and policy dimensions, the model offers

a practical tool for evaluating and improving cybersecurity posture in developing economies. The study contributes to both theory and practice by addressing the limitations of existing models and proposing a scalable approach that can be adapted to different national and organizational contexts.

6.2 Recommendations

Based on the findings of this study, the following recommendations are proposed:

Governments and organizations should invest in cybersecurity education, training programs, and professional development initiatives to build a skilled workforce capable of managing IoT security challenges.

There is a need for the development and enforcement of comprehensive IoT-specific cybersecurity policies and regulations that address emerging threats and ensure compliance across sectors.

Organizations should adopt robust and scalable security technologies tailored to IoT environments, ensuring proper integration, monitoring, and continuous updates to address evolving threats.

Stakeholders should align IoT adoption strategies with cybersecurity preparedness by incorporating security considerations at every stage of technology deployment.

Future research should focus on automating the IoT-CSAM model through the development of software tools and dashboards, enabling real-time assessment and decision-making. Moreover, researchers are encouraged to explore advanced statistical techniques, machine learning approaches, and cross-country comparative studies to refine and extend the model.

Furthermore, the limitation arising from the use of a relatively small dataset, coupled with the lack of real-world case studies, is acknowledged. Future studies should therefore address these gaps by employing larger and more diverse datasets, undertaking external validation procedures, and applying them in practical environments to strengthen their robustness and enhance their real-world relevance.

Acknowledgement: We hereby acknowledge that the paper titled "An Integrated Internet of Things Cybersecurity Assessment Model (IoT-CSAM) for Developing Economies" is our original work and has not been submitted elsewhere for an academic purpose. We confirm that all sources used in this paper have been appropriately cited and acknowledged.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Davis Matovu; data collection: Ali Mwase; analysis and interpretation of results: Ali Mwase, Gilbert Gilibrays Ocen; draft manuscript preparation: Ali Mwase, Davis Matovu, Gilbert Gilibrays Ocen. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated and/or analyzed during the current study are not publicly available due to ethical and confidentiality restrictions associated with the research participants and institutional requirements. However, the data are available from the corresponding author upon reasonable request and subject to approval by the relevant ethics bodies, where applicable.

Ethics Approval: Ethical approval was obtained from the Ugandan Ministry of ICT and National Guidance (Approval No. ADM70/81/88), which was relevant to the study because the research was affiliated with the ICT and cybersecurity domain and involved issues related to information and communication technology. Before data collection, participants were informed about the study and provided written informed consent. Participation was voluntary, with the right to withdraw at any time, while confidentiality, anonymity, and privacy were maintained throughout the study in accordance with established ethical guidelines and institutional research policies.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Transforma Insights. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology (in millions). [cited 2026 Jan 1]. Available from: https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/.
2. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: a survey. J Netw Comput Appl. 2017;88(4):10–28. doi:10.1016/j.jnca.2017.04.002.
3. Symantec. Internet security threat report. 2022 [cited 2025 Jan 1]. Available from: https://docs.broadcom.com/doc/istr-24-2019-en.
4. Ande R, Adebisi B, Hammoudeh M, Saleem J. Internet of Things: evolution and technologies from a security perspective. Sustain Cities Soc. 2020;54(5):101728. doi:10.1016/j.scs.2019.101728.
5. Maddikunta PK, Pham QV, Nguyen DC, Huynh-The T, Aouedi O, Yenduri G, et al. Incentive techniques for the Internet of Things: a survey. J Netw Comput Appl. 2022;206(4):103464. doi:10.1016/j.jnca.2022.103464.
6. Viet NA, Minh LQ, Hau DH, Tuan NN, Quang NN, Chinh ND, et al. Toward cyber-security architecture framework for developing countries: an assessment model. In: International Conference on Advances in Information and Communication Technology. Cham, Switzerland: Springer International Publishing; 2016. p. 652–8.
7. European Union Agency for Cybersecurity ENISA. Baseline security recommendations for IoT in the context of critical information infrastructures. Athens, Greece: European Union Agency for Cybersecurity (ENISA); 2017.
8. Ammar M, Russello G, Crispo B. Internet of Things: a survey on the security of IoT frameworks. J Inf Secur Appl. 2018;38(9):8–27. doi:10.1016/j.jisa.2017.11.002.
9. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw. 2015;76(15):146–64. doi:10.1016/j.comnet.2014.11.008.
10. Friedman RP. Factors shaping policy for cybersecurity resilience in critical infrastructure (CI) organizations: proposing an adaptive cyber resilience policy model (ACRPM) [dissertation]. Lynchburg, VA, USA: Liberty University; 2025.
11. Musa U, Adenomon Monday O, Bassey SI, Aimufua GI. Critical security gaps in IoT ecosystems: a quantitative risk assessment framework. GAS J Eng Technol. 2025;2(8):1–12.
12. Benias N, Markopoulos AP. A review on the readiness level and cyber-security challenges in Industry 4.0. In: Proceedings of the 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM); 2017 Sep 23–25; Kastoria, Greece. p. 1–5.
13. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the Internet of Things: a comprehensive review. Sensors. 2023;23(8):4117. doi:10.3390/s23084117.
14. Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas KN, Nadeau E, et al. Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. [cited 2025 Jan 1]. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf.
15. Hair JF, Black WC, Babin BJ, Anderson RE. Multivariate data analysis. 8th ed. Andover, UK: Cengage Learning EMEA; 2019.
16. Laghari AA, Khan AA, Ksibi A, Hajjej F, Kryvinska N, Almadhor A, et al. A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. Sci Rep. 2025;15(1):26843. doi:10.1038/s41598-025-11738-9.
17. Clark MJ, Alper AG, Galicia R. Digital public infrastructure and development: a world bank group approach. Washington, DC, USA: World Bank; 2025.
18. Falowo O, Falowo S. Low internet penetration in Sub-Saharan Africa and the role of LEO satellites in addressing the issue. Telecom. 2026;7(1):7.
19. International Telecommunication Union (ITU). Global connectivity report 2025. [cited 2025 Jan 1]. Available from: https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2025.
20. Moloja D. Enhancing cybersecurity resilience: addressing emerging technology challenges in developing countries using Activity Theory. In: Proceedings of the 2025 Cybersecurity4D (C4D); 2025 Aug 17–22; Gqeberha, South Africa. p. 1–7.

21. Hukuk Z. ENISA publishes guidelines on securing the IoT. 2020 [cited 2025 Jan 1]. Available from: https://www.zumbul.av.tr/en/data-privacy/enisa-publishes-guidelines-on-securing-iot-supply-chain.
22. U.S. Department of Energy. Cybersecurity capability maturity model (C2M2). [cited 2025 Jan 1]. Available from: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
23. George AS, Baskar T, Srikaanth PB. Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partn Univers Int Innov J. 2024;2(1):51–75.
24. Kebande VR, Mudau PP, Ikuesan RA, Venter HS, Choo KKR. Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Sci Int Rep. 2020;2:100117. doi:10.1016/j.fsir.2020.100117.
25. Frye JN, Veitch CK, Mateski ME, Michalski JT, Harris JM, Trevino CM, et al. Cyber threat metrics. Albuquerque, NM, USA: Sandia National Laboratories; 2012. Report No.: SAND2012-2427.
26. Conklin WA. Computer security behaviors of home PC users: a diffusion of innovation approach. San Antonio, TX, USA: The University of Texas at San Antonio; 2006.
27. Tripathi S. System dynamics perspective for adoption of Internet of Things: a conceptual framework. In: Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT); 2019 Jul 6–8; Kanpur, India. p. 1–10.
28. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection—Information security management systems—Requirements. Geneva, Switzerland: ISO; 2022.
29. National Institute of Standards and Technology. The CSF 1.1 five functions. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2018.
30. ISACA. COBIT 2019 framework: introduction and methodology. Schaumburg, IL, USA: ISACA; 2018.
31. Committee of Sponsoring Organizations of the Treadway Commission COSO. Enterprise risk management framework: integrating with strategy and performance. 2017 [cited 2025 Jan 1]. Available from: https://www.coso.org/guidance-erm.
32. Authority CC. Process framework for cybersecurity [Internet]. [cited 2026 Sep 29]. Available from: https://cloudcomplianceauthority.com/process-framework-for-cybersecurity/.
33. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. J Manag Inf Syst. 2007;24(3):45–77. doi:10.2753/MIS0742-1222240302.
34. Krejcie RV, Morgan DW. Determining sample size for research activities. Educ Psychol Meas. 1970;30(3):607–10. doi:10.1177/001316447003000308.
35. Yousuf MI. Using experts' opinions through the Delphi technique. Pract Assess Res Eval. 2007;12(1):4.
36. Aziz Al Kabir M, Elmedany W, Sharif MS. Securing IoT devices against emerging security threats: challenges and mitigation techniques. J Cyber Secur Technol. 2023;7(4):199–223. doi:10.1080/23742917.2023.2228053.