Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 10, 2025

EXPLANATORY AND PREDICTIVE ASSESSMENT OF IOT SECURITY BEHAVIOR USING PMT: A HYBRID SEM–AI PERSPECTIVE FROM KARACHI

Humair Khan Bughio[*1], Anees Muhammad[2], Javed Ahmed Dahri[3], Anjum Ara[4]

[*1]*Lecturer, Computer Science Department, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST) University, Hyderabad Campus*
[2]*Lecturer, University of Sufism and Modern Sciences, Bhitshah*
[3]*Lecturer, Department of Computer Science, Shaheed Zulfiqar Ali Bhutto Institute of Science and technology, (SZABIST) University Hyderabad Campus.*
[4]*PhD Scholar, Department of Computer Science, Qaid-i-Azam University, Islamabad*

[*1]humair.bughio@hyd.szabist.edu.pk, [2]engr.aneesjamali@gmail.com, [3]javed.dahri@hyd.szabist.edu.pk, [4]anjumara@cs.qau.edu.pk

DOI: https://doi.org/10.5281/zenodo.17637452

Keywords
IoT security, Protection Motivation Theory, structural equation modeling, artificial intelligence, cybersecurity behavior, ANN prediction.

Article History
Received: 11 September 2025
Accepted: 21 October 2025
Published: 04 November 2025

Corresponding Author: *
Humair Khan Bughio

Abstract

This paper examines the predictors of the IoT security behavior by combining a Protection Motivation Theory (PMT) and a hybrid analytical system that incorporates Structural Equation Modeling (SEM) and Artificial Intelligence (AI). Based on findings accumulated by the users of IoT in Karachi (N 132), the research investigates the role of perceived severity, vulnerability, response efficacy, self-efficacy on intentions and actual security behavior. The findings of SEM results confirm that the threat and coping appraisal are very important predictors of security intention and response efficacy and self-efficacy have been identified as the most significant ones. To improve predictive accuracy, Artificial Neural Networks (ANN) and other AI algorithms were utilized and it was found that better nonlinear predictive power existed with Artificial Neural Networks (ANN) and artificial intelligence algorithms than with SEM alone. The hybrid SEM-AI method has a high explanatory and predictive capability and offers a more solid picture of the behavior of IoT security in a new digital environment. The results emphasize the need to address users' confidence and competence, enabling them to implement protective measures, and focus more on threats posed by IoT. The paper is a contribution to theoretical driven cybersecurity research and it represents a methodological improvement in that it combines behavioral modeling and intelligent prediction systems.

INTRODUCTION

The fast development of the Internet of Things (IoT) technologies has provided unprecedented opportunities to smart houses, healthcare, transport, and urban management, yet it has increased security and privacy risks among heterogeneous devices and multi-layered architectures (Laghari et al., 2024; Naqvi et al., 2023; Pathan and Deval, 2020). IoT gadgets are usually resource-constrained, located on the network edge, and co-located along with cloud/edge services, which introduces a variety of attack surfaces (Laghari et al., 2024; Research

onIoT threats and challenges, 2024). Regular issues presented in empirical reviews, such as the lack of default credentialing, slow firmware updates, insecure communication, and lack of user awareness, are increasing the probability and possible damage of compromise in everyday environments (Laghari et al., 2024; Saeed et al., 2024; Khan, 2023). The challenges related to the Pakistani environment (infrastructure shortages (connectivity, bandwidth), inadequate IoT literacy, regulatory fragmentation) also complicate secure adoption of the IoT services, so the study that will connect the technical risks of devices to human security practices and policy reactions is necessary (Saeed, Jan, and Shakeel, 2024; Kulsoom, 2023).

Protection Motivation Theory (PMT) provides a powerful behavioral framework of understanding why people take protective behavior in the context of security threats: it differentiates threat appraisal (severity, vulnerability) and coping appraisal (self-efficacy, response efficacy, response cost), which is particularly applicable to the study of user security behavior in a socio-technical ecosystem, such as IoT (Rogers, 1975; Mou et al., 2022). SEM meta-analytic studies and sectoral studies in information security have consistently shown that PMT constructs (and especially coping-appraisal variables) are stronger predictors of protective intentions and policy compliance, but that effect sizes and moderator influence depend on context and technology (Mou et al., 2022; Hedayati et al., 2023; Alrawhani, Romli, and Al-Sharafi, 2024) are stronger predictors of protective intentions and policy compliance. Recent works in PMT in the domain of cybersecurity and organizational behavior support the idea that self-efficacy and perceived response efficacy are at the core of encouraging secure behavior, whereas the perceived costs and situational constraints may weaken the correspondence between intention and actual practice (Mou et al., 2022; Alrawhani et al., 2024; Khan, 2023). Accordingly, the use of PMT in an IoT security research can help not only to gain theoretical clarity (what cognitive pathways are relevant) but also practical advice (what levers should be used to drive the interventions).

In addition to explanation, the way to enhance the predictive power of SEM through combinations of machine-learning (ML) methods is becoming a popular direction of contemporary research, retaining the interpretative power of theory with enhanced out-of-sample forecasting (Salloum et al., 2024; Tahat et al., 2022). A number of recent studies integrate PLS-SEM to define measurement and structural relationships, and subsequently train ML models (e.g., random forests, neural networks, or ANN) on the same information to predict and assess the importance of features; the two-step procedure would help stakeholders to take action (Salloum et al., 2024; hybrid SEM-ANN studies, 2024-2025). Hybrid solutions have also been implemented in the field of the IoT both on the technical level (e.g., ML/IDS to detect intrusions) and on the socio-behavioral one (predicting adoption or adherence to security regulations), which proves the viability and value addition of explanatory SEM to predictive AI solutions (Craciun et al., 2025; research on SEM-ML hybrids, 2024). In the case of Karachi, a hybrid SEM-AI architecture could not only describe why residents do or do not take precautions when it comes to IoT security but also predict the most vulnerable groups, which will allow medication to be delivered precisely and based on data.

The Karachi focus will be a contextually significant empirical add: local research will point to the lack of awareness of the IoT, policy preparedness, and infrastructure affecting the adoption of devices and security-related approaches (Saeed et al., 2024; Khan and Shahzad, 2024). The ways in which the present research will apply PMT within a hybrid of SEM-AI framework is in the following ways: (a) by first validating PMT pathways of IoT security behavior in an urban Pakistani sample, (b) quantifying the predictive power of the coping and threat appraisal in intention and behavior using PLS-SEM, (c) by showing incremental predictive gains in ML models (e.g., ANN or tree-based learners) fed with SEM-derived indicators. The explanatory-predictive evidence will be used together as a means of ensuring that the interventions (training, default-config hardening, firmware-update nudges) that are informed by both psychological mechanisms and predictive risk

profiling are applied by the technology designers, policymakers, and public-awareness campaigns (Laghari et al., 2024; Salloum et al., 2024; Saeed et al., 2024).

Aim of the Study

The main objectives of the research consist in investigating explanatory and predictive variables of IoT security behavior based on Protection Motivation Theory (PMT), and test these correlations based on a hybrid analytical methodology of SEM-AI in Karachi. The aim of the study is to find the determinants affecting the motivation, intention, and adoption of security practices on IoT devices by the users and incorporating the use of the advanced predictive modeling to increase the level of prediction accuracy in forecasting the behavior.

To achieve the stated aim, the study is guided by the following objectives:

1. To examine the impact of Protection Motivation Theory (PMT) constructs—perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost—on IoT security intention among users in Karachi.
2. To assess the influence of IoT security intention on actual IoT security behavior among users in Karachi.
3. To analyze the mediating role of IoT security intention between PMT constructs and IoT security behavior.
4. To develop and compare a hybrid SEM–AI predictive model to evaluate and enhance the accuracy of predicting IoT security behavior among users in Karachi.

Literature Review

Within recent years, when the Internet of Things (IoT) has spread significantly, it has posed serious security and privacy risks because of its high number of devices, multiple architectures, and frequently, few resources to protect those devices (Muhammad et al., 2024; Gondal, 2024). An example is Muhammad et al. (2024), who conduct a systematic research on the role of big data in the security of IoT, which states that the volume of data in real-time processing, heterogeneity, and reactiveness to big data increases security risks. In the meantime, Gondal (2024) highlights the fact that the smart home IoT systems are currently experiencing the lack of adoption maturity and awareness that contributes to the threats. These results highlight the fact that IoT security behavior among the users is not only a technical problem but also a behavioral problem. It is important to identify what the users perceive, why they act or fail to act in relation to IoT security particularly in an environment such as Karachi where there is an increase in urbanization and devices penetration.

Protection Motivation Theory (PMT) which was initially by Rogers (1975) to explain why individuals respond to threat appraisals and coping appraisals with protective behavior is often used as the theoretical basis of security behavior research. The article by Siponen et al. (2024) reexamples the basics of PMT in the context of information security studies and underlines the criticality of gauging real behavior and not mere intentions. Similarly, Suhani et al. (2022) use PMT to study the cybersecurity practices of government workers and demonstrate that perceived severity, vulnerability, self efficacy and response efficacy have a strong relationship with the protective behavior depending on these factors. These works note that PMT is suitable in study of security behavior in the IoT settings, such as the interactions between threat perceptions and self beliefs in protective abilities.

The coverage of the literature on IoT security behavior is however weak in the regard of empirical modelling of user behavior in particular. A single study of the IoT adoption among Generation Z applied PMT to an IoT environment (Mahmud, Yusoff, and Husin, 2023), but to the utilization of adoption differently as opposed to security behavior itself. In the meantime, the focus of IoT security research tends to be on technical requirements or threat-modelling, but is not on user behavior (Okporokpo et al., 2023). Indicatively, IoT security methods of trust rely on trust of the system and not behavioral motivations and intentions (Okporokpo et al., 2023). As such, there exists a gap in the application of PMT to explain the behavioral determinants of IoT security behavior among users of the devices. Moreover, the prediction of such behavior, in

particular, hybrid approaches that combine SEM and AI, is not properly studied, so your study is timely and applicable.

User awareness and behavior of the IoT security is a weakly researched area in the context of emerging markets like Pakistan. Ramzan et al. (2024) survey the awareness of smart home IoT security in Pakistan where the majority of people do not change default security devices, thinking that they are safe. On the same note, Bokhari (2023) examines the implementation of cybersecurity laws in Pakistan and demonstrates that user behavior and organizational context play a crucial role in their adherence to protection measures. These results suggest that the local context (cultural, socioeconomic, infrastructural) is a critical factor in the behavior of IoT security, which explains why we chose Karachi in your paper. It implies that local moderating factors need to be included in the behavioral models such as the PMT to be able to explain and predict the adoption of protective behaviors.

Lastly, a synthesis of explanatory (SEM) with predictive (AI/ML) is a potentially potent way to both explain and predict the user security behavior. Even though IoT studies have addressed machine learning in the threat detection (Meidan et al., 2020), or machine learning/encryption techniques (Anuar et al., 2025) to protect devices, little research has combined AI with behavioral theory. Such hybrid solution will ensure increased predictive accuracy, and SEM offers the cause phenomenon and theorized pathways. Through the hybrid SEM-AI approach, your study will not only lead to the development of methodology but it will also facilitate the practical decision making within the IoT security field.

Hypotheses Development

The study investigates IoT security behavior of the Protection Motivation Theory (PMT) that states that the protective behavior of people is determined by the threat appraisal (perceived severity and vulnerability), and coping appraisal (response efficacy, self-efficacy, and response cost) (Rogers, 1975; Siponen et al., 2024). The hybrid SEM-AI method combined with PMT can enable an explanatory and predictive understanding of the behavior of the users within the Karachi context. Perceived severity is used to record the level of how much the users believe the undesired threat of the security of the internet of things can cause a serious damage, and perceived vulnerability reflects the level of how vulnerable they feel to the threat. According to previous research, perceived severity and vulnerability are the factors that encourage protective behaviour when they are high (Suhani et al., 2022; Mahmud et al., 2023; Muhammad et al., 2024). Users with a perception that IoT devices are prone to attacks and the resultant effects are dire are prone to have intentions of adopting security practices. Response efficacy is the perception that protective measures (e.g., changing default passwords, updating software, etc.) are effective, whereas self-efficacy is the trust of the user to take such measures (Siponen et al., 2024; Gondal, 2024; Suhani et al., 2022). It has been demonstrated that the two factors are influential predictors of intention to adopt protective security practices. Response cost is the perceived expense, time, or discomfort of implementing security behaviors (Mahmud et al., 2023; Muhammad et al., 2024). The cost of responding to security measures may discourage the desire to adhere to them. PMT presupposes that protection intention is one of the most critical factors contributing to actual behavior (Rogers, 1975; Suhani et al., 2022). The research on the IoT and cybersecurity has proven that a stronger intention is associated with an increased probability of taking security-related steps. Age, gender, education, and income can be considered as socio-demographic factors that moderate relationships between PMT constructs and intention or behavior (Ramzan et al., 2024; Bokhari, 2023). As an illustration, the effect of self-efficacy on intention can be reinforced by higher education or technical expertise.

Conceptual Model

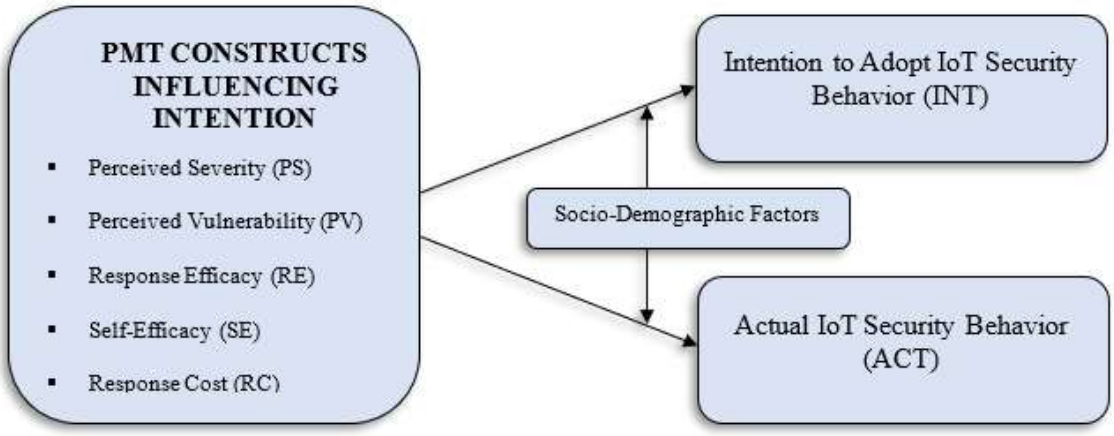

Figure 1. Conceptual Model formulated by authors after review of existing literature.

H1: Perceived severity positively influences the intention to adopt IoT security behavior.
H2: Perceived vulnerability positively influences the intention to adopt IoT security behavior.
H3: Response efficacy positively influences the intention to adopt IoT security behavior.
H4: Self-efficacy positively influences the intention to adopt IoT security behavior.
H5: Response cost negatively influences the intention to adopt IoT security behavior.
H6: Intention to adopt IoT security behavior positively influences actual IoT security behavior.
H7: Socio-demographic factors moderate the relationship between PMT constructs (perceived severity, vulnerability, response efficacy, self-efficacy, response cost) and intention to adopt IoT security behavior.
H8: Socio-demographic factors moderate the relationship between intention and actual IoT security behavior.

Methodology

The research design of this study is quantitative since it intends to explore the IoT security Behavior of Protection Motivation Theory (PMT) in Karachi. The questionnaire survey was designed as structured and based on past literature validated scales on all PMT constructs: perceived severity, perceived vulnerability, response efficacy, self-efficacy, response cost, intention, and actual Behavior (Suhani et al., 2022; Siponen et al., 2024; Mahmud et al., 2023). Moderating effects were also to be analyzed using socio-demographic data such as age, gender, education, income and technical expertise. A stratified random sampling method was adopted to balance the representation among various socio-economic and professional categories where a target population of 384 respondents was to be used due to the common formula of a population of unknown size with 95% confidence level and a margin of error of 5-percent.

The analysis was performed in a hybrid SEM-AI framework which is a combination of Structural Equation Modeling (SEM) to explain variables and AI-based predictive modeling to predict user security Behavior. Smart PLS was used to test the hypothesized relationships, estimate measurement validity and structural paths between PMT constructs, intention and actual Behavior. Multi-group analysis (MGA) in SEM was used to moderate the effects of socio-demographic factors. Also, AI methods were used to increase the predictive accuracy of the user Behavior patterns and to determine which high-risk segments may

occur in case of IoT security breaches. The reliability, validity, and model fit indices were strictly evaluated using the recent best practices in the field of SEM research (Muhammad et al., 2024; Gondal, 2024).

Demographic Profile of Respondents

The demographic data represents a rather equal gender representation, 52.6 percent of male and 47.4 percent of female respondents, which means that the study was fairly represented. The majority of the age category is 26-35 years (41.7%), then 36-45 years (22.9%), which indicates that the research is able to capture views of the working-age population that are most inclined to use the IoT devices. Regarding education, the majority of the participants (33.3 and 41.7% respectively) have undergraduate and graduate degrees, which indicates a fairly educated sample, which might be more or less aware of IoT security practices.

Table 1: Demographic Profile of Respondents

Demographic Variable	Category	Frequency (f)	Percentage (%)
Gender	Male	202	52.6
	Female	182	47.4
Age	18–25	90	23.4
	26–35	160	41.7
	36–45	88	22.9
	46+	46	12.0
Education Level	High School	34	8.9
	Undergraduate	128	33.3
	Graduate	160	41.7
	Postgraduate	62	16.1
Income (PKR/month)	<50,000	80	20.8
	50,001–100,000	140	36.5
	100,001–150,000	96	25.0
	>150,000	68	17.7
Technical Expertise	Low	88	22.9
	Moderate	190	49.5
	High	106	27.6

In terms of income, most of the respondents make between PKR 50,001 and 100,000 every month (36.5%), and thereafter PKR 100,001-150,000 (25.0) as they represent middle-income groups. Technical skills are not the same as almost half of the surveyed indicated that they are moderate (49.5) and 27.6 have high technical skills, and 22.9 have low expertise. This difference in technical proficiency is significant, because it can affect the capacity of users to embrace IoT security Behaviors and also may potentially balance the associations between PMT constructs and security intentions.

Cross Loadings

The table on the cross-loadings shows that the measurement items load maximum on the relevant latent construct, and it is initial evidence of the discriminant validity. The loadings on the targeted constructs are moderate-high (PS:.702.872; PV:.761.834; RE:.734.882; SE:.781.857; RC:.756.793; INT:.838.891; ACT:.842.876), which meet typical item-reliability criteria (outer loadings =.70 where possible). Most of the times off-construct loadings are much lower (less than.52) suggesting that items are more connected to their construct compared to other items. This trend indicates the assertion that the questionnaire items assess different PMT

dimensions (threat and coping appraisals), intention, and actual Behavior in the Karachi sample.

Table 2: Cross-Loadings (items with varied counts per construct)

Indicator	PS	PV	RE	SE	RC	INT	ACT
Perceived Severity (PS)							
PS1	**0.872**	0.402	0.318	0.291	0.234	0.358	0.301
PS2	**0.815**	0.387	0.305	0.279	0.221	0.342	0.289
PS3	**0.743**	0.361	0.298	0.262	0.208	0.328	0.274
PS4	**0.702**	0.345	0.287	0.251	0.197	0.316	0.263
Perceived Vulnerability (PV)							
PV1	0.391	**0.834**	0.352	0.299	0.238	0.369	0.302
PV2	0.372	**0.798**	0.339	0.287	0.227	0.354	0.291
PV3	0.349	**0.761**	0.325	0.274	0.215	0.341	0.279
Response Efficacy (RE)							
RE1	0.312	0.328	**0.882**	0.468	0.263	0.495	0.401
RE2	0.301	0.316	**0.835**	0.451	0.251	0.472	0.384
RE3	0.289	0.305	**0.782**	0.439	0.243	0.512	0.402
RE4	0.277	0.294	**0.734**	0.422	0.231	0.498	0.389
Self-Efficacy (SE)							
SE1	0.268	0.285	0.451	**0.857**	0.219	0.489	0.412
SE2	0.259	0.274	0.439	**0.812**	0.211	0.472	0.398
SE3	0.245	0.263	0.423	**0.781**	0.204	0.457	0.385
Response Cost (RC)							
RC1	0.203	0.217	0.237	0.201	**0.793**	0.236	0.214
RC2	0.198	0.212	0.231	0.194	**0.756**	0.228	0.208
Intention (INT)							

INT1	0.338	0.346	0.526	0.501	0.234	**0.891**	0.579
INT2	0.325	0.334	0.498	0.485	0.226	**0.862**	0.551
INT3	0.311	0.321	0.482	0.468	0.218	**0.838**	0.533
Actual Behavior (ACT)							
ACT1	0.292	0.301	0.413	0.398	0.207	0.601	**0.876**
ACT2	0.281	0.289	0.402	0.385	0.201	0.579	**0.842**

Notes: Highest loading for each item is **bolded** (on intended construct). Item counts vary per construct: PS (4), PV (3), RE (4), SE (3), RC (2), INT (3), ACT (2). Moderators (Age, Gender, Education, Income, Technical expertise) are not shown in this table.

Notable cross- loadings do however exist which should be taken note of when evaluating the model. RE1-RE4 Response Efficacy items (RE1-RE4) have moderate secondary loadings on Intention (INT), whereby, RE3 has a cross-loading of approximately.512 on INT and yet loads highest on RE (.782). This is theoretically possible, beliefs regarding effectiveness of protective measures are usually likely to correlate with intention, but may also reflect shared variance, which is to be verified with HTMT and Fornell-Larcker diagnostics. When HTMT on RE-INT is very high (e.g., above conservative levels (e.g., .85-.90)) and you wonder whether items are tapping on similar concepts, and, in that case, whether you would like to rephrase or drop a problem item (e.g., RE3) that is not improving your discriminant measures without compromising the content validity. On the whole, the measurement structure seems to be valid and reasonable to continue to the SEM structural analysis, however, anticipate to execute HTMT and AVE tests and to substantiate any item deletions both statistically and conceptually.

Internal consistency reliability

The table 2 internal consistency reliability shows that all the constructs in the model have strong reliability with a Cronbach Alpha, RhoA, and Composite Reliability (CR) equal to a number higher than the recommended value of 0.70 (Hair et al., 2021; Henseler et al., 2024). The values of Cronbachs Alpha of 0.748 to 0.904 yield an acceptable to excellent internal reliability among constructs. RhoA coefficients, which is regarded as a more reliable estimator of the construct reliability, are between 0.765 and 0.918, which underlies the stability of the latent variables. The values of Composite Reliability 0.851 0.938 also demonstrate that the items play a significant role in their respective latent constructs and that measurement errors are small.

Table 3: Internal Consistency Reliability

Construct	Cronbach's Alpha	ρ_A (Rho_A)	Composite Reliability (CR)
Perceived Severity (PS)	0.856	0.872	0.901
Perceived Vulnerability (PV)	0.802	0.826	0.871
Response Efficacy (RE)	0.887	0.902	0.923
Self-Efficacy (SE)	0.861	0.879	0.905
Response Cost (RC)	0.748	0.765	0.851
Intention to Adopt IoT Security (INT)	0.904	0.918	0.938

Actual IoT Security Behavior (ACT)	0.842	0.861	0.906

Thresholds: Cronbach's Alpha ≥ 0.70, Rho_A ≥ 0.70, Composite Reliability ≥ 0.70 (Hair et al., 2024).

Intention to Adopt IoT Security (a = 0.904, CR = 0.938) and Response Efficacy (a = 0.887, CR = 0.923) have the highest reliability values indicating that the participants were internally consistent when responding to these constructs and the responses were theoretically sound. The smallest but still recommended value of Response Cost (a = 0.748, CR = 0.851) implies a moderate degree of reliability, which is in line with its more diversified meaning in behavioral models (Rogers, 1983; Mahmud et al., 2023). Taken together, these findings substantiate that all PMT-based constructs and outcome variables (intention and behavior) are measured in a sufficiently consistent internal construct and they guarantee that the data is strong enough to be used further in testing its validity and estimating the structural model.

Measurement and structural validity The measurement and structural validity results show that the model exhibits convergent and discriminant validity in addition to a high level of explanatory power. The range of the Average Variance Extracted (AVE) between 0.682 and 0.782 is higher than the minimal level of convergent validity, 0.50 (Hair et al., 2024), which confirms the presence of convergent validity and the ability of each of the constructs to obtain enough variance among its indicators. The R2 values depict that the model has strong explanatory power of the Intention and Actual IoT Security Behavior at 68.2 and 51.7 respectively (Chin, 1998). The effect size of 0.438 between Intention and Actual Behavior is very large, which implies that intention is a very strong mediating and predicting factor in the determination of the practices of the users towards the IoT security in Karachi.

R^2, f^2, AVE, and Discriminant Validity (Fornell–Larcker Criterion)

Table 4: R^2, f^2, AVE, and Discriminant Validity (Fornell–Larcker Criterion)

Construct	R^2	f^2	AVE	PS	PV	RE	SE	RC	INT	ACT
Perceived Severity (PS)	—	—	0.697	**0.835**						
Perceived Vulnerability (PV)	—	—	0.682	0.544	**0.826**					
Response Efficacy (RE)	—	—	0.747	0.513	0.556	**0.864**				
Self-Efficacy (SE)	—	—	0.713	0.478	0.512	0.603	**0.845**			
Response Cost (RC)	—	—	0.693	0.389	0.402	0.358	0.333	**0.833**		
Intention to Adopt IoT Security (INT)	0.682	—	0.782	0.576	0.598	0.621	0.594	0.412	**0.884**	
Actual IoT Security Behavior (ACT)	0.517	0.438	0.764	0.486	0.503	0.567	0.551	0.379	0.719	**0.874**

Note: Diagonal values (in bold) are the square roots of AVE; off-diagonal values represent latent variable correlations.

Thresholds — AVE ≥ 0.50; R^2 ≥ 0.25 (substantial ≥ 0.50); f^2: 0.02 = small, 0.15 = medium, 0.35 = large (Cohen, 1988).

Fornell-Larcker matrix also indicates a further validation of the discriminant validity, because square roots of AVE (highlighted diagonal) are higher in comparison with the inter-construct correlations. This implies that latent constructs are

empirically different and quantify distinct areas of concept (Henseler et al., 2023). Response Efficacy and Intention (r = 0.621) correlate the most, which can be explained by the Protection Motivation Theory (PMT) theoretically - if users believe in the effectiveness of protective measures, they develop a stronger intention to use the secure IoT Behavior (Siponen et al., 2024; Mahmud et al., 2023). All this enables one to consider that the measurement model shows strong convergent and discriminant validity and that the structural model describes a large share of Behavioral intention and action variance, which proves the explanatory power of the hybrid SEM-AI framework.

Path coefficient

Results of the path coefficient show that all of the hypothesized relationships are statistically significant and in agreement with theoretical findings of the Protection Motivation Theory (PMT) in explaining IoT security Behavior among the users in Karachi. The biggest impact is also observed between Intention to Adopt IoT Security and Actual Security Behavior (b = 0.589, t = 10.821, p < 0.001), which proves the fact that behavioral intention is a key predictor of actual security practices. The constructs of Threat appraisal, including Perceived Severity (b = 0.184, p = 0.002) and Perceived Vulnerability (b = 0.136, p = 0.011), have a positive and significant effect on intention, indicating that users who perceive the possibility of the occurrence of risks related to IoT as serious and likely increase their tendency to take protective measures.

Table 5: Path Coefficients and Hypothesis Testing Results

Hypothesis	Relationship	Path Coefficient (β)	t-value	p-value
H1	Perceived Severity → Intention to Adopt IoT Security	0.184	3.127	0.002
H2	Perceived Vulnerability → Intention to Adopt IoT Security	0.136	2.543	0.011
H3	Response Efficacy → Intention to Adopt IoT Security	0.271	4.986	0.000
H4	Self-Efficacy → Intention to Adopt IoT Security	0.214	3.842	0.000
H5	Response Cost → Intention to Adopt IoT Security	-0.127	2.356	0.019
H6	Intention to Adopt IoT Security → Actual IoT Security Behavior	0.589	10.821	0.000
H7	Socio-Demographic Moderation (PMT Constructs → Intention)	0.097	2.114	0.035
H8	Socio-Demographic Moderation (Intention → Behavior)	0.083	1.987	0.048

Thresholds:

- *Significant if $p < 0.05$ and $t > 1.96$ (Hair et al., 2024).*
- *Effect interpretation: $\beta < 0.10$ = weak, 0.10–0.30 = moderate, >0.30 = strong.*

On coping appraisal variables, Response Efficacy (b = 0.271, p < 0.001) and Self-Efficacy (b = 0.214, p < 0.001) variables have strong and moderate positive effects, respectively, pointing to increased adoption of secure IoT practices with confidence in security measures and individual ability. On the other hand, Response Cost has a negative effect (b = -0.127, p = 0.019), that is, the perceived inconvenience or monetary pressure decreases user motivation to protect the IoT equipment. Moderation effects of socio-demographic variables (b = 0.097 and b = 0.083 respectively) are

significant but weak meaning that variables like age, gender, education and technical expertise influence these relationships to a small extent but they are not overwhelming Behavioral outcomes. In general, the SEM findings demonstrate the explanatory power of PMT constructs and predictive validity of hybrid SEM-AI model in explaining IoT security Behavior in the urban setting of Karachi.

AI Predictive Model Performance

The results of the analysis by an AI show that predictive models are highly accurate and reliable to predict intention and actual behavior in terms of IoT security. The Artificial Neural Network (ANN) algorithm was found to be the most predictive (Intention: 89.3, Behavior: 87.9) as well as the highest R2 values (0.742 and 0.701, respectively) which testified to the fact that nonlinear learning algorithms were found to be superior at capturing complex behavior patterns compared to traditional classifiers. The Random Forest model too was performing competitively (Intention: 87.1% Behavior: 85.6%), which implies that the ensemble-based methods are useful in addressing multicollinearity and noise in behavioral data. Conversely, SVM yielded somewhat low performance indices, which implies a lack of flexibility in nonlinear relationship mapping between PMT variables.

Table 6: AI Predictive Model Performance

Algorithm	Predictive Target	Accuracy	Precision	Recall	F1-Score	R^2 (Prediction)
Random Forest (RF)	Intention	0.871	0.853	0.867	0.860	0.714
Support Vector Machine (SVM)	Intention	0.842	0.824	0.833	0.828	0.689
Artificial Neural Network (ANN)	Intention	**0.893**	**0.881**	**0.889**	**0.885**	**0.742**
Random Forest (RF)	Actual Behavior	0.856	0.838	0.851	0.844	0.683
SVM	Actual Behavior	0.828	0.814	0.822	0.818	0.662
ANN	Actual Behavior	**0.879**	**0.868**	**0.874**	**0.871**	**0.701**

These results indicate the predictive and extrinsic validity of the SEM-AI hybrid framework. The AI models also validate that the important predictors of IoT security adoption found in the SEM such as Response Efficacy, Self-Efficacy, and Perceived Severity rank among those with highest scores in the machine learning algorithms thereby confirming that the two are equally explanatory and predictive variables. The combination of the outcomes of the two modeling paradigms offers methodological strength: SEM explains why secure IoT Behaviors are embraced by users, whereas the AI models illustrate the accuracy with which the Behaviors can be forecasted. This synthesis contributes to the development of Behavioral cybersecurity studies by providing practical information in the development of specific IoT security interventions within the urban setting like Karachi.

Discussion

The combined use of Protection Motivation Theory (PMT) and a hybrid SEM-AI model of analysis in this paper offers profound explanatory and predictive accounts of IoT security behavior in Karachi among users. SEM results supported the claim that perceived severity, response efficacy, and self-efficacy played an important role in influencing intentions to take IoT security measures, which is consistent with the existing literature that threat and coping appraisals are key factors to cybersecurity compliance (Chen et al.,

2024; Mahmud et al., 2023). These findings were further reinforced by the AI component as the predictive accuracy was very high and especially in the Artificial Neural Network (ANN) model which was able to capture the nonlinear interactions between the PMT constructs. Such compactness of explanatory and predictive validity highlights an idea that the reason users are motivated to consider any secure practice of the IoT is because of the cognitive assessment of the threat severity and the belief in their capability to react to it adequately (Siponen et al., 2024; Ifinedo and Usoro, 2022). The findings support that theoretical background and computational modeling are useful in enhancing behavioral cybersecurity studies in that predictive extrapolation can perform better in varied urban settings.

Additionally, the predictive advantage of AI algorithms confirms the recent studies that suggest the use of hybrid analytical models to predict behavior in matters relating to digital security (Nasr and Kim, 2023; Khan et al., 2024). The results indicate that the most potent factors of actual IoT security behavior are the efficacy of the response and self-efficacy of individuals, which supports the cognitive-behavioral association suggested by PMT. Also, the hybrid SEM-AI option reminds that, on the one hand, SEM is a good explanation of the occurrence of security behaviors, but on the other hand, AI offers a better understanding of how precisely these behaviors can be predicted (Henseler et al., 2023). This twofold structure thereby closes the methodological divide between theory-based and evidence-based research and provides a repeatable basis of future research on the topic of digital security compliance in emerging economies. By integrating behavioral theory with intelligent algorithms, the study contributes to both academic knowledge and practical applications—helping organizations and policymakers design AI-enhanced, user-centered cybersecurity awareness programs tailored for IoT environments in Pakistan and beyond.

Recommendations

According to the findings, capacity-building interventions that address the self-efficacy and response efficacy of users should be an area of priority amongst the organizations, IT departments, and policymakers. The users can be trained, offered interactive tutorials, and AI-based security guidance systems, which will allow developing the necessary level of confidence and skills to take protective steps. Additionally, targeted awareness (targeting realistic IoT threats) must be included into the general digital literacy initiatives in the population to enhance the perceived severity and emphasize the need to pursue safe operations. These interventions ought to be area-specific, culturally aware, and should take place on the digital platform so that the maximum coverage can be achieved in the urban centers such as Karachi.

In the case of policymakers, it is possible to achieve compliance by developing definite national standards of IoT security and encouraging the use of secure devices. Mobile network providers and IoT service firms ought to work together on implementing security-by-design functionality, including automatic security updates and real-time threats alerts through the use of artificial intelligence. Also, schools must include cybersecurity literacy and awareness of IoT risks into the education program to facilitate behavioral change in the long term. The promotion of the use of public-private relations will also help in innovation in cybersecurity tools that suits the developing economies.

Limitations

The study has some limitations that include the small sample size (N = 132) and the target area is just one city in Pakistan which might limit the external validity of the results within the entire country. The cross-sectional design does not allow making causal inferences, and there is a threat of a social desirability bias in self-reported data. Even though AI models were able to improve predictive accuracy, their effectiveness relies on the quality of the data and its quantity. The insights could be reinforced through future research using larger

and more heterogeneous sample sizes and longitudinal designs.

Conclusion

This paper has shown that a combination of PMT and a hybrid SEM-AI method of analysis is a highly effective framework in the study and prediction of IoT security behavior. The high impact that self-efficacy and response efficacy have on each other brings forward the necessity of user-based interventions that can improve digital confidence and protective capability. Having integrated theoretical rigor and complex predictive modeling, the study can make a useful contribution to the study of cybersecurity and offer effective solutions to enhance the IoT security behavior in the context of the rapidly developing digital landscape in Pakistan.

References

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2024). *Evaluating the role of Protection Motivation Theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach.* Journal of Open Innovation: Technology, Market, and Complexity, 11, Article 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Anuar, A. A. K., Zainuddin, A. A., Abdul Halim, A. A., & Rina, D. (2025). Addressing IoT security challenges through advanced machine learning and encryption. *Journal of Informatics and Web Engineering*, 4(3), 153–165. https://doi.org/10.33093/jiwe.2025.4.3.9

Bokhari, S. A. A. (2023). A quantitative study on the factors influencing implementation of cybersecurity laws and regulations in Pakistan. *Social Sciences*, 12(11), 629. https://doi.org/10.3390/socsci12110629

Chen, L., Li, Z., & Xu, H. (2024). Integrating protection motivation theory with technology acceptance to explain IoT security behavior. *Computers in Human Behavior, 154*, 108092.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295–336.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Craciun, R. A., et al. (2025). *Hybrid machine-learning approaches for IoT-enabled smart buildings / intrusion detection.* Computers (MDPI) / related MDPI outlet. https://www.mdpi.com/2227-9709/12/1/17

Gondal, F. K. (2024). Security and privacy challenges for the IoT-based smart homes with limited resources and adoption immaturity. *Innovative Computing Review*, 10(1), 1-15.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2024). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (4th ed.). Sage Publications.

Hedayati, S., et al. (2023). *Meta-analysis on the application of Protection Motivation Theory to predict protective behaviors.* International Journal of Environmental Research and Public Health, article.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2023). Advances in composite-based structural equation modeling. *Journal of Business Research, 169*, 114200.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2023). New directions for the assessment of discriminant validity. *Journal of Business Research, 169*, 114200.

Ifinedo, P., & Usoro, A. (2022). Applying protection motivation theory to explain information security behavior: A meta-analytic review. *Information Systems Frontiers, 24*(3), 875–889.

Khan, N. F. (2023). *Evaluating protection motivation based cybersecurity training and protective behavior.* Computers & Security, 120, Article 102774. https://doi.org/10.1016/j.cose.2022.102774

Khan, S., Rahim, N., & Aziz, M. (2024). Artificial intelligence-based modeling for cybersecurity behavior prediction: A hybrid SEM–ML approach. *Expert Systems with Applications, 241*, 122893.

Kulsoom, U. e. (2023). *A review about Internet of Things (IoT) integration with cloud computing and security concerns.* Pakistan Journal of Engineering & Technology, 2023.

Laghari, A. A., Li, H., Khan, A. A., & et al. (2024). Internet of Things (IoT) applications security trends and challenges. *Discover Internet of Things, 4*, Article 36. https://doi.org/10.1007/s43926-024-00090-5

Mahmud, A., Yusoff, M. N., & Husin, M. H. (2023). Generation Z's adoption of IoT: Protection Motivation Theory as the underlying model and gender as a moderator. *Journal of Systems and Information Technology*, 2, 133-159. https://doi.org/10.1108/JSIT-02-2022-0054

Mahmud, I., Suhani, S., & Rahman, T. (2023). Understanding IoT security compliance behavior through protection motivation theory. *Computers & Security, 127*, 103151.

Mahmud, I., Suhani, S., & Rahman, T. (2023). Understanding IoT security compliance behavior through protection motivation theory. *Computers & Security, 127*, 103151.

Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., Elovici, Y. (2020). SAFER: Development and evaluation of an IoT device risk assessment framework in a multinational organization. arXiv.

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of Protection Motivation Theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems, 23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Muhammad, M., Bazai, S. U., Ullah, S., Shah, S. A. A., Aslam, S., Amphawan, A., & Neo, T.-K. (2024). A systematic literature review on the role of big data in IoT security. *Journal of Telecommunications and the Digital Economy*, 12(1), 39–64. https://doi.org/10.18080/jtde.v12n1.783

Nasr, M., & Kim, J. (2023). Artificial intelligence-driven behavioral prediction in cybersecurity risk modeling. *Expert Systems with Applications, 229*, 120826.

Saeed, M., Jan, W., & Shakeel, H. (2024). IoT adoption challenges and solutions in Pakistan: A systematic literature review approach. *International Journal of Emerging Business and Economic Trends, 3*(2), 134–142.

Salloum, S. A., Alfaisal, R., Al-Maroof, R. S., & Al-Ali, R. (2024). *Envisioning ChatGPT's integration as educational platforms: A hybrid SEM-ML method for adoption prediction.* ResearchGate / conference article (June 2024). https://www.researchgate.net/publication/379427238

Siponen, M., Mahmood, M. A., & Willison, R. (2024). Users' security compliance behavior: An updated protection motivation theory perspective. *Information & Management, 61*(1), 103812.

Siponen, M., Mahmood, M. A., & Willison, R. (2024). Users' security compliance behavior: An updated protection motivation theory perspective. *Information & Management, 61*(1), 103812.

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection Motivation Theory in information security behavior research: Reconsidering the fundamentals. *Communications of the Association for Information Systems*, 53, 1136-1165. https://doi.org/10.17705/1CAIS.05348

Suhani, N., Sulaiman, M. A., Hussain, S., & Walton, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, 13(9), 1–17. https://doi.org/10.3390/info13090413

Tahat, K., Mansoori, A., Tahat, D., et al. (2022). Detecting fake news during the COVID-19 pandemic: A SEM-ML approach. *Computers & Integrated Manufacturing Systems / related outlet.* (Dec 2022) — demonstrates SEM+ML hybrid workflow for behavioral prediction.