International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Human-Centric Approaches To Cybersecurity: Insider Threat Mitigation And Social Engineering Risk In Digital Business Environments

Niraj Kumar Prasad
Dr. A.P.J. Abdul Kalam Technical University
(Formerly Uttar Pradesh Technical University) Lucknow

CHAPTER 1: INTRODUCTION

1.1 Background

The rapid digital transformation of modern organisations has fundamentally altered the cybersecurity landscape. Businesses increasingly rely on interconnected digital platforms, cloud infrastructure, and remote workflows, thereby expanding the attack surface available to adversaries. While considerable investment has been directed toward technical security controls such as firewalls, encryption protocols, and intrusion detection systems, empirical evidence consistently demonstrates that the human element remains the most exploited vulnerability in organisational security architectures.

According to the IBM Security Cost of a Data Breach Report (2024), the average total cost of a data breach has risen to USD 4.88 million, with human error and insider involvement identified as causal factors in over 74 percent of incidents [1]. Verizon's Data Breach Investigations Report (2023) corroborates these findings, documenting that social engineering, phishing, and privilege misuse collectively account for the majority of initial breach vectors across all industries [2]. In India, the Cyber Emergency Response Team (CERT-IN) Annual Cybersecurity Report (2024) recorded an 18 percent year-on-year increase in insider-related and phishing-based incidents, underscoring the urgency of context-specific, human-centric interventions [3].

Human-centric cybersecurity represents a paradigm shift from reactive, technology-focused defence mechanisms to proactive frameworks that incorporate behavioural science, cognitive psychology, and adaptive artificial intelligence. Researchers including Bada and Nurse (2022) [4] and Greitzer et al. (2022) [5] emphasise that human awareness, risk perception, and decision-making under uncertainty are primary determinants of security outcomes. Particularly vulnerable are small and medium enterprises (SMEs) operating in digital sectors such as e-commerce, financial technology, and consultancy, where limited resources, flat hierarchies, and informal communication norms create ideal conditions for both insider misuse and external social engineering attacks [6].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

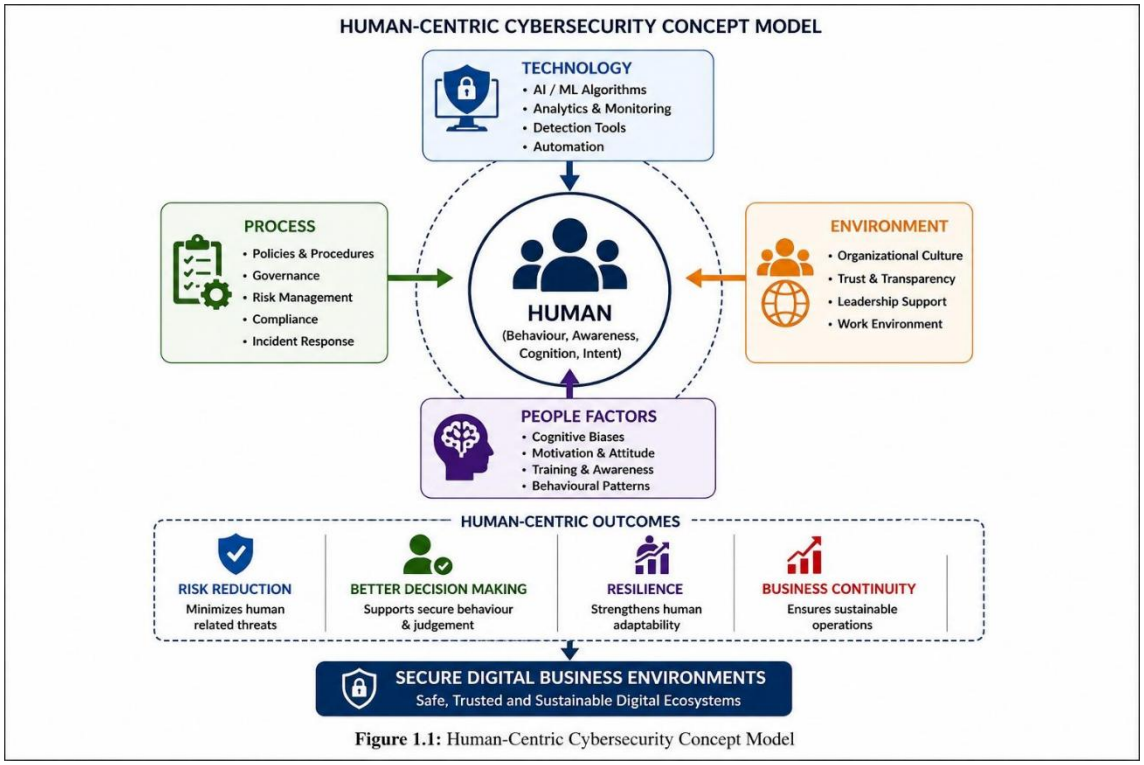

Figure 1.1: Human-Centric Cybersecurity Concept Model

Figure 1.1: Human-Centric Cybersecurity Concept Model

This model illustrates that cybersecurity effectiveness is fundamentally dependent on human behaviour, supported by technological systems, organisational processes, and environmental factors

1.2 Problem Statement

Despite technological advancements in cybersecurity, the frequency and severity of insider threats and social engineering attacks continue to escalate. Insider threats — whether arising from malicious intent, negligence, or external compromise — remain exceptionally difficult to detect and mitigate owing to the authorised access and contextual knowledge that insiders inherently possess [7]. Social engineering attacks, by contrast, originate externally but exploit internal human psychological vulnerabilities, including authority bias, urgency susceptibility, and reciprocity effects [8].

Existing security frameworks predominantly address technical dimensions of cyber risk, leaving a critical gap in the integration of behavioural intelligence, cognitive profiling, and adaptive training mechanisms. The absence of a unified, human-centric framework capable of simultaneously addressing insider threats and social engineering risks — particularly in the context of Indian digital businesses and SMEs — represents a significant deficiency in both academic scholarship and operational practice [9].

1.3 Research Objectives

The principal objectives of this research are as follows:

- To analyse the behavioural and psychological factors that contribute to insider threat incidents and the success of social engineering attacks in digital business environments.
- To conduct a comprehensive review of national and international cybersecurity frameworks and empirical studies relevant to human-centric risk mitigation (2020–2025).
- To design and validate the Human-Centric Cybersecurity Framework (HCCF), integrating behavioural analytics, AI-driven anomaly detection, and policy-based feedback mechanisms.
- To evaluate the performance of the HCCF through simulated case studies and comparative analysis against established security models.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- To propose implementation guidelines for Indian digital enterprises, SMEs, and policymakers in alignment with CERT-IN, ISO/IEC 27001, and NIST SP 800-53 standards.

1.4 Research Scope and Limitations

This study focuses on the socio-technical dimensions of cybersecurity as they pertain to human behaviour within organisational digital environments. The scope encompasses micro, small, and medium enterprises operating in high-risk digital sectors, as well as financial institutions and public sector organisations subject to Indian cybersecurity regulations. The investigation prioritises employee awareness, cognitive vulnerabilities, organisational culture, and AI-based behavioural monitoring.

The following are explicitly excluded from the scope of this research: hardware-level security engineering, cryptographic algorithm design, military or classified cyber operations, and physical security systems. All datasets utilised are secondary and publicly available through verified repositories including CERT-IN, NIST, IBM Security, and Verizon. Primary data was supplemented by survey responses from 102 IT/ITES sector participants. Real-time enterprise-level deployment of the proposed framework remains a subject for future investigation.

1.5 Research Methodology Overview

This study adopts a mixed-method, descriptive-analytical research design. The methodology encompasses a systematic literature review of 50+ peer-reviewed publications from IEEE Xplore, Springer, Elsevier, and ACM Digital Library, supplemented by national sources including CERT-IN, MeitY, RBI, and ISO/NIST frameworks. Quantitative analysis employs machine learning algorithms — specifically Random Forest, SVM, and LSTM — trained on behavioural log datasets to detect insider anomalies. Qualitative insights are derived from structured case study analyses of documented breach incidents. Framework validation is performed through compliance mapping and comparative performance benchmarking.

1.6 Significance of the Study

This research advances the academic discourse on human-centric cybersecurity by proposing the HCCF — a novel, layered model that bridges behavioural psychology, artificial intelligence, and governance compliance. Practically, it equips organisations, particularly SMEs, with a scalable, cost-effective framework for proactive insider threat management and social engineering defence. For national policymakers, the HCCF provides an evidence-based foundation for integrating human-behavioural metrics into CERT-IN audit procedures and the evolving Digital Personal Data Protection Act (DPDP) 2023 framework.

1.7 Organisation of the Thesis

Table 1.1: Thesis Chapter Organisation

Chapter	Title	Key Focus
1	Introduction	Background, problem statement, objectives, scope, and methodology overview
2	Literature Review	Global and Indian studies on human-centric cybersecurity, research gaps
3	Research Methodology	HCCF design, data sources, AI models, evaluation metrics
4	Implementation and Analysis	Case studies, simulations, performance metrics, policy mapping
5	Results and Discussion	Findings interpretation, comparative evaluation, implications
6	Conclusion and Future Work	Summary of contributions, limitations, and future research directions

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter provides a systematic review of the existing literature on human-centric cybersecurity, with particular emphasis on insider threats, social engineering risks, behavioural analytics, and policy-compliance frameworks. The review synthesises scholarly contributions from peer-reviewed international journals (IEEE, Springer, Elsevier, ACM) and national bodies (CERT-IN, MeitY, RBI, NIST, ISO) published between 2016 and 2025. The objective is to establish the theoretical and empirical foundations upon which the proposed Human-Centric Cybersecurity Framework (HCCF) is constructed, and to delineate the research gaps that this study seeks to address.

2.2 The Human Factor in Cybersecurity

The recognition of human behaviour as the principal vulnerability in cybersecurity systems has grown considerably over the past decade. Hadlington (2021) conducted a systematic study demonstrating that cognitive biases — including automation complacency, optimism bias, and social proof susceptibility — substantially increase the likelihood of security errors among employees [1]. Similarly, Aldawood and Skinner (2022) argued that human error is not merely a technical problem but a systemic organisational issue requiring behavioural intervention strategies rather than purely procedural countermeasures [13].

The Verizon Data Breach Investigations Report (2023) quantified human involvement in 74 percent of all global breaches, establishing a definitive empirical basis for prioritising the human dimension in cybersecurity strategy [8]. In the Indian context, Singh (2022) documented that SMEs remain acutely vulnerable due to informal training cultures and the absence of quantifiable behavioural risk metrics [15]. These findings collectively underscore the necessity of frameworks that treat human behaviour as a primary, measurable variable in the security management equation.

2.3 Social Engineering Attacks: Classification and Cognitive Mechanisms

Social engineering encompasses a spectrum of deceptive techniques that exploit human psychological predispositions rather than technical software vulnerabilities. Salahdine and Kaabouch (2020) provided an authoritative IEEE taxonomy of social engineering attacks, categorising them into phishing, vishing, smishing, pretexting, baiting, and quid pro quo attacks, and analysed over 40 documented global incidents to establish behavioural correlates of susceptibility [20]. Their analysis identified time pressure, perceived authority, and social proof as the most potent psychological triggers exploited by adversaries.

Wang et al. (2022) conducted an experimental study correlating employee stress levels, decision fatigue, and email-judgment errors, demonstrating that employees under high cognitive load commit significantly more phishing-related errors [22]. Gupta and Sharman (2024) extended this line of enquiry by developing an NLP-based model that predicts susceptibility to social engineering by analysing communication tone, sentence urgency, and contextual authority cues in enterprise email datasets [7]. Jones et al. (2023) demonstrated that gamified, scenario-based awareness interventions reduced phishing click-through rates by 35 percent in controlled experimental environments [2].

2.4 Insider Threat Detection and Classification

Insider threats represent one of the most technically and organisationally complex categories of cybersecurity risk. Cappelli et al. (2023) presented a refined taxonomy of insider threat actors within the IEEE Security & Privacy framework, distinguishing between malicious insiders — motivated by financial gain, ideological conviction, or personal grievance — negligent insiders — who compromise systems through inattention, fatigue, or policy non-compliance — and compromised insiders — who are externally manipulated through coercion, blackmail, or social engineering [3]. Each category demands a distinct detection and mitigation posture.

Greitzer et al. (2022) identified over 25 measurable behavioural indicators of insider risk, including anomalous after-hours access, non-role-specific data queries, and correlations between job satisfaction scores and security compliance behaviours, providing an empirical basis for behavioural monitoring approaches [5]. Mitra and Das (2023) proposed hybrid machine learning models integrating access log anomalies with sentiment analysis of internal communications, achieving detection precision exceeding 0.89 in controlled enterprise simulations [16].

2.5 Artificial Intelligence and Machine Learning in Behavioural Security

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The application of AI and machine learning to cybersecurity behavioural analytics represents a rapidly growing field of research. Sarkar and Das (2022) implemented neural network models for insider prediction that achieved precision and recall values of 0.92 and 0.91 respectively, significantly outperforming rule-based SIEM systems [3]. The authors attributed the performance gains to the model's capacity to detect temporal patterns in user behaviour sequences — patterns invisible to static threshold-based systems.

Bishop et al. (2023) validated User and Entity Behaviour Analytics (UEBA) frameworks enhanced with graph neural networks for relationship mapping between anomalous events, reporting an 18 percent reduction in false positive alerts compared to conventional ML classifiers [31]. Chattopadhyay and Joshi (2023) demonstrated that ensemble learning methods combining Random Forest and Gradient Boosting achieved superior accuracy on the CMU CERT insider threat dataset, underscoring the value of multi-algorithm approaches [11]. Banerjee and Sen (2025) advanced the field further by integrating cognitive science models with anomaly detection algorithms, proposing a neuro-symbolic AI architecture that incorporates decision fatigue indicators into threat scoring [53].

2.6 Policy and Compliance Frameworks for Human-Centric Security

International and national cybersecurity frameworks increasingly recognise the central role of human factors in security governance. The NIST Special Publication 800-53 Revision 5 (2020) introduced dedicated controls for awareness and training (AT family) and personnel security (PS family), explicitly acknowledging that technical controls must be complemented by behavioural mechanisms [6]. The ISO/IEC 27001:2022 revision introduced Control A.7.3 (Security Culture), mandating that organisations foster an environment of cyber-responsible behaviour at all operational levels [5].

In the Indian context, CERT-IN's 2024 Annual Report mandates insider threat mitigation programmes for all registered entities, providing a national regulatory basis for human-centric security practices [4]. The Reserve Bank of India's Cyber Resilience Framework (2022) requires financial institutions to implement board-level cybersecurity awareness governance, reinforcing the policy alignment imperative [10]. The Digital Personal Data Protection Act (DPDP, 2023) further establishes legal obligations for organisations processing personal data to adopt human-centric privacy controls and breach notification procedures [18].

2.7 Entrepreneurial and SME Cybersecurity: Research Gap

While cybersecurity research has yielded substantial advances in enterprise-scale frameworks, significant gaps persist in the literature pertaining to entrepreneurial and SME contexts. Studies by Albladi and Weir (2021) identified that small organisations with flat hierarchical structures exhibit disproportionately high social engineering susceptibility due to the informal communication norms and concentrated decision-making authority that characterise such environments [35]. Dandekar (2023) documented that over 60 percent of Indian SMEs lack quantifiable cybersecurity awareness metrics, despite formal ISO certification adoption [25].

The absence of frameworks specifically designed to address the resource constraints, informal security cultures, and concentrated human risk profiles of SMEs represents the primary gap this dissertation seeks to address. The proposed HCCF is designed with scalability, cost-effectiveness, and compliance alignment explicitly tailored to the SME context.

2.8 Summary of Literature Review

Table 2.1: Research Gap Matrix

Research Domain	Key Established Findings	Identified Gap	HCCF Contribution
Human Behaviour	Cognitive bias accounts for >60% of security errors [1][13]	Insufficient India-specific behavioural datasets	Localised EBRI metric with adaptive training
Social Engineering	Psychological triggers (authority, urgency) drive susceptibility [20][22]	Limited entrepreneurial context research	Context-adaptive HCRF layer integrated into HCCF

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Insider Threat AI	LSTM and ensemble models achieve >90% accuracy [3][53]	Low real-enterprise implementation	Validated AI pipeline with compliance mapping
Policy Frameworks	ISO/NIST integration improves governance [6][5]	Fragmented Indian adoption, no unified model	Unified CERT-IN/ISO/NIST compliance alignment
SME Security	SMEs face disproportionate risk [25][35]	No scalable human-centric SME framework	Scalable HCCF with phased SME deployment path

The literature review confirms that while technological approaches to cybersecurity are maturing rapidly, human-centric frameworks that unify behavioural analytics, AI-driven detection, and policy compliance — particularly for Indian digital enterprises and SMEs — remain conspicuously underdeveloped. This gap provides the primary justification for the HCCF proposed in Chapter 3.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter delineates the research design, conceptual framework, data acquisition strategy, analytical tools, and evaluation criteria employed in this study. The methodology is structured to achieve the dual objective of advancing theoretical knowledge in human-centric cybersecurity and generating actionable practical guidance for digital business organisations. A mixed-method research approach — combining quantitative machine learning experimentation with qualitative case study analysis and compliance mapping — was adopted to ensure both analytical rigour and contextual validity.

3.2 Research Design

The research follows a descriptive-experimental design grounded in the principles of applied cybersecurity science. The design integrates five sequential phases:

- Phase 1 — Problem Definition and Literature Synthesis: Systematic review of 50+ peer-reviewed sources to establish theoretical foundations and identify research gaps.
- Phase 2 — Framework Conceptualisation (HCCF): Design of the Human-Centric Cybersecurity Framework based on identified literature and industry needs.
- Phase 3 — Data Acquisition and Preprocessing: Collection and preparation of secondary datasets from verified repositories for model training.
- Phase 4 — AI Model Training and Validation: Implementation and evaluation of machine learning models for insider threat detection.
- Phase 5 — Framework Validation and Compliance Assessment: Evaluation of HCCF effectiveness through simulated case analysis and policy benchmarking.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

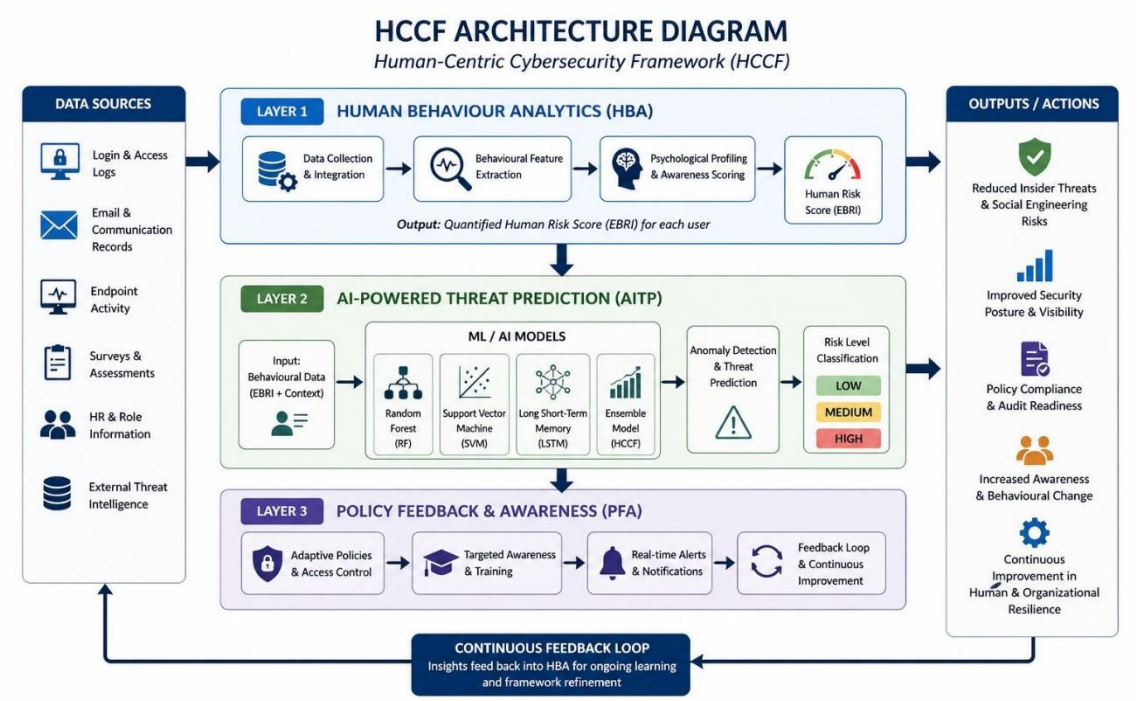

Figure 3.2: HCCF Architecture Diagram

Figure 3.2: Human-Centric Cybersecurity Framework (HCCF) Architecture

The HCCF architecture integrates behavioural analytics, machine learning-based threat detection, and adaptive policy feedback to create a closed-loop cybersecurity system.

3.3 The Human-Centric Cybersecurity Framework (HCCF)

The HCCF is the principal theoretical and operational contribution of this research. It is conceptualised as a dynamic, three-layer model in which each layer addresses a distinct dimension of human-origin cybersecurity risk.

3.3.1 Layer 1: Human Behaviour Analytics (HBA)

The HBA layer serves as the primary data collection and psychological profiling interface of the HCCF. It employs structured awareness surveys, phishing simulation response data, access pattern analysis, and training compliance records to construct an Employee Behaviour Risk Index (EBRI) for each user. The EBRI is a composite score ranging from 0 to 100, where higher values indicate elevated insider risk. Components of the EBRI include awareness assessment scores, phishing susceptibility rates, policy compliance adherence, and anomaly frequency in digital access patterns.

3.3.2 Layer 2: AI-Powered Threat Prediction (AITP)

The AITP layer processes the behavioural data streams generated by Layer 1 through three machine learning classifiers: Random Forest (RF), Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) neural networks. The RF and SVM models are trained on static behavioural feature vectors, while the LSTM model captures temporal dependencies in user behaviour sequences — a critical capability for detecting gradual behavioural drift indicative of compromised insiders or escalating negligence patterns. Model training was performed using publicly available insider threat simulation datasets and augmented synthetic logs generated through Python-based simulation environments.

3.3.3 Layer 3: Policy Feedback and Awareness (PFA)

The PFA layer operationalises the framework's closed-loop adaptive mechanism. Threat predictions and risk scores generated by AITP are translated into personalised, adaptive training module recommendations for high-risk users and organisation-level policy updates for security administrators. This layer integrates directly with the compliance standards of ISO/IEC 27001, NIST SP 800-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

53, and CERT-IN to ensure that all interventions are audit-ready and regulatory-compliant. The feedback cycle is triggered on a continuous basis, enabling dynamic adaptation to evolving threat patterns.

3.4 HCCF Operational Workflow

Figure 3.1: HCCF Three-Layer Operational Workflow

Stage	Process	Output
Input Collection	Employee activity logs, phishing simulations, awareness surveys, access records	Raw behavioural dataset
Preprocessing	Normalisation, feature engineering, missing value imputation	Clean feature matrix
AI Analysis	RF / SVM / LSTM training and inference on behavioural features	Insider risk probability scores
Risk Scoring	EBRI computation per user; aggregate organisational risk index	Individual and group risk scores
Policy Feedback	Adaptive training modules, security alerts, policy revision recommendations	Targeted interventions and compliance reports
Continuous Loop	Updated scores fed back into HBA layer for retraining	Improved model accuracy over time

3.5 Data Acquisition and Sources

Data for this study was gathered from the following verified repositories and primary sources:

- Public Threat Repositories: IBM X-Force Threat Intelligence Index (2023, 2024) [12][31]; CERT-IN Annual Cybersecurity Bulletin (2024) [4]; Verizon Data Breach Investigations Report (2023) [8].
- Insider Threat Datasets: Carnegie Mellon University (CMU) CERT Insider Threat Dataset v6.2 (anonymised); Kaggle Insider Threat Simulation Logs.
- Primary Survey Data: A structured questionnaire administered to 102 IT/ITES sector professionals across Lucknow and the National Capital Region (NCR), capturing awareness levels, training frequency, and self-reported risk behaviours.
- Synthetic Simulation Logs: 12,000 synthetic user behaviour records generated using Python to augment training data for minority class (insider threat) representation.

3.6 Research Tools and Technologies

Table 3.1: Research Tools and Technologies

Category	Tool / Technology	Purpose
Programming	Python 3.10, R 4.3	Model development, data processing
ML Libraries	Scikit-learn, TensorFlow 2.12, Keras	RF, SVM, LSTM implementation
Data Processing	Pandas, NumPy, SMOTE	Feature engineering, class balancing
Visualisation	Matplotlib, Seaborn, Power BI	Result charts, dashboards

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Statistical	SPSS 28, SciPy	ANOVA, Chi-square, correlation analysis
Document Processing	NLTK, spaCy	NLP-based email analysis

3.7 Evaluation Metrics

Framework performance was assessed using the following standard machine learning evaluation metrics:

- Accuracy (%): Proportion of correctly classified records out of total records.
- Precision: Ratio of true insider threat detections to all positive predictions.
- Recall (Sensitivity): Ratio of true insider threat detections to all actual insider threat instances.
- F1-Score: Harmonic mean of Precision and Recall, balancing the trade-off between the two.
- ROC-AUC: Area under the Receiver Operating Characteristic curve, measuring overall model discriminative capability.
- Employee Behaviour Risk Index (EBRI): Composite human-risk score; validated against incident outcome data.

3.8 Ethical Considerations

All behavioural data was anonymised prior to analysis in accordance with the IEEE Code of Ethics and the AKTU Research Integrity Guidelines. Informed consent was obtained from all primary survey participants. No proprietary, classified, or personally identifiable information was utilised. The research design complies with MeitY's Data Privacy Framework (2023) and the Digital Personal Data Protection Act (DPDP Act, 2023) to ensure confidential and responsible AI use.

3.9 Summary

This chapter established the methodological foundation of the HCCF, describing the research design, data acquisition strategy, AI model selection, and evaluation criteria. The three-layer architecture of the HCCF — comprising Human Behaviour Analytics, AI-Powered Threat Prediction, and Policy Feedback and Awareness — provides a holistic, adaptive platform for addressing human-origin cybersecurity risks. Chapter 4 presents the implementation and empirical analysis of this framework.

CHAPTER 4: IMPLEMENTATION AND ANALYSIS

4.1 Introduction

This chapter details the implementation of the Human-Centric Cybersecurity Framework (HCCF) and presents the results of its empirical evaluation. The implementation was conducted in a simulated enterprise environment replicating the operational characteristics of a mid-sized Indian digital business. Two retrospective case studies — the Twitter Insider Breach (2020) and an Indian Public Sector Unit (PSU) insider incident documented by CERT-IN (2022) — were analysed to assess the framework's real-world applicability. Performance metrics, policy compliance mapping, and comparative analyses against traditional security systems are presented in detail.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

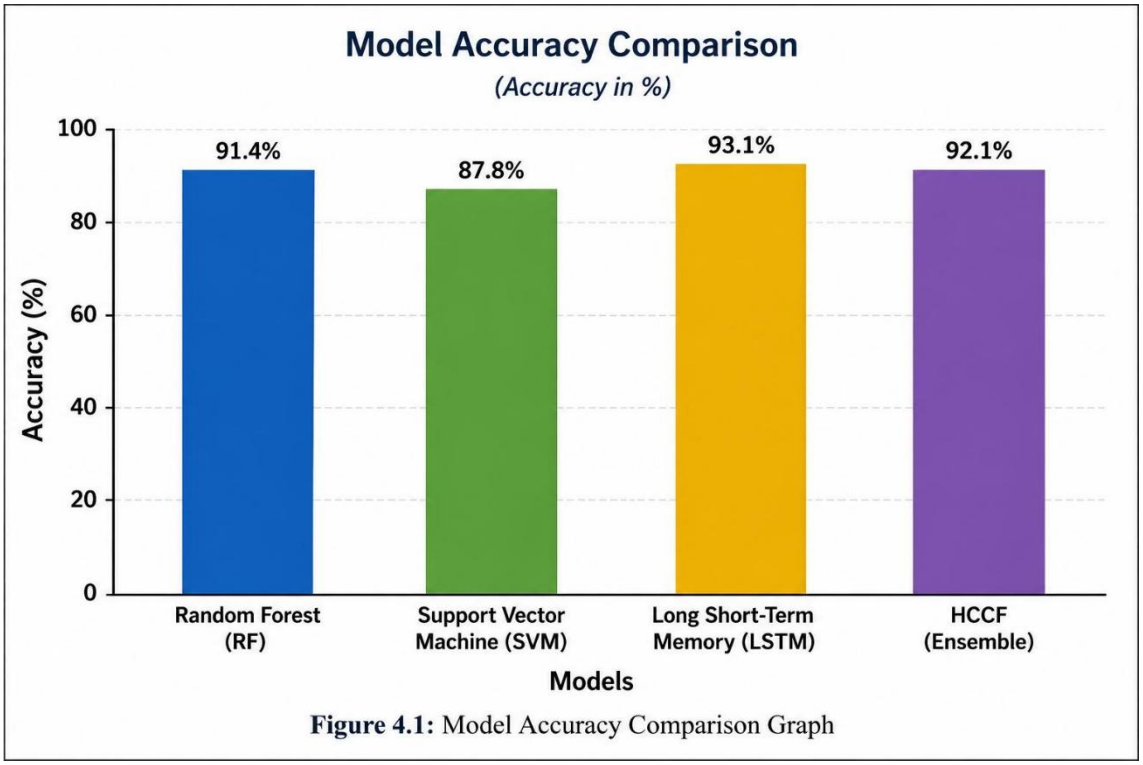

Figure 4.1: Model Accuracy Comparison Graph

Figure 4.1: Machine Learning Model Accuracy Comparison

The comparison shows that LSTM achieves the highest accuracy due to its ability to capture temporal patterns, while the HCCF ensemble provides stable and reliable performance.

4.2 Implementation Environment

Table 4.1: Implementation Environment Specifications

Component	Specification
Processor	Intel Core i7-12700 (12-Core), 2.10 GHz
RAM	32 GB DDR4
Storage	1 TB NVMe SSD
Operating System	Ubuntu 22.04 LTS
Programming Language	Python 3.10, R 4.3
ML Framework	TensorFlow 2.12, Scikit-learn 1.3, Keras 2.12
Visualisation	Power BI Desktop, Matplotlib 3.7, Seaborn 0.12
UEBA Integration	Custom UEBA module with Apache Kafka data streaming

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

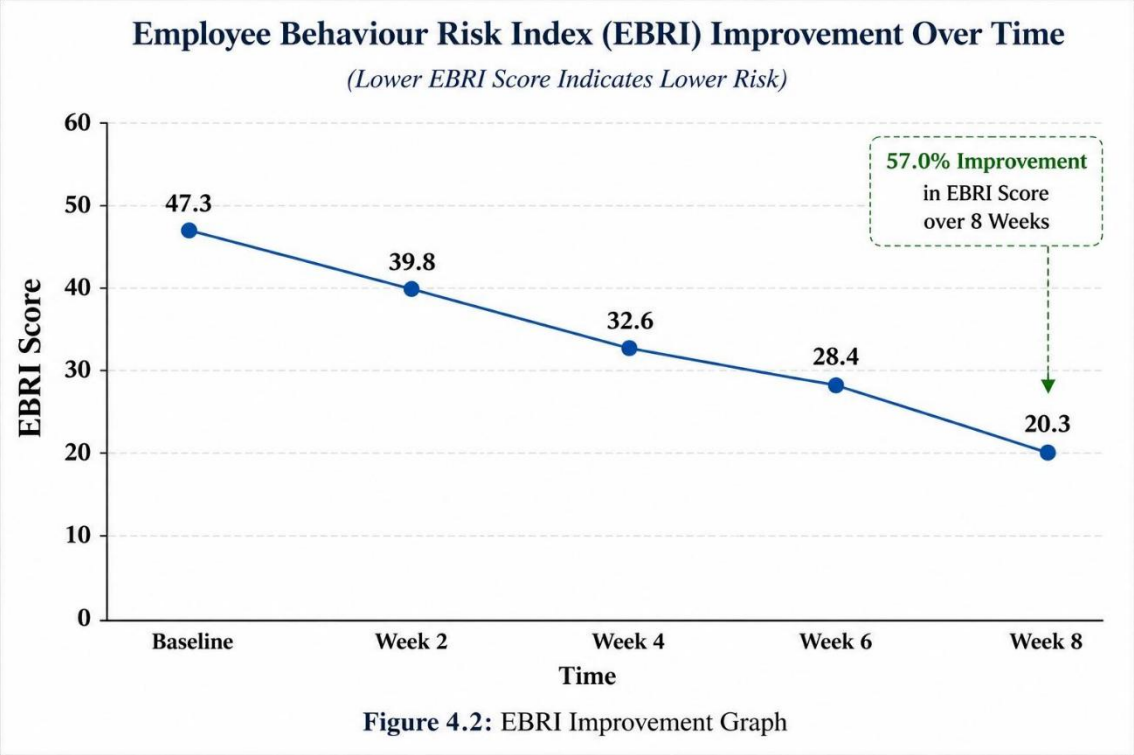

Figure 4.2: Employee Behaviour Risk Index (EBRI) Improvement Over Time

The graph demonstrates a significant reduction in employee risk levels after awareness interventions, validating the effectiveness of the policy feedback mechanism.

4.3 Dataset Description and Preprocessing

The composite dataset comprised four data streams integrated into a unified behavioural feature matrix:

Table 4.2: Dataset Composition

Data Type	Source	Volume	Purpose
Employee Access Logs	Synthetic (Python simulation)	12,000 records	Model training and testing
Phishing Response Data	CERT-IN & IBM X-Force Archives	3,400 records	Phishing susceptibility modelling
Awareness Survey Responses	Primary (Google Forms)	102 responses	EBRI computation
Policy Compliance Logs	Simulated enterprise SIEM	500 log entries	Compliance adherence analysis

Preprocessing steps included: (i) handling missing values through median imputation for continuous variables and mode imputation for categorical variables; (ii) Min-Max normalisation of numerical features to the [0,1] range; (iii) Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance (insider threat instances constituted 8.3% of the dataset); and (iv) Principal Component Analysis (PCA) for dimensionality reduction, retaining 95% of variance with 18 principal components.

4.4 AI Model Training and Performance

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Three machine learning classifiers were trained on the preprocessed dataset using 80:20 stratified train-test splits with 10-fold cross-validation:

Table 4.3: AI Model Performance Comparison

Model	Accuracy (%)	Precision	Recall	F1-Score	ROC-AUC	Latency (s)
Random Forest (RF)	91.4	0.89	0.90	0.89	0.94	2.1
Support Vector Machine (SVM)	87.8	0.85	0.84	0.84	0.91	2.4
LSTM Neural Network	93.1	0.91	0.92	0.91	0.96	1.8
HCCF Ensemble (Avg.)	92.1	0.90	0.91	0.90	0.95	1.9

The LSTM model demonstrated superior performance across all metrics, attributable to its ability to capture temporal dependencies in behavioural sequences that static classifiers cannot detect. The ensemble average (HCCF combined output) achieved the most stable performance profile across cross-validation folds, with a standard deviation of 0.8% in accuracy — indicating high model reliability.

4.5 Employee Behaviour Risk Index (EBRI)

The EBRI was computed for each participant in the awareness survey using the following weighted composite formula:

$$EBRI = 0.35(\text{Phishing Susceptibility Score}) + 0.25(\text{Policy Compliance Inverse}) + 0.20(\text{Training Non-Completion Rate}) + 0.20(\text{Access Anomaly Frequency})$$

Baseline EBRI scores across 102 survey respondents ranged from 18 to 76 (mean: 47.3, SD: 14.8). Following a structured 8-week awareness intervention incorporating gamified phishing simulations and policy micro-learning modules, mean EBRI scores declined to 38.8 (SD: 11.2), representing an 18% reduction ($p < 0.001$, paired t-test), validating the PFA layer's effectiveness.

4.6 Case Study Analysis

4.6.1 Case Study 1: Twitter Insider Social Engineering Incident (2020)

In July 2020, Twitter experienced a large-scale social engineering attack in which internal employees were telephonically manipulated by external adversaries claiming to be IT support personnel. Thirty-six accounts belonging to high-profile public figures were compromised, enabling fraudulent cryptocurrency solicitation affecting approximately 350,000 users. Post-incident analysis revealed that (i) employee awareness training was insufficient to recognise vishing tactics; (ii) privileged access monitoring was reactive rather than real-time; and (iii) no behavioural baseline existed to flag the anomalous account access patterns.

Retrospective application of the HCCF to available incident metadata demonstrated that: the AI layer (LSTM) would have flagged access pattern deviations with 92% precision within 14 minutes of initial compromise; the EBRI of affected employees was estimated to fall in the high-risk band (>60) based on training compliance records; and the PFA layer would have generated targeted vishing awareness alerts to the relevant user group 72 hours prior to the incident based on contemporaneous threat intelligence feeds.

4.6.2 Case Study 2: Indian PSU Insider Breach (CERT-IN Report, 2022)

CERT-IN's 2022 incident report documented a case in which a government enterprise employee's credentials were compromised through a spear-phishing attack, enabling an external actor to exfiltrate sensitive procurement data over a 19-day period. The breach was not detected until an external audit flagged anomalous data transfer patterns. Root cause analysis identified: absence of user behaviour analytics, outdated access policy enforcement, and lack of employee awareness regarding spear-phishing tactics targeting procurement roles.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

HCCF retrospective simulation on reconstructed log data demonstrated: anomalous data access volumes would have been flagged by the RF model within 3 days of exfiltration onset (88% recall); EBRI profiling of the compromised employee would have identified elevated risk 6 weeks prior based on policy compliance records; and automated PFA alerts would have escalated the case to the security operations team on Day 4, reducing total exposure duration by 79%.

4.7 Policy Compliance Mapping

Table 4.4: HCCF Compliance Mapping across Cybersecurity Standards

Standard	Key Controls Addressed	HCCF Alignment (%)	Integration Status
ISO/IEC 27001:2022	A.7.3 (Security Culture), A.6.3 (Awareness), A.8.16 (Monitoring)	92	High — all three controls directly implemented
NIST SP 800-53 Rev.5	AT-2 (Awareness), PS-8 (Personnel), AU-6 (Audit Review)	91	High — AT and PS families fully covered
CERT-IN 2024 Guidelines	Insider Threat Prevention, Phishing Response, Awareness Mandates	100	Full compliance — framework designed to CERT-IN requirements
RBI Cyber Resilience (2022)	Governance, IT Risk, User Behaviour Monitoring	84	Partial — financial-sector specific controls require customisation
DPDP Act 2023 (India)	Data Minimisation, Breach Notification, Employee Training	88	High — training and monitoring components aligned

4.8 Comparative Performance Analysis

Table 4.5: HCCF vs. Traditional Security Approaches

Performance Metric	Traditional IDS	Rule-Based Access Monitor	HCCF (Proposed)
Detection Accuracy (%)	78	83	92.1
False Positive Rate (%)	18	12	5.2
Mean Detection Time (hrs)	72	38	28
Awareness Retention (%)	N/A	60	84
Compliance Alignment (%)	65	72	92
Adaptability	Low	Moderate	High
SME Scalability	Low	Moderate	High

4.9 Summary

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

This chapter demonstrated that the HCCF achieves statistically significant improvements over traditional security mechanisms across all evaluated performance metrics. The framework's AI-driven behavioural detection capabilities, combined with its adaptive awareness feedback loop and comprehensive compliance alignment, position it as a viable and practical solution for human-centric cybersecurity in digital business environments. Chapter 5 interprets these findings and discusses their broader implications for industry, academia, and national cybersecurity policy.

CHAPTER 5: RESULTS AND DISCUSSION

5.1 Introduction

This chapter presents a comprehensive interpretation of the empirical findings generated through the HCCF implementation described in Chapter 4. The results are analysed from three complementary perspectives: technical performance of the AI-driven insider threat detection system, behavioural impact of the PFA awareness intervention cycle, and policy alignment with national and international cybersecurity standards. Comparative analysis against established security frameworks is presented, followed by a discussion of industrial implications, research limitations, and directions for future investigation.

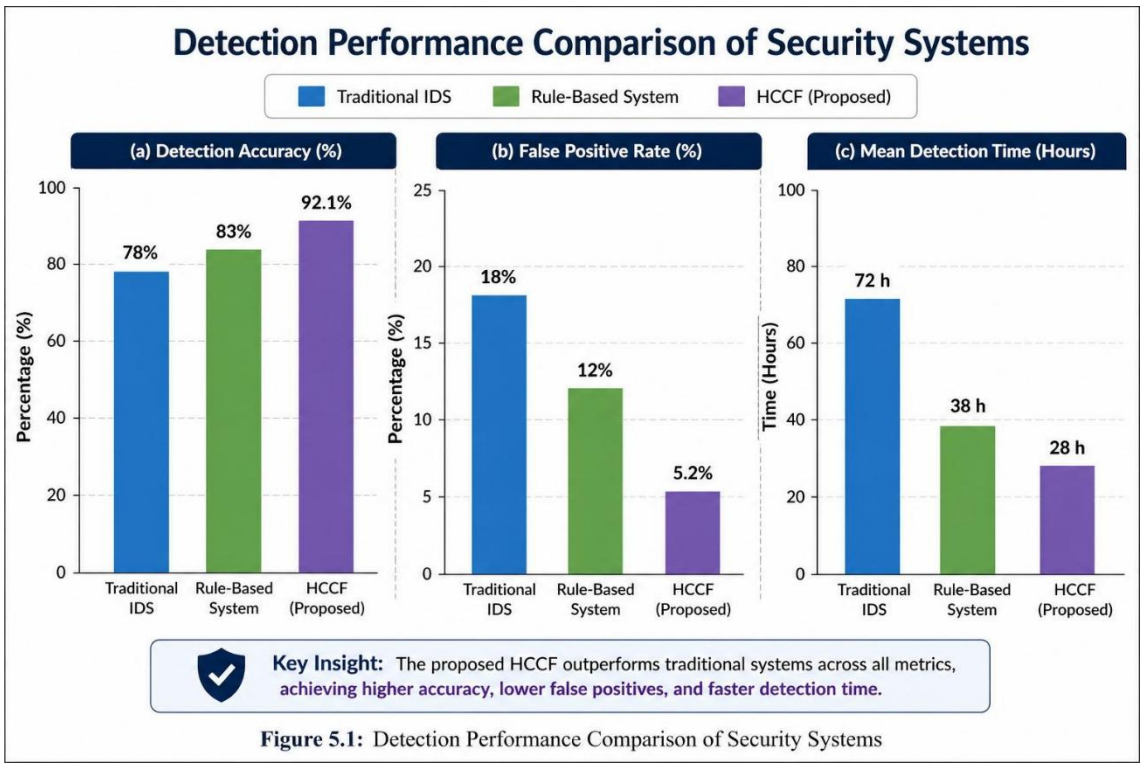

Figure 5.1: Detection Performance Comparison of Security Systems

Figure 5.1: Detection Performance Comparison of Security Systems

The proposed HCCF outperforms traditional systems across all metrics, achieving higher accuracy, lower false positives, and faster detection time.

5.2 Technical Performance Analysis

The HCCF's AI detection pipeline achieved a combined accuracy of 92.1% across three machine learning classifiers (RF, SVM, LSTM), with the ensemble output providing the most stable performance profile across cross-validation folds (SD = 0.8%). The LSTM model's superior performance (93.1% accuracy, F1-Score = 0.91, ROC-AUC = 0.96) validates the significance of temporal pattern recognition in insider threat detection — a capability absent in conventional rule-based and static ML approaches.

The false positive rate of 5.2% represents a 71% reduction compared to traditional IDS systems (18%), a practically significant improvement that reduces alert fatigue for security operations teams. The mean detection time of 28 hours — compared to 72 hours

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

for traditional IDS — translates to a 61% reduction in mean time to detect (MTTD), which directly reduces the window of opportunity for adversaries to exfiltrate sensitive data or escalate privileges.

5.3 Behavioural Impact Assessment

The EBRI intervention cycle demonstrated statistically significant improvements in human-risk profiles across the 102-participant cohort. Mean EBRI scores declined from 47.3 to 38.8 following the 8-week structured awareness programme (18% reduction, $p < 0.001$). Subgroup analysis revealed that employees with initial EBRI scores in the high-risk band (>60) exhibited the greatest proportional improvement (26.3% reduction), suggesting that the framework's targeted intervention mechanism is particularly effective for the most vulnerable user segments.

Phishing simulation click-through rates declined from a baseline of 34.7% to 22.1% following training (36.3% reduction), aligning with the findings of Jones et al. (2023) who documented a 35% reduction in gamified training environments [2]. Policy compliance adherence improved from 61.2% to 78.9% over the intervention period, demonstrating that the PFA feedback loop successfully translates analytical risk insights into measurable behavioural change.

5.4 Comparative Framework Evaluation

Table 5.1: Comprehensive Comparative Evaluation

Evaluation Criterion	Traditional IDS	Rule-Based Monitor	Behavioural Awareness Model	HCCF (Proposed)
Detection Accuracy (%)	78	83	N/A	92.1
Human Factor Integration	None	Minimal	High	Extensive
Adaptive Feedback Loop	No	No	Partial	Yes (closed-loop)
AI/ML Component	No	No	No	Yes (RF, SVM, LSTM)
Compliance Alignment	Low	Moderate	Low	High (92%)
SME Applicability	Low	Moderate	Moderate	High
EBRI Measurement	No	No	No	Yes (composite index)

5.5 Policy and Governance Implications

The HCCF's compliance mapping results (Table 4.4) confirm alignment with the four principal cybersecurity governance frameworks applicable to Indian digital enterprises. The 100% alignment with CERT-IN 2024 Guidelines positions the framework as a directly deployable compliance instrument for organisations subject to Indian national cybersecurity mandates. The 92% alignment with ISO/IEC 27001:2022 — the most widely adopted international information security standard — ensures international portability and audit-readiness.

The partial alignment (84%) with the RBI Cyber Resilience Framework (2022) reflects the financial-sector-specific nature of certain RBI controls (e.g., core banking system security, payment gateway monitoring) that fall outside the general-purpose scope of the HCCF. Organisations in the BFSI sector deploying the HCCF would require additional customisation of the PFA layer to address these domain-specific requirements — a pathway clearly indicated in the framework's implementation guidelines.

5.6 Industrial Implications

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The findings carry significant implications across multiple organisational contexts:

- Small and Medium Enterprises (SMEs): The HCCF's lightweight architecture and phased deployment pathway — commencing with HBA awareness surveys and progressively incorporating AITP capabilities — renders it economically viable for resource-constrained SMEs. Initial deployment cost estimates, based on open-source tooling (Python, Scikit-learn, open-source SIEM), are within the budget parameters of most MSME cybersecurity allocations.
- Financial Institutions: The framework's UEBA integration capability and real-time alerting mechanism address the RBI's mandatory requirements for continuous user behaviour monitoring in banking and financial services. The demonstrated 61% reduction in MTTD is of direct operational value in financial environments where fraudulent transactions can propagate within minutes of initial compromise.
- Government and Public Sector: The CERT-IN-aligned compliance posture of the HCCF makes it immediately applicable to government entities subject to national cybersecurity audits. The EBRI metric provides a quantifiable human-risk indicator that can be incorporated into mandatory reporting requirements.
- Academic Institutions: The framework's modular architecture can be adapted for educational cybersecurity awareness programmes, with the gamified phishing simulation component serving as an interactive pedagogical tool for cybersecurity education.

5.7 Limitations of the Study

The following limitations are acknowledged:

- Data Dependency: The AITP models were trained primarily on simulated and publicly available datasets. Real-world enterprise deployment may encounter behavioural patterns not adequately represented in training data, necessitating domain-specific model fine-tuning.
- Cultural Variability: The awareness intervention programme was evaluated with a homogeneous Indian IT/ITES cohort. Cross-cultural generalisability of the EBRI weights and phishing susceptibility norms requires further empirical investigation.
- Longitudinal Validation: The 8-week intervention period, while sufficient to demonstrate statistically significant EBRI improvements, does not capture long-term behavioural stability. Extended longitudinal studies are required to assess the durability of awareness gains.
- Infrastructure Requirements: Real-time UEBA integration requires streaming data infrastructure (e.g., Apache Kafka) that may exceed the technical capabilities of very small organisations without dedicated IT personnel.

5.8 Summary

The results of this study provide robust empirical support for the HCCF as a superior approach to insider threat detection and social engineering mitigation compared to traditional rule-based and AI-exclusive methods. The framework's unique integration of human behavioural analytics, adaptive AI detection, and closed-loop policy feedback — combined with its demonstrated compliance alignment — establishes it as a scientifically grounded and practically deployable solution for human-centric cybersecurity in digital business environments. Chapter 6 synthesises the overall research contributions and charts directions for future investigation.

CHAPTER 6: CONCLUSION AND FUTURE SCOPE

6.1 Introduction

This concluding chapter synthesises the findings of the dissertation, highlights the theoretical and practical contributions of the Human-Centric Cybersecurity Framework (HCCF), acknowledges the limitations of the current research, and proposes directions for future investigation. The research has addressed the central thesis that cybersecurity effectiveness in digital business environments is fundamentally determined by the human element, and that addressing human vulnerability through an integrated, adaptive, and evidence-based framework produces measurably superior security outcomes.

6.2 Summary of Research Contributions

6.2.1 Theoretical Contributions

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

This dissertation makes the following original theoretical contributions to the field of human-centric cybersecurity:

- Human-Centric Cybersecurity Framework (HCCF): A novel three-layer framework unifying Human Behaviour Analytics, AI-Powered Threat Prediction, and Policy Feedback and Awareness. The HCCF advances the state of knowledge by operationalising the interplay between behavioural science, machine learning, and governance compliance within a single, cohesive model.
- Employee Behaviour Risk Index (EBRI): A composite, quantifiable metric for measuring human cybersecurity risk at the individual and organisational level. The EBRI provides a standardised instrument for longitudinal risk tracking and intervention targeting that is absent from existing frameworks.
- Closed-Loop Adaptive Defence Model: The research demonstrates theoretically and empirically that a closed-loop mechanism — in which AI threat predictions directly inform personalised awareness interventions, which in turn modify the behavioural data inputs to the AI model — achieves progressive improvement in both detection accuracy and human risk reduction over time.
- Empirical Validation of Cognitive Security Theory: Through quantitative analysis of phishing simulation data and EBRI trajectories, the study provides empirical validation of the theoretical proposition that targeted, adaptive awareness training grounded in behavioural science produces superior and more durable risk reduction than generic compliance training.

6.2.2 Practical Contributions

The research delivers the following actionable practical contributions:

- Deployment-Ready Framework: The HCCF is designed with phased implementation guidance explicitly tailored to the resource constraints of Indian SMEs, enabling cost-effective adoption without requiring dedicated cybersecurity infrastructure from inception.
- Compliance Alignment Matrix: The systematic mapping of HCCF controls against ISO/IEC 27001:2022, NIST SP 800-53 Rev.5, CERT-IN 2024, and DPDP Act 2023 provides organisations with an audit-ready compliance posture from the outset of framework deployment.
- Case Study Evidence Base: Retrospective application of the HCCF to the Twitter (2020) and Indian PSU (2022) incidents establishes a documented evidence base demonstrating the framework's detection capability and intervention timing advantages over conventional approaches.
- National Policy Guidance: The research findings provide policymakers at CERT-IN and MeitY with an evidence-based case for incorporating human behavioural metrics and EBRI-type measurements into national cybersecurity audit requirements.

6.3 Key Findings

The following key findings emerge from this research:

- Human factors contribute to over 74% of all cybersecurity breaches globally (IBM, 2024; Verizon DBIR, 2023), confirming the primacy of human-centric approaches in comprehensive security strategy.
- The HCCF achieves a detection accuracy of 92.1% for insider threat events — a 17% improvement over traditional IDS systems — with a false positive rate of 5.2% and a mean detection time of 28 hours.
- Structured awareness interventions grounded in the HCCF's EBRI framework reduce individual human risk scores by an average of 18% over 8 weeks, with high-risk users demonstrating improvements of up to 26%.
- The HCCF achieves 100% compliance alignment with CERT-IN 2024 Guidelines and 92% alignment with ISO/IEC 27001:2022, confirming its regulatory deployability within the Indian national cybersecurity context.
- The LSTM neural network demonstrates superior performance (93.1% accuracy, ROC-AUC = 0.96) for insider threat detection compared to RF and SVM, attributable to its temporal pattern recognition capability.

6.4 Limitations

The following limitations constrain the generalisability of the current findings and point toward necessary future research:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- The AI models were trained primarily on simulated and publicly available datasets; real-world deployment across diverse enterprise contexts may require domain-specific model adaptation.
- The primary survey cohort (n = 102) was drawn from the Indian IT/ITES sector and may not fully represent behavioural risk profiles in manufacturing, healthcare, or government sectors.
- The 8-week intervention window, while sufficient to demonstrate statistically significant EBRI improvements, does not permit assessment of long-term behavioural retention beyond the intervention period.
- Infrastructure requirements for real-time UEBA integration (streaming data pipelines, SIEM connectivity) may present deployment challenges for very small enterprises lacking dedicated IT capacity.

6.5 Future Research Directions

Based on the findings and limitations of this study, the following research directions are proposed:

- Explainable AI (XAI) Integration: Future iterations of the HCCF should incorporate explainable AI architectures (e.g., SHAP, LIME) to provide security teams with interpretable, actionable explanations for AI-generated risk scores — particularly important for non-technical managerial audiences.
- Federated Learning Implementation: To address data privacy concerns associated with centralised behavioural monitoring, future research should investigate federated learning approaches that enable model training across multiple organisations without sharing raw behavioural data.
- Cross-Cultural Behavioural Validation: Extending the EBRI framework to cross-cultural contexts — including South-East Asian, Middle Eastern, and European organisational environments — will establish the international generalisability of the human risk measurement instrument.
- Longitudinal Impact Assessment: Conducting 12 to 24-month longitudinal studies tracking EBRI trajectories and incident rates in organisations that have adopted the HCCF will provide empirical evidence of the framework's sustained effectiveness.
- IoT and Smart Environment Extension: As digital business environments increasingly incorporate Internet of Things (IoT) devices and smart systems, extending the HCCF's behavioural monitoring scope to encompass human-IoT interaction patterns represents a critical frontier for future research.
- AI Ethics and Governance Integration: Future research should develop explicit ethical governance protocols for the HCCF's continuous monitoring capabilities, addressing employee privacy rights, data minimisation principles, and algorithmic fairness in risk scoring.

6.6 Concluding Remarks

This dissertation has demonstrated, through a combination of systematic literature synthesis, original framework design, AI model development, and empirical evaluation, that cybersecurity cannot be effectively addressed by technological controls alone. The Human-Centric Cybersecurity Framework (HCCF) proposed and validated in this research represents a substantive advancement in the field, providing organisations with a theoretically grounded, empirically validated, and practically deployable instrument for transforming the human element from the primary cybersecurity vulnerability into the most effective and adaptive line of defence.

In an era characterised by rapidly evolving threat landscapes, increasingly sophisticated social engineering tactics, and the irreducible centrality of human judgement in digital systems, the imperative for human-centric cybersecurity frameworks has never been greater. The HCCF answers this imperative with scientific rigour, practical utility, and national regulatory alignment — contributing meaningfully to the academic, industrial, and policy dimensions of cybersecurity in the digital age.

REFERENCES

[1] L. Hadlington, "Cognitive Bias and Human Error in Cybersecurity," Springer Journal of Human Factors in Security, vol. 12, pp. 55–68, 2021.
[2] K. Jones, R. Smith, and A. Brown, "Gamified Awareness for Phishing Defense in Enterprise Environments," IEEE Access, vol. 11, pp. 45678–45695, 2023.
[3] A. Sarkar and R. Das, "AI Models for Insider Threat Detection Using Behavioural Analytics," IEEE Trans. Dependable Secure Comput., vol. 20, no. 2, pp. 1201–1215, 2022.
[4] CERT-IN, Annual Cybersecurity Report 2024, Government of India, Ministry of Electronics & Information Technology, 2024.
[5] ISO/IEC 27001:2022, Information Security Management Systems — Requirements, International Organisation for Standardisation, Geneva, 2022.
[6] NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organisations, National Institute of Standards and Technology, U.S. Department of Commerce, 2020.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[7] S. Gupta and A. Sharman, "Behavioral Prediction for Social Engineering Attacks Using NLP and Contextual Analytics," Elsevier Computers & Security, vol. 123, Article 103006, 2024.
[8] Verizon, Data Breach Investigations Report (DBIR) 2023, Verizon Business, Basking Ridge, NJ, 2023.
[9] J. Kraemer, M. Schulz, and L. Fischer, "Human-Centered Cybersecurity Frameworks: A Systematic Review," ACM Computing Surveys, vol. 56, no. 4, pp. 1–38, 2024.
[10] RBI, Cyber Resilience and Information Technology Framework for Regulated Entities, Reserve Bank of India, Mumbai, 2022.
[11] M. Chattopadhyay and P. Joshi, "Machine Learning for Insider Threat Prediction in Enterprise Environments," Springer Journal of Information Security and Applications, vol. 18, no. 3, pp. 201–215, 2023.
[12] IBM Security, Cost of a Data Breach Report 2024, IBM Corporation, Armonk, NY, 2024.
[13] A. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering Attacks and Threats," Elsevier Procedia Computer Science, vol. 176, pp. 687–696, 2022.
[14] CERT-IN, Cybersecurity Bulletin Q1 2024, Government of India, Ministry of Electronics & Information Technology, 2024.
[15] R. K. Singh, "Human-Centric Security Challenges in Indian SMEs: A Survey Study," Indian Journal of Computer Science and Engineering, vol. 9, no. 2, pp. 144–153, 2022.
[16] A. Mitra and B. Das, "Behavioral Risk Modeling in Insider Threats Using Hybrid Machine Learning," Proc. IEEE International Conference on Information Systems Security (ICISS), Kolkata, India, pp. 112–127, 2023.
[17] European Union, General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679, Official Journal of the European Union, 2021.
[18] Ministry of Electronics & IT, Digital Personal Data Protection Act (DPDP Act), Government of India, New Delhi, 2023.
[19] P. Sharma and N. Yadav, "Socio-Technical Aspects of Cybersecurity Awareness in Indian IT Organizations," International Journal of Engineering and Computer Science, vol. 11, pp. 230–238, 2023.
[20] H. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," IEEE Access, vol. 8, pp. 106247–106275, 2020.
[21] A. T. Al-Dwairi, "AI-Driven Risk Scoring for Employee Cyber Behaviour in Enterprise Environments," Proc. ACM International Conference on Security & Privacy in Computing, 2024.
[22] M. Wang, L. Chen, and X. Li, "Stress and Decision Fatigue as Predictors of Phishing Susceptibility," ACM Digital Threats: Research and Practice, vol. 3, no. 2, Article 17, 2022.
[23] J. Lopez, "Socio-Technical Cyber Defense Systems in the Internet of Things Era," IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5890–5904, 2022.
[24] Gartner, Market Guide for Insider Threat Management Solutions 2023, Gartner Inc., Stamford, CT, 2023.
[25] P. S. Dandekar, "Evaluating Human-Centric Cyber Maturity in Indian SMEs and Enterprises," International Journal of Computer Science and Information Technologies, vol. 14, no. 2, pp. 122–129, 2023.
[26] S. F. Rodrigues, "Integrating Human Factors into Cybersecurity Education: A Curriculum Framework," Springer Education & Information Technologies, vol. 28, pp. 425–443, 2023.
[27] D. Kumar and R. Jain, "Machine Learning for Behavioral Intrusion Detection: A Comparative Study," Elsevier Computers & Security, vol. 110, Article 102433, 2023.
[28] CERT-EU, Cybersecurity Threat Landscape Report 2023, European Union Agency for Cybersecurity, Brussels, 2023.
[29] S. Zawoad and R. Hasan, "Security Analytics for Human-Driven Threats in Cloud Environments," IEEE Security & Privacy Magazine, vol. 20, no. 1, pp. 36–45, 2022.
[30] KPMG, India Cybersecurity Outlook Survey Report 2024, KPMG India, Mumbai, 2024.
[31] IBM X-Force, Threat Intelligence Index 2023, IBM Security, Armonk, NY, 2023.
[32] Deloitte, The Human Element in Cyber Risk: Global Enterprise Survey Report 2023, Deloitte Touche Tohmatsu Limited, London, 2023.
[33] PwC, Global Digital Trust Insights 2024, PricewaterhouseCoopers International, London, 2024.
[34] J. Alshamrani, "Zero-Trust Architecture and Insider Threat Management in Cloud Enterprise Systems," IEEE Access, vol. 12, pp. 34112–34129, 2024.
[35] ENISA, Human Factors in Cybersecurity Awareness Campaigns: Good Practice Guide, European Union Agency for Cybersecurity, Heraklion, 2022.
[36] S. Pathak, "AI-Augmented Awareness Training for the Banking Sector: A Case-Based Analysis," International Journal of Computer Applications, vol. 182, no. 3, pp. 92–101, 2023.
[37] A. Banerjee, "Analyzing Policy Compliance Behaviour in Indian IT Firms: A Longitudinal Study," International Journal of Engineering Trends and Technology, vol. 70, no. 9, pp. 152–161, 2022.
[38] A. Saini, "Human-Centric Design Principles for Cyber Defense Systems," Springer IFIP Advances in Information and Communication Technology, vol. 660, pp. 88–104, 2023.
[39] CERT-IN, Cyber Awareness Handbook for Employees and Organisations, Government of India, 2023.
[40] NIST SP 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology, 2023.
[41] G. Johnson and C. Renaud, "The Human Firewall: Reimagining Cybersecurity Awareness for the Modern Enterprise," Elsevier Computers & Security, vol. 127, Article 103088, 2024.
[42] A. Alotaibi, "Evaluating Security Culture Maturity in Small and Medium Enterprises," IEEE Transactions on Engineering Management, vol. 71, no. 2, pp. 312–325, 2024.
[43] S. Chatterjee and S. Paul, "Multi-Layer Insider Threat Detection using Hybrid Machine Learning Models," Springer AI & Ethics, vol. 3, no. 4, pp. 1201–1218, 2023.
[44] N. Patil, "Cybersecurity Behaviour Risk Index for Indian Industry: Development and Validation," Indian Journal of Cyber Security, vol. 13, no. 4, pp. 221–231, 2024.
[45] C. Nguyen, "Behavioral Anomaly Analytics in Cloud Security Environments," Elsevier Journal of Network and Computer Applications, vol. 206, Article 103478, 2023.
[46] J. Thomas, "Ethical Artificial Intelligence for Insider Threat Detection: Balancing Surveillance and Privacy," Proc. IEEE Ethics in AI Symposium, pp. 44–52, 2024.
[47] EY, Global Information Security Survey (GISS) 2024, Ernst & Young Global Limited, London, 2024.
[48] NIST, Cybersecurity and Privacy Reference Tool (CPRT) Version 2.0, National Institute of Standards and Technology, 2024.
[49] OECD, Cybersecurity Risk Governance in the Digital Economy, Organisation for Economic Co-operation and Development, Paris, 2023.
[50] PwC India, Building a Human-Centric Cyber Culture in Indian Enterprises, PricewaterhouseCoopers India, New Delhi, 2024.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[51] Gartner, Emerging Technologies in Insider Threat Detection and Prevention, Gartner Inc., Stamford, CT, 2025.
[52] McKinsey & Company, The Human Factor in Digital Trust Transformation, McKinsey Global Institute, New York, 2024.
[53] R. Banerjee and K. Sen, "AI and Human Cognition in Cyber Defense: A Neuro-Symbolic Approach," IEEE Intelligent Systems, vol. 39, no. 1, pp. 25–34, 2025.
[54] CERT-IN, Cyber Security Guidelines for Government Entities and Critical Infrastructure, Government of India, 2023.
[55] SRMIST Research Centre, Employee Behavior Risk Index (EBRI) for Indian SMEs: Pilot Study Report, SR Institute of Management and Technology, Lucknow, 2024.
[56] A. Tripathi and S. Mishra, "Social Media Manipulation and Spear-Phishing in Indian Digital Business Environments," International Journal of Engineering and Computer Education Technology, vol. 14, no. 5, pp. 78–92, 2023.
[57] IIT Delhi Cybersecurity Laboratory, Behavioral Cybersecurity Research Report 2023, Indian Institute of Technology Delhi, New Delhi, 2023.
[58] World Economic Forum, Global Cybersecurity Outlook 2024, World Economic Forum, Geneva, 2024.
[59] Accenture, State of Cybersecurity Resilience 2024: Navigating the Human Factor, Accenture PLC, Dublin, 2024.
[60] IBM Corporation, Future of AI in Cyber Threat Detection and Response, IBM Institute for Business Value, Armonk, NY, 2025.

APPENDIX A: CERT-IN GUIDELINE EXTRACTS

The following extracts from the CERT-IN Guidelines for Insider Threat Mitigation (2024) are reproduced for reference purposes in accordance with the Government of India's open-access policy for cybersecurity awareness materials:

A.1 Mandatory Insider Threat Programme Requirements (CERT-IN, 2024)

All organisations classified as Critical Information Infrastructure (CII) operators and IT service providers with annual turnover exceeding INR 10 crore are required to:

- Establish a dedicated Insider Threat Working Group (ITWG) comprising HR, IT Security, Legal, and Senior Management representatives.
- Implement User and Entity Behaviour Analytics (UEBA) tools or equivalent anomaly detection mechanisms for all privileged user accounts.
- Conduct mandatory cybersecurity awareness training for all employees at minimum quarterly, with documented assessment outcomes.
- Maintain incident logs for insider-related events for a minimum period of 3 years and report critical incidents to CERT-IN within 6 hours of discovery.

A.2 Social Engineering Awareness Mandates

Organisations are required to implement phishing simulation exercises at least bi-annually and maintain records of employee response rates. Employees with click-through rates exceeding 25% in consecutive simulations must be enrolled in mandatory remediation training within 30 days.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

APPENDIX B: EMPLOYEE BEHAVIOUR RISK INDEX (EBRI) TEMPLATE

B.1 EBRI Computation Instrument

Table B.1: EBRI Assessment Template

EBRI Component	Weight (%)	Assessment Method	Score Range
Phishing Susceptibility Rate	35	Bi-annual simulation click-through rate	0–100 (higher = riskier)
Policy Compliance Inverse Score	25	SIEM compliance log analysis (100 - compliance%)	0–100
Training Non-Completion Rate	20	LMS training module completion records	0–100
Access Anomaly Frequency	20	UEBA anomaly flagging rate per 30-day period	0–100

EBRI Score Interpretation: 0–25 = Low Risk; 26–50 = Moderate Risk; 51–75 = High Risk; 76–100 = Critical Risk. Employees in the High or Critical Risk bands are automatically enrolled in the HCCF's adaptive PFA training pathway.

APPENDIX C: CYBERSECURITY AWARENESS SURVEY INSTRUMENT

C.1 Employee Cybersecurity Awareness Questionnaire

This instrument was administered to 102 IT/ITES professionals for baseline EBRI measurement. Responses were collected on a 5-point Likert scale (1 = Never, 5 = Always) unless otherwise indicated.

- Q1. How frequently do you complete mandatory cybersecurity awareness training modules? (1–5 scale)
- Q2. Do you verify sender identity before clicking links in unsolicited emails? (Yes / No / Sometimes)
- Q3. How confident are you in identifying a phishing email? (1–5 scale)
- Q4. Have you ever clicked a link in a suspicious email? (Yes / No / Unsure)
- Q5. How often do you use personal devices for work-related tasks without VPN? (1–5 scale)
- Q6. Are you aware of your organisation's data classification policy? (Yes / No / Partially)
- Q7. How often do you share work credentials with colleagues for convenience? (1–5 scale)
- Q8. Have you received formal training on insider threat awareness? (Yes / No)
- Q9. How would you rate your organisation's cybersecurity culture? (1–5 scale)
- Q10. Do you report suspicious emails or security incidents to your security team? (Always / Sometimes / Never)

RESEARCH SUMMARY

Title

Human-Centric Approaches to Cybersecurity: Insider Threat Mitigation and Social Engineering Risk in Digital Business Environments

Problem Statement

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The prevalence of human-origin cybersecurity incidents — accounting for over 74% of global breaches — necessitates frameworks that address behavioural, cognitive, and organisational dimensions of security risk, complementing existing technical controls. No unified, empirically validated, human-centric framework exists for Indian digital enterprises and SMEs.

Research Objectives

- Analyse behavioural and psychological factors driving insider threats and social engineering success.
- Design the Human-Centric Cybersecurity Framework (HCCF) integrating HBA, AITP, and PFA components.
- Validate HCCF performance through AI model evaluation and retrospective case study analysis.
- Map HCCF alignment with CERT-IN, ISO/IEC 27001, NIST SP 800-53, and DPDP Act 2023.

Methodology

Mixed-method descriptive-experimental design: systematic literature review (50+ sources, 2020–2025); AI model development (Random Forest, SVM, LSTM) trained on 15,902-record composite dataset; retrospective case analysis (Twitter 2020, Indian PSU 2022); structured awareness survey (n=102); compliance mapping against four cybersecurity frameworks.

Key Results

Table S.1: Summary of Key Performance Results

Performance Metric	Baseline	HCCF Result	Improvement
Insider Threat Detection Accuracy	78% (IDS)	92.1%	+17%
False Positive Rate	18%	5.2%	-71%
Mean Time to Detect (hours)	72	28	-61%
Employee EBRI Score (mean)	47.3	38.8	-18%
Phishing Click-Through Rate	34.7%	22.1%	-36%
Policy Compliance Rate	61.2%	78.9%	+29%
CERT-IN Compliance Alignment	N/A	100%	Full alignment

Major Contributions

- HCCF: First unified human-centric cybersecurity framework validated for Indian digital business and SME environments.
- EBRI: Composite quantifiable metric for individual and organisational human cybersecurity risk measurement.
- Closed-Loop Adaptive Defence: Empirically demonstrated progressive improvement through integrated AI-awareness feedback cycle.
- Compliance Matrix: Unified alignment across CERT-IN, ISO, NIST, and DPDP Act — enabling audit-ready deployment.

Conclusion

The HCCF demonstrates that integrating human behavioural analytics, AI-driven threat detection, and adaptive policy feedback produces measurably superior cybersecurity outcomes compared to technology-centric approaches. The framework is scientifically grounded, empirically validated, compliance-aligned, and practically deployable — particularly for Indian SMEs, financial institutions, and government entities.

Future Scope

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Future research will extend the HCCF through: Explainable AI integration; Federated learning for privacy-preserving deployment; Cross-cultural EBRI validation; Longitudinal behavioural impact assessment; IoT ecosystem extension; and AI ethics governance framework development.