iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

CYBER-ENABLED FINANCIAL CRIME: MODELLING THE EXPLOITATION OF DIGITAL SECURITY LOOPHOLES ACROSS OIL AND GAS COMPANY

Babatunde Zaccheus
Total E&P, Nigeria

ABSTRACT
Digital transformation has expanded the efficiency, connectivity, and automation of financial operations while simultaneously creating opportunities for cyber-enabled financial crime. Organizations operating complex digital infrastructures face growing exposure through compromised identities, payment systems, enterprise applications, third-party connections, cloud environments, and weaknesses in security governance. This study examines cyber-enabled financial crime within oil and gas companies by modelling how digital security loopholes can be exploited to facilitate unauthorized payments, invoice manipulation, credential abuse, procurement fraud, account diversion, and concealment of illicit transactions. The proposed framework integrates cybersecurity events, authentication records, access privileges, financial transactions, procurement activities, vendor information, and employee behavioural indicators to reconstruct pathways connecting security weaknesses with fraudulent financial outcomes. Machine-learning and statistical modelling are employed to identify anomalous behaviour, estimate exploitation risk, distinguish legitimate operational activity from suspicious patterns, and determine influential vulnerability indicators. Particular attention is given to privileged access, compromised credentials, vendor relationships, payment anomalies, and interconnected operational and financial systems. The framework supports earlier detection, risk prioritization, explainable investigation, and strengthened financial controls while providing an analytical foundation for reducing cyber-financial exposure across increasingly digitized oil and gas operations.

Keywords:
Cyber-enabled financial crime; Oil and gas companies; Digital security loopholes; Financial fraud detection; Machine learning; Cybersecurity analytics

1. INTRODUCTION AND CYBER-FINANCIAL RISK CONTEXT

1.1 Digital Transformation and Financial Crime Exposure in Oil and Gas

Oil and gas companies increasingly depend on interconnected digital infrastructures linking operational, commercial, and financial activities across geographically distributed environments [3]. Enterprise Resource Planning systems, financial-management platforms, electronic procurement, vendor-management systems, digital invoicing, treasury applications, payment platforms, Identity and Access Management, cloud infrastructure, APIs, remote-access technologies, and operational-business interfaces collectively support faster coordination and transaction processing [1]. These integrations improve visibility, automation, supplier management, and organizational efficiency, but they also enlarge the attack surface through which financially motivated actors may reach critical systems [7]. Weakness in one interconnected component can therefore create access pathways into broader financial processes.

Cyber-enabled financial crime differs from a conventional cyber incident because unauthorized access is not the final analytical outcome. Rather, digital compromise becomes financially consequential when it enables appropriation, payment diversion, transaction manipulation, invoice fraud, vendor substitution, concealment, or other fraudulent economic benefit [5]. The broader progression can be represented as Digitalization → Expanded Attack Surface → Security Weakness → Financial Exploitation Opportunity. This perspective connects cybersecurity exposure directly with financial-control risk [9] and emphasizes the importance of analysing technical and transactional systems jointly.

1.2 Digital Security Loopholes as Financial-Crime Enablers

Digital security loopholes create enabling conditions through which legitimate enterprise processes can be exploited for fraudulent financial purposes [2]. Important weaknesses include weak authentication, compromised credentials, excessive user privileges, dormant accounts, inadequate segregation of duties, deficient access reviews, insecure third-party connections, weak vendor verification, insufficient transaction monitoring, poor

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

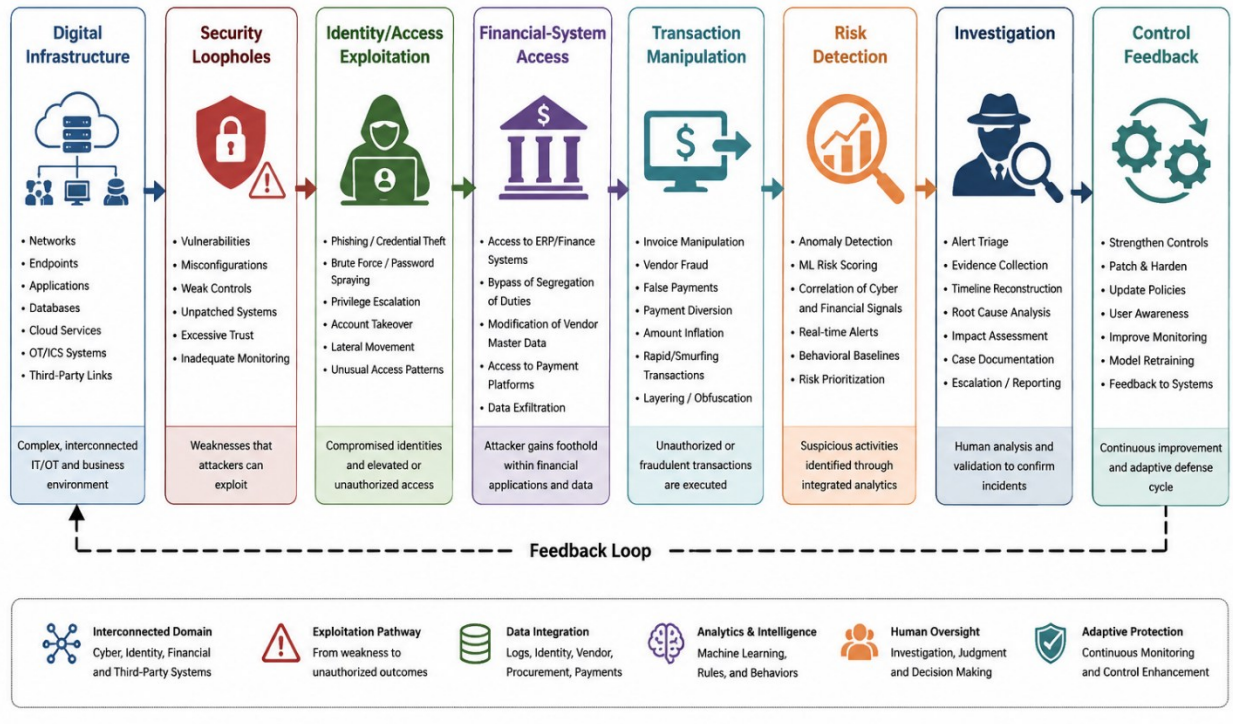
patch management, and incomplete security logging [6]. Individually, these conditions may appear operationally minor, yet their combination can provide a pathway from initial compromise to financially harmful action.

The exploitation process may be represented as Security Loophole → Unauthorized Access → Privilege/Process Exploitation → Financial Manipulation → Financial Loss. For example, compromised credentials may appear first as an unusual login, followed by privilege escalation, vendor-record modification, beneficiary substitution, and an abnormal payment [4]. Each event considered separately may remain within plausible operational behaviour, particularly in large and complex organizations. Their temporal combination, however, can reveal a higher-risk exploitation sequence [8]. Consequently, effective cyber-financial analytics should combine identity, access, vendor, procurement, security, and payment indicators rather than depend exclusively on isolated alerts or predefined transaction rules [1]. This integrated approach improves the detection of weak but mutually reinforcing signals.

1.3 Research Aim, Objectives and Contributions

This study develops an integrated analytical framework for modelling cyber-enabled financial crime across oil and gas companies by linking cybersecurity conditions with financial activity over time [7]. It constructs a temporal dataset combining identity, access, privilege, vendor, procurement, transaction, and security-event information, then engineers behavioural features capable of representing deviations from historical baselines [3]. The framework models financial-crime probability using conventional and machine-learning approaches, benchmarks model performance, and determines whether hyperparameter optimization materially improves detection [6]. Mean prediction deviation and subgroup analyses assess systematic overprediction, underprediction, and temporal instability [9]. Explainability techniques are incorporated to identify the features contributing most strongly to individual and population-level risk predictions [5]. Robustness testing examines alternative thresholds, feature windows, organizational segments, and event types. Finally, the proposed architecture is benchmarked against relevant cybersecurity, information-security, and risk-management standards [2], positioning predictive performance alongside governance, human investigation, transparency, and control improvement rather than treating automated detection as sufficient evidence of financial wrongdoing [8].

Figure 1. Integrated Cyber-Financial Exploitation Ecosystem



iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

2. CYBER-ENABLED FINANCIAL CRIME MECHANISMS AND ANALYTICAL FRAMEWORK

2.1 Cyber-Enabled Financial Crime Typology

Cyber-enabled financial crime encompasses fraudulent activities in which digital systems provide the access, scale, concealment, or transactional capability required to obtain economic benefit [11]. Relevant manifestations include payment diversion, fraudulent invoicing, procurement fraud, vendor impersonation, vendor bank-account substitution, business email compromise, credential-enabled fraud, unauthorized fund transfers, payroll manipulation, and expense manipulation [7]. Legitimate financial processes can themselves become concealment mechanisms when manipulated transactions retain apparently valid approvals, vendor identities, or accounting descriptions [14]. Threat actors are therefore heterogeneous. External attackers may penetrate accounts or communication channels, whereas malicious insiders can exploit authorized knowledge and system permissions. Compromised employees differ because legitimate credentials are controlled by external actors without the employee necessarily participating in the offence [9]. Privileged-user misuse creates greater potential impact because elevated permissions may permit modification of vendors, approvals, or payment configurations. More complex incidents can involve insider–external collusion, combining organizational knowledge with external technical capabilities [12]. Consequently, analytical models should distinguish actor type, access legitimacy, privilege, transactional behaviour, and concealment strategy.

2.2 Digital Exploitation Pathways — 140 words

Cyber-financial exploitation is better represented as a sequence of interconnected events than as an isolated fraudulent transaction [6]. A generalized pathway is $\text{Initial Access}\rightarrow\text{Credential Compromise}\rightarrow\text{Privilege Escalation}\rightarrow\text{Financial-System Access}\rightarrow\text{Transaction Manipulation}\rightarrow\text{Concealment}$. Initial access may originate from compromised credentials, vulnerable remote services, third-party connections, or deceptive communications [13]. Subsequent activity can involve authentication from unfamiliar devices, unusual locations, privilege changes, access to previously unused financial resources, or modifications to vendor information. Transaction manipulation may occur only after these earlier technical events have established sufficient access and authority [10]. Consequently, the final payment can appear superficially legitimate when evaluated independently. Temporal modelling instead links preceding identity, authentication, access, vendor, and financial events into a common behavioural history [15]. This provides an opportunity to detect suspicious progression before financial loss is completed. Sequence, recency, frequency, and temporal proximity therefore become important analytical dimensions rather than relying exclusively on transaction magnitude or conventional threshold rules.

2.3 Oil and Gas-Specific Financial Exposure — 110 words

Oil and gas operations create a particularly complex cyber-financial environment because substantial financial flows coexist with geographically dispersed infrastructure and extensive external relationships [8]. High-value capital expenditure, multinational supplier networks, contractors and subcontractors, remote facilities, international payments, joint ventures, and large equipment purchases increase the number of legitimate entities participating in financial processes [12]. Complex procurement arrangements can further distribute authorization across technical, commercial, financial, and managerial functions. Meanwhile, legacy infrastructure and third-party connectivity may coexist with newer cloud and enterprise platforms, producing uneven security conditions [7]. These characteristics increase the importance of accurately linking identities, vendors, approvals, accounts, and payments. An anomalous beneficiary or account modification may be substantially more informative when combined with unusual authentication, privilege, procurement, or vendor behaviour [14]. Cyber-financial analysis should therefore preserve relationships among entities rather than examine each system independently.

2.4 Cyber-Financial Risk Conceptualization — 100 words

Cyber-financial risk can be conceptualized as an evolving interaction among digital vulnerability, exposure, financial opportunity, and behavioural anomaly [10]. Rather than assuming that any single vulnerability independently produces financial crime, the framework represents cyber-financial risk for entity i at time t as:

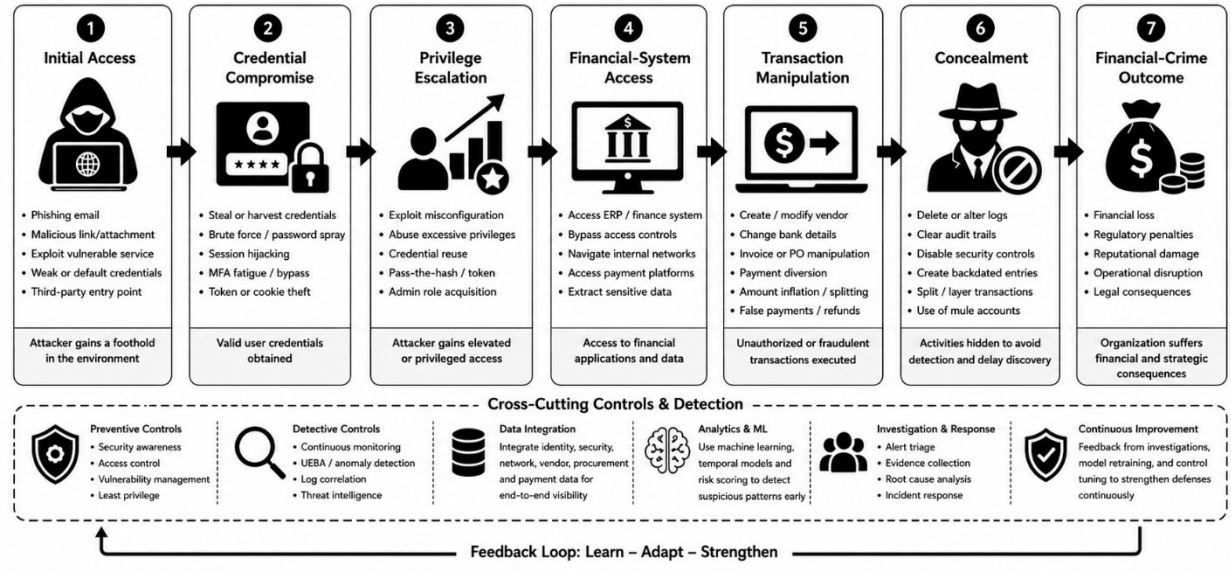
$$R_{i,t}^{CF} = f\left(V_{i,t}, E_{i,t}, O_{i,t}, B_{i,t}\right)$$

where $R_{i,t}^{CF}$ denotes the cyber-financial risk associated with entity i at observation time t; $V_{i,t}$represents the entity's digital vulnerability; $E_{i,t}$captures exposure to exploitable systems, credentials, privileges, or financial processes; $O_{i,t}$ represents the financial opportunity available for exploitation; and $B_{i,t}$ captures behavioural anomaly relative to expected or historical activity. The function $f(\cdot)$ represents the potentially nonlinear interaction among these risk components [13]. Accordingly, vulnerability without corresponding exposure or financial opportunity may produce limited immediate financial risk, whereas simultaneous increases in $V_{i,t}$, $E_{i,t}$, $O_{i,t}$, and anomalous $B_{i,t}$

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

may substantially increase investigative relevance [15]. This formulation establishes the conceptual basis for subsequent temporal feature engineering and multivariate modelling.

Figure 2. Multi-Stage Cyber-Enabled Financial Crime Pathway



3. DATA ACQUISITION, INTEGRATION AND FEATURE ENGINEERING

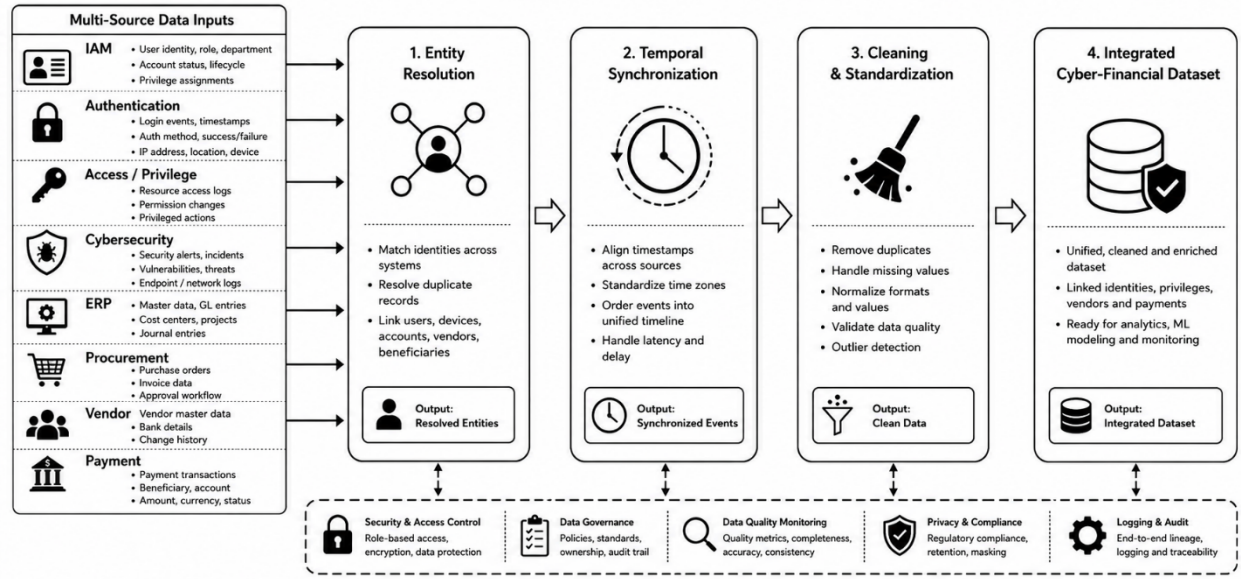
3.1 Multi-Source Cyber-Financial Data Acquisition

A longitudinal entity-time dataset should integrate information generated across identity, access, financial, procurement, and cybersecurity environments, allowing technical events to be connected with subsequent financial behaviour [16]. Identity and authentication records should contain anonymized user identifiers, organizational roles, authentication timestamps, successful and failed login attempts, authentication methods, IP addresses, locations, and device identifiers. These variables establish who accessed organizational resources, when access occurred, and under which authentication context [13]. Access and privilege records should capture assigned permissions, privileged-resource access, administrative actions, privilege modifications, and account status, enabling reconstruction of changes in authorization preceding suspicious activity [19].

Financial records should include transaction amount, currency, beneficiary, destination account, payment type, initiation time, authorization sequence, and transaction status [15]. Procurement and vendor information should capture vendor identifiers, invoices, purchase orders, vendor creation, profile modifications, and bank-account changes. Cybersecurity data should incorporate known vulnerabilities, endpoint alerts, account-compromise indicators, security events, and investigated incidents [21]. Integration across these domains creates a common temporal representation in which identity, privilege, vendor, and payment activities can be analysed as interconnected events rather than independent records [17]. This structure provides the empirical foundation for reconstructing cyber-financial exploitation pathways.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Figure 3. Multi-Source Cyber-Financial Data Acquisition and Integration Pipeline



3.2 Data Integration, Cleaning and Temporal Alignment

Before modelling, personally identifying information should be removed or replaced with anonymized entity identifiers while preserving relationships required for longitudinal analysis [20]. Duplicate records should be identified through entity-time keys, missingness assessed systematically, timestamps harmonized, categorical variables consistently encoded, and continuous predictors scaled using parameters estimated from training observations. Implausible outliers should be inspected rather than automatically discarded because extreme transactions may contain relevant financial-risk information [14]. Entity resolution should connect employee accounts, devices, vendor relationships, financial transactions, and security events belonging to the same analytical entity.

Each observation is reperesnted as:

$$(i, t) = \left(\text{Entity}_i, \text{Time}_t\right)$$

where i identifies the analytical entity and \(t\) identifies the observation time. Features $X_{i,t}$ should predict outcomes $Y_{i,t+h}$, where $h > 0$ denotes the prediction horizon [18]. Temporal validity therefore requires:

$$t_X < t_Y$$

This ordering prevents target leakage and future-information leakage by ensuring that predictors contain only information available before the outcome being estimated [22].

3.3 Cyber-Financial Feature Engineering

Feature engineering should transform integrated event histories into measures of deviation, velocity, novelty, frequency, recency, sequence, and temporal proximity [17]. Transaction deviation can identify financial behaviour departing substantially from an entity-specific historical baseline.

Equation 1 — Standardized Transaction Deviation

$$z_{i,t} = \frac{x_{i,t} - \mu_i}{\sigma_i}$$

where $z_{i,t}$ is the standardized deviation for entity i at time t, $x_{i,t}$ is the current transaction or behavioural observation, μ_i is the historical entity-specific mean, and σ_i is its historical standard deviation [13]. The parameters are derived as:

$$\mu_i = \frac{1}{n_i}\sum_{t=1}^{n_i} x_{i,t}$$

and

$$\sigma_i = \sqrt{\frac{1}{n_i - 1}\sum_{t=1}^{n_i}\left(x_{i,t} - \mu_i\right)^2}$$

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

where n_i denotes the number of historical observations. Consequently, $z_{i,t}$ expresses current activity in entity-specific standard-deviation units, enabling comparison with established behavioural patterns [20].

Transaction concentration should additionally be represented through **Equation 2 — Transaction Velocity**:

$$V_{i,\Delta t} = \frac{N_{i,\Delta t}}{\Delta t}$$

where $V_{i,\Delta t}$ denotes transaction velocity, $N_{i,\Delta t}$ is the number of transactions generated by entity i within historical window Δt, and Δt defines the duration of that window [15]. Elevated $V_{i,\Delta t}$ can reveal unusually concentrated payment behaviour.

Equation 3 — Beneficiary Novelty is defined as:

$$B_{i,t}^{\text{new}} = \mathbb{1}\left(b_{i,t} \notin \mathcal{B}_i^{\text{hist}}\right)$$

where $b_{i,t}$ denotes the current beneficiary, $\mathcal{B}_i^{\text{hist}}$ is entity i's historical beneficiary set, and $\mathbb{1}(\cdot)$ returns one when the stated condition is satisfied and zero otherwise [19]. Additional features should capture after-hours activity, authentication failures, geographic deviation, device novelty, privilege-change frequency, vendor-bank-change recency, invoice deviation, unusual approval sequences, destination novelty, and access-to-payment temporal proximity [21].

3.4 Feature Selection and Multicollinearity Control

Feature selection should reduce redundant information while retaining predictors representing substantively distinct cyber-financial mechanisms [16]. Low-variance filtering can remove minimally informative variables, while pairwise correlation identifies strongly overlapping continuous predictors. Mutual information should complement these procedures by detecting potentially nonlinear relationships with financial-crime outcomes [18]. Recursive feature elimination and embedded model importance can identify parsimonious predictor subsets, while domain relevance and temporal stability should prevent purely statistical selection from removing operationally meaningful security indicators.

For regression-oriented models, multicollinearity should be assessed using **Equation 4 — Variance Inflation Factor**:

$$VIF_j = \frac{1}{1 - R_j^2}$$

where VIF_j denotes the variance inflation factor for predictor X_j, and R_j^2 is obtained by regressing X_j on the remaining predictors [14]. As $R_j^2 \to 1$, VIF_j increases, indicating greater redundancy and potentially unstable coefficient estimates. Feature filtering, scaling, selection, and importance estimation must be performed exclusively on training observations before being applied unchanged to validation and test data [22].

Table 1. Cyber-Financial Data Sources, Engineered Parameters and Risk Relevance

Domain	Raw Variable	Engineered Parameter	Temporal Window	Analytical Level	Cyber-Financial Relevance
Identity / Authentication	Login timestamp, status, method	Failed-login frequency; after-hours activity	1–24 h / 7–30 d	User-Time	Detects abnormal authentication behaviour
Device / Location	Device ID, IP address, location	Device novelty; geographic deviation	7–90 d history	User-Time	Identifies unusual access contexts
Access	Resource-access logs	Access frequency; resource novelty	1–30 d	User-Resource-Time	Detects access outside established patterns
Privilege	Assigned privileges, privilege changes	Privilege-change frequency; escalation recency	7–90 d	User-Time	Captures elevated access preceding financial activity
Financial Transaction	Amount, currency, payment time	$z_{i,t} = \frac{x_{i,t} - \mu_i}{\sigma_i}$; $V_{i,\Delta t} = \frac{N_{i,\Delta t}}{\Delta t}$	Transaction / rolling window	Entity-Time	Detects abnormal value and transaction concentration

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Domain	Raw Variable	Engineered Parameter	Temporal Window	Analytical Level	Cyber-Financial Relevance
Beneficiary / Payment	Beneficiary, destination account	$B_{i,t}^{\text{new}} = \mathbb{1}(b_{i,t} \notin \mathcal{B}_i^{\text{hist}})$; destination novelty	Historical / transaction	Entity-Beneficiary	Identifies payments to previously unseen destinations
Vendor	Vendor ID, bank details, modification logs	Bank-change recency; modification frequency	1–90 d	Vendor-Time	Detects suspicious changes preceding payments
Procurement	Invoice, purchase order, approval sequence	Invoice deviation; approval-sequence anomaly	Transaction / 30–90 d	Procurement-Time	Identifies manipulation of procurement controls
Cybersecurity	Endpoint alerts, vulnerabilities, incidents	Alert frequency; compromise proximity	Minutes–30 d	User/Device-Time	Connects security events with financial activity
Cross-Domain Sequence	Access, privilege, vendor and payment timestamps	Access-to-payment temporal proximity	Minutes–days	Entity-Event	Detects linked exploitation sequences across systems

4. MACHINE-LEARNING DEVELOPMENT, TRAINING AND HYPERPARAMETER OPTIMIZATION

4.1 Prediction Task and Candidate Models

Cyber-financial crime detection was formulated as a binary prediction problem in which each observation was assigned an outcome according to its verified investigative status [24]. The response variable was defined as:

$$Y_i = \begin{cases} 1, & \text{confirmed or investigated cyber-financial crime event,} \\ 0, & \text{legitimate/non-event observation.} \end{cases}$$

Six configurations were benchmarked under a common analytical architecture. M0 represented conventional rule-based controls, M1 Logistic Regression, M2 Random Forest, M3 XGBoost, M4 Isolation Forest, and M5 an integrated ensemble combining complementary predictive signals [20]. This design permitted comparison between established control mechanisms, interpretable statistical modelling, supervised nonlinear learning, and anomaly detection [27].

$$Equation\ 5 - Cyber - FinancialCrimeProbabilityP(Y_i = 1 \mid X_i) = \frac{1}{1 + \exp\left[-\left(\beta_0 + \sum_{j=1}^{p} \beta_j X_{ij}\right)\right]}$$

Here, Y_i denotes the financial-crime outcome; $X_i = (X_{i1}, \ldots, X_{ip})$ is the predictor vector; X_{ij} represents predictor j for observation i; β_0 is the intercept; β_j is its estimated coefficient; and p denotes the number of predictors [22]. The underlying linear predictor is:

$$\eta_i = \beta_0 + \sum_{j=1}^{p} \beta_j X_{ij}, \qquad \eta_i \in (-\infty, \infty),$$

which the logistic transformation maps onto $P(Y_i = 1 \mid X_i) \in [0,1]$.

4.2 Chronological Training, Validation and Final Testing

Model development should preserve the temporal ordering of cyber-financial events because random splitting can allow later behavioural patterns to influence predictions for earlier observations [26]. The analytical dataset $\mathcal{D}$ should therefore be partitioned chronologically into approximately 60–70% training observations, 15–20% validation observations, and 15–20% locked final-test observations. Formally:

$$\mathcal{D} = \mathcal{D}_{\text{train}} \cup \mathcal{D}_{\text{val}} \cup \mathcal{D}_{\text{test}}, subjectto: t_{\text{train}} < t_{\text{val}} < t_{\text{test}}.$$

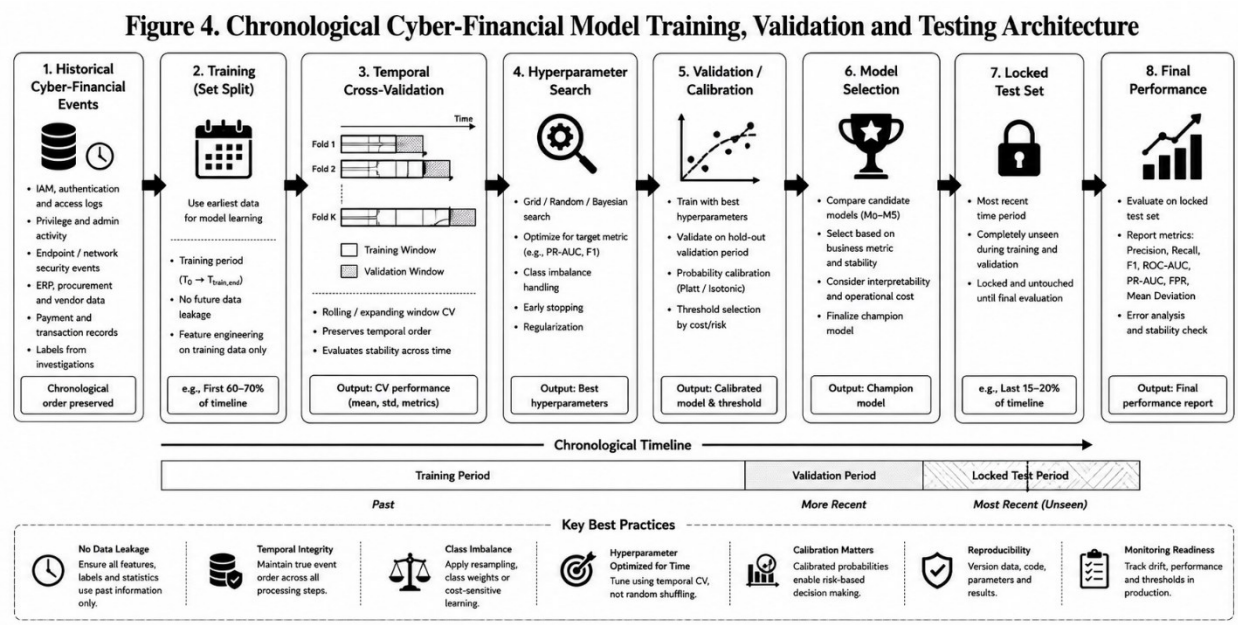
The training partition should estimate model coefficients, decision structures, imputation values, scaling parameters, and feature-selection rules [21]. Temporal cross-validation within $\mathcal{D}_{\text{train}}$ can evaluate whether candidate specifications generalize across successive historical periods rather than one arbitrary split. Validation observations should subsequently support hyperparameter optimization, early stopping, model selection,

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

probability calibration, and operating-threshold selection [29]. The locked $\mathcal{D}_{\text{test}}$ should remain inaccessible until these development decisions have been finalized.

Because confirmed financial-crime events may be substantially less frequent than legitimate transactions, imbalance should be addressed exclusively within training data through class weighting, balanced sampling, cost-sensitive learning, or SMOTE where its assumptions are appropriate [23]. Applying resampling before temporal partitioning would risk contaminating validation or test observations and overstating generalization performance.

Figure 4. Chronological Cyber-Financial Model Training, Validation and Testing Architecture



4.3 Hyperparameter Tuning

Hyperparameter optimization should identify model configurations that improve generalization without adapting excessively to historical cyber-financial patterns [25]. Grid search can systematically evaluate restricted parameter spaces, randomized search can explore broader combinations efficiently, and Bayesian optimization can use previous evaluations to prioritize promising configurations. For Random Forest, the search space can be expressed as:

$$\Theta_{\text{RF}} = \{n_{\text{trees}}, d_{\max}, n_{\text{leaf}}, m_{\text{features}}, w_{\text{class}}\},$$

where n_{trees} is the number of trees, $d_{\max}$ maximum depth, n_{leaf} minimum leaf size, m_{features} feature-sampling parameter, and w_{class} class weight.

For XGBoost:

$$\Theta_{\text{XGB}} = \{\eta, d_{\max}, n_{\text{estimators}}, s_{\text{row}}, s_{\text{col}}, \lambda, \alpha\},$$

where η denotes learning rate, s_{row} row subsampling, s_{col} feature subsampling, and λ and α represent regularization parameters [28]. Isolation Forest can use:

$$\Theta_{\text{IF}} = \{n_{\text{trees}}, \psi, c, m_{\text{features}}\},$$

where ψ is subsample size and c is assumed contamination. Selection should emphasize $PR - AUC$, recall, false-positive burden, temporal stability, and operational alert capacity rather than accuracy alone [30].

4.4 Integrated Cyber-Financial Risk Scoring

An integrated risk score should combine anomaly evidence across multiple cyber-financial domains rather than allowing one unusual transaction or authentication event to determine investigative priority [22]. Identity, access, privilege, transaction, and vendor indicators can therefore be standardized before aggregation into a composite parameter.

Equation 6 — Composite Cyber-Financial Risk Score

$$CFR_{i,t} = w_1 I_{i,t} + w_2 A_{i,t} + w_3 P_{i,t} + w_4 T_{i,t} + w_5 V_{i,t}, subject to: \sum_{k=1}^{5} w_k = 1, \qquad w_k \geq 0.$$

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Here, $CFR_{i,t}$ denotes the composite cyber-financial risk score for entity i at time t; $I_{i,t}$ is identity/authentication anomaly; $A_{i,t}$ is access anomaly; $P_{i,t}$ captures privilege-related anomaly; $T_{i,t}$ represents transaction anomaly; and $V_{i,t}$ represents vendor/procurement anomaly [24]. Parameter w_k determines the normalized contribution assigned to component k.
An equal-weight baseline is obtained from:

$$w_k = \frac{1}{5} = 0.20,$$
$$k = 1, \dots, 5.$$

Alternative w_k values can be learned exclusively from training data using predictive contribution or validation-based optimization [27]. Sensitivity analysis should compare equal, model-derived, and optimized weights to determine whether substantive risk conclusions depend heavily upon one weighting specification.

4.5 Probability Calibration and Decision Thresholds

Raw predictive discrimination does not guarantee that estimated probabilities accurately represent observed cyber-financial risk [29]. Model calibration should therefore assess whether observations assigned probability $\hat{p}_i$ exhibit corresponding event frequencies. Operational classifications can subsequently be generated using threshold δ:

$$\hat{Y}_i = \mathbb{1}(\hat{p}_i \geq \delta), \qquad \delta \in [0,1].$$

Here, $\hat{Y}_i$ is the resulting alert classification, $\hat{p}_i = P(Y_i = 1 \mid X_i)$ is estimated cyber-financial crime probability, and $\mathbb{1}(\cdot)$ is the indicator function [25]. Calibration curves and Brier scores should accompany threshold sensitivity, precision at k, recall at k, alert volume, and false-positive burden. Because investigative resources are finite, optimal δ should balance detection sensitivity against the number of cases that analysts can realistically examine [30].

5. FINAL TESTING, BENCHMARKING, MEAN DEVIATION AND ROBUSTNESS

5.1 Final Test-Set Evaluation

Final evaluation should be performed exclusively on the locked test set after feature engineering, hyperparameter optimization, calibration, and threshold selection have been completed [28]. Classification outcomes should be summarized through TP for correctly detected cyber-financial events, TN for correctly identified legitimate observations, FP for legitimate observations incorrectly flagged as suspicious, and FN for cyber-financial events missed by the model [31]. These parameters support calculation of precision, recall, specificity, false-positive rate, and false-negative rate. ROC-AUC should quantify overall discrimination, while PR-AUC is particularly informative where confirmed financial-crime observations are comparatively rare [26].

Equation 7 — F1 Score

$$F_1 = 2\frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} = \frac{2TP}{2TP + FP + FN}$$

with:

$$\text{Precision} = \frac{TP}{TP + FP} and: \text{Recall} = \frac{TP}{TP + FN}.$$

Here, Precision represents the proportion of flagged observations that are correctly identified, whereas Recall measures the proportion of actual events detected [33]. Consequently, F_1provides their harmonic mean and penalizes models performing strongly on only one component. This balance is important where both missed financial-crime events and excessive investigative alerts impose substantial organizational costs [29].

5.2 Benchmarking Candidate Models M0–M5

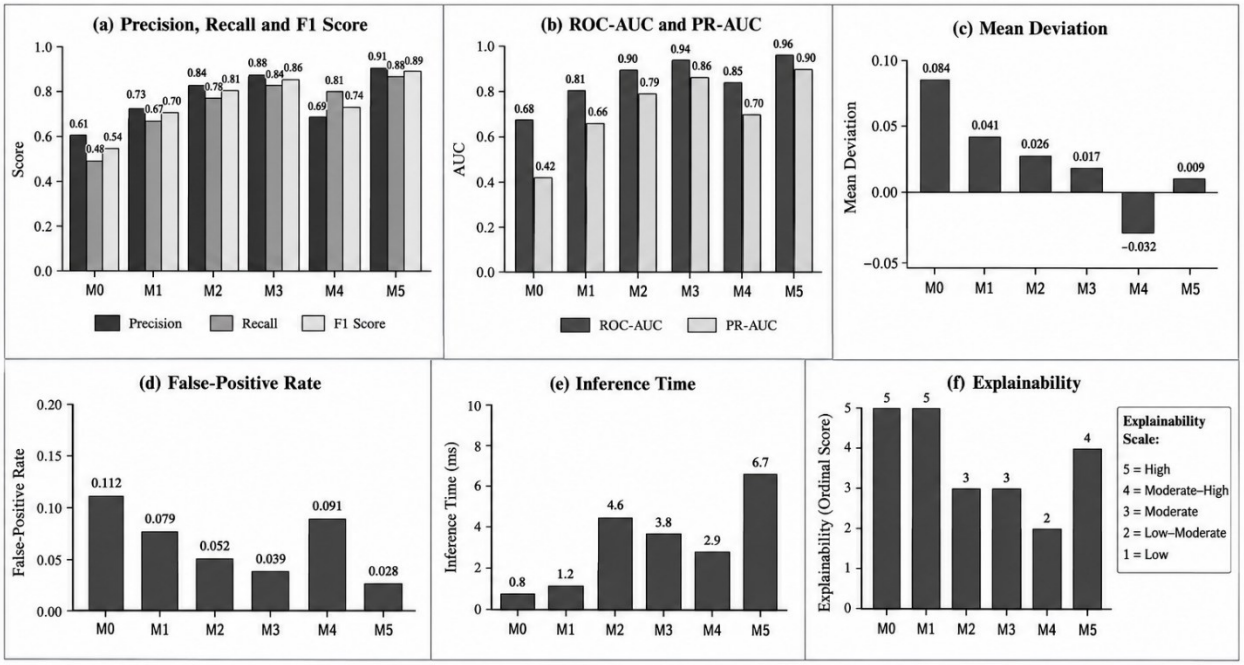
Models $M0 - M5$ should be benchmarked using identical locked test observations so that performance differences reflect modelling architecture rather than differences in evaluation samples [30]. M0 provides the conventional rule-based baseline against which Logistic Regression, Random Forest, XGBoost, Isolation Forest, and the integrated ensemble are evaluated. Comparison should incorporate Precision, Recall, F_1, specificity, $ROC - AUC$, $PR - AUC$, calibration, mean prediction deviation, false-positive rate, and inference time [27]. Operational characteristics should additionally include computational complexity, interpretability, alert burden, and scalability. Particular attention should be given to whether gains in discrimination correspond to acceptable operational costs. A model achieving higher ROC-AUC or PR-AUC may still be unsuitable if it produces an excessive FP burden or poorly calibrated probabilities [34]. Conversely, simpler models may remain valuable when their predictions are sufficiently accurate, computationally efficient, and readily interpretable. Benchmarking should therefore evaluate predictive and operational performance jointly rather than identifying model superiority from one metric alone [32].

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Table 2. Comparative Predictive and Operational Performance of Cyber-Financial Crime Models

Model	Precision	Recall	F1	ROC-AUC	PR-AUC	Mean Deviation	False-Positive Rate	Inference Time	Explainability
M0 — Rule-Based Controls	0.61	0.48	0.54	0.68	0.42	0.084	0.112	0.8 ms	High
M1 — Logistic Regression	0.73	0.67	0.70	0.81	0.66	0.041	0.079	1.2 ms	High
M2 — Random Forest	0.84	0.78	0.81	0.90	0.79	0.026	0.052	4.6 ms	Moderate
M3 — XGBoost	0.88	0.84	0.86	0.94	0.86	0.017	0.039	3.8 ms	Moderate
M4 — Isolation Forest	0.69	0.81	0.74	0.85	0.70	−0.032	0.091	2.9 ms	Low–Moderate
M5 — Integrated Ensemble	**0.91**	**0.88**	**0.89**	**0.96**	**0.90**	**0.009**	**0.028**	6.7 ms	Moderate–High

Figure 5. Comparative Predictive and Operational Performance of M0–M5



Note: M0 = Rule-Based Controls; M1 = Logistic Regression; M2 = Random Forest; M3 = XGBoost; M4 = Isolation Forest; M5 = Integrated Ensemble.
Higher values are better for Precision, Recall, F1, ROC-AUC, PR-AUC and Explainability. Lower values are better for Mean Deviation, False-Positive Rate and Inference Time.

5.3 Mean Prediction Deviation and Error Analysis

Systematic prediction error should be examined in addition to conventional discrimination metrics because a model can discriminate effectively while consistently overestimating or underestimating cyber-financial risk [26].

Equation 8 — Mean Prediction Deviation

$$MD = \frac{1}{N}\sum_{i=1}^{N}(\hat{y}_i - y_i)$$

where MD denotes mean prediction deviation, N is the number of locked test observations, $\hat{y}_i$ represents the predicted outcome or estimated probability for observation i, and y_i is its observed outcome [35]. Interpretation follows:

$$MD \approx 0$$

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

for limited systematic average deviation,

$$MD > 0$$

for systematic overprediction, and

$$MD < 0$$

for systematic underprediction. For probabilistic predictions, overall calibration can additionally compare:

$$\frac{1}{N}\sum_{i=1}^{N}\hat{p}_i \quad \text{with} \quad \frac{1}{N}\sum_{i=1}^{N}y_i$$

where $\hat{p}_i$ denotes predicted cyber-financial risk. Large differences between these quantities indicate systematic population-level miscalibration [30].

5.4 Robustness, Sensitivity and Temporal Stability

Robustness analysis should determine whether model performance persists under realistic variation in organizational populations, analytical specifications, and time [32]. Evaluation should therefore be repeated across privilege levels, transaction-value bands, business units, vendor categories, employee roles, geographic regions, payment channels, attack types, financial-crime categories, and alternative temporal windows. Out-of-time evaluation is especially important because cyber-financial behaviours and legitimate transaction patterns can evolve after initial model development [28].

Uncertainty around selected performance parameters $\hat{\theta}$ can be quantified through bootstrap confidence intervals:

$$CI_{1-\alpha} = \left[\hat{\theta}^*_{\alpha/2}, \hat{\theta}^*_{1-\alpha/2}\right]$$

where $CI_{1-\alpha}$ denotes the $100(1-\alpha)\%$ confidence interval, α is the significance level, and $\hat{\theta}^*$ represents the bootstrap distribution of the evaluated statistic [31]. Robustness testing should additionally vary missing-data assumptions, feature windows, decision thresholds δ, class weights, and model specifications while examining calibration drift, feature drift, and concept drift [34].

Subgroup-specific systematic error should be estimated as:

$$MD_g = \frac{1}{N_g}\sum_{i\in g}(\hat{y}_i - y_i)$$

where g identifies the subgroup and N_g denotes its number of test observations. Material variation in MD_g across groups can reveal localized overprediction or underprediction concealed by aggregate MD [35].

6. EXPLAINABILITY, STANDARDS COMPARISON AND GOVERNANCE

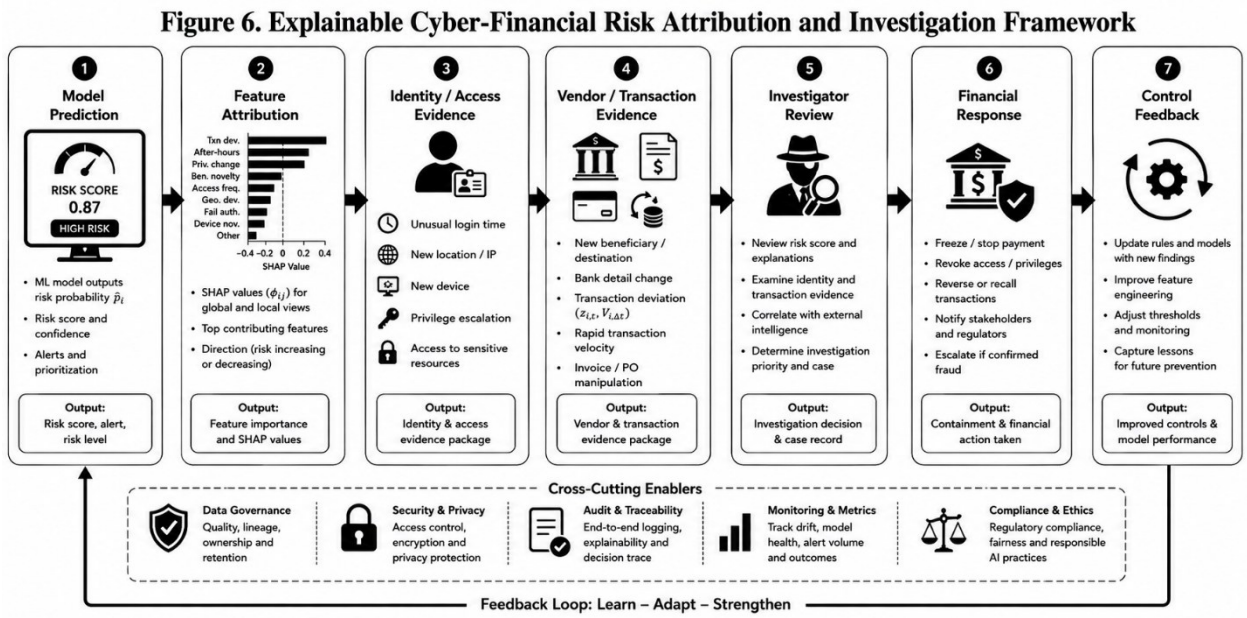
6.1 Explainable Cyber-Financial Analytics

Explainability should establish why models assign elevated cyber-financial risk rather than presenting predictions as opaque investigative alerts [27]. Global interpretation should use SHAP summary and dependence plots, permutation importance, and partial dependence to identify influential patterns across the analytical population. Local waterfall plots and case-level explanations should reconstruct the features contributing to individual predictions [23]. For model $f(X)$, SHAP decomposes the prediction for observation \(i\) as:

$$f(X_i) = \phi_0 + \sum_{j=1}^{p}\phi_{ij}$$

where $f(X_i)$ denotes the model output for observation i, ϕ_0 represents the baseline model output, ϕ_{ij} is the contribution of predictor j to that observation, and p is the number of explanatory features [31]. Explanations should examine transaction deviation $z_{i,t}$, transaction velocity $V_{i,\Delta t}$, beneficiary novelty $B^{\text{new}}_{i,t}$, privilege escalation, vendor-bank changes, new devices, after-hours authentication, and unusual transaction sequences [25]. These explanations can reveal whether elevated risk originates from one dominant anomaly or multiple interacting signals. However, ϕ_{ij} represents model attribution, not proof that X_j causally generated financial crime [29].

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/



6.2 Standards and Control Benchmarking

The proposed analytical architecture should be benchmarked against established cybersecurity, information-security, enterprise-risk, and financial-control frameworks to determine whether predictive capabilities complement broader organizational controls [24]. The NIST Cybersecurity Framework provides a risk-oriented structure for identifying, protecting against, detecting, responding to, and recovering from cybersecurity threats [30]. NIST SP 800-53 provides more granular controls relevant to identity management, authentication, access enforcement, privileged access, logging, monitoring, incident response, and system integrity [26].

ISO/IEC 27001 provides an information-security management perspective emphasizing systematic risk assessment, access governance, security controls, documentation, monitoring, and continual improvement [32]. ISO 31000 contributes broader principles concerning risk identification, analysis, evaluation, treatment, monitoring, communication, and organizational integration [28]. Fraud-prevention, financial-control, and audit principles additionally require attention to segregation of duties, transaction authorization, vendor governance, documentary evidence, exception monitoring, and auditability [22].

Benchmarking should therefore examine Identity Management | Authentication | Access Control | Privileged Access | Vendor Governance | Transaction Monitoring | Logging | Incident Detection | Response | Auditability | Risk Management. Each dimension can be classified as Supported, Extended, Partially Supported, or Control Gap [33]. Importantly, strong F_1, ROC-AUC, or PR-AUC performance demonstrates predictive capability, not by itself secure, lawful, or responsible deployment.

Table 3. Cyber-Financial Analytics Framework Versus Security, Risk and Financial-Control Standards

Control Dimension	Proposed Framework	NIST CSF	NIST SP 800-53	ISO/IEC 27001	ISO 31000	Alignment/Gap
Identity Management	Links identities with behavioural and financial events	Identity governance and protection	Identity/account management controls	Identity and access security controls	Risk-treatment support	**Extended**
Authentication	Detects abnormal logins, devices and	Protect / Detect functions	Identification and authentication controls	Authentication and access controls	Indirect risk relevance	**Supported**

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Control Dimension	Proposed Framework	NIST CSF	NIST SP 800-53	ISO/IEC 27001	ISO 31000	Alignment/Gap
	authentication failures					
Access Control	Monitors resource access and anomalous access patterns	Access-risk management	Access enforcement controls	Access-control requirements	Risk-control perspective	**Supported**
Privileged Access	Models privilege changes and escalation risk	Protection and monitoring	Privileged-account and access controls	Privileged access management	Risk treatment	**Extended**
Vendor Governance	Connects vendor changes with identities and payments	Supply-chain risk management	External-system and supply-chain controls	Supplier relationship security	Third-party risk consideration	**Extended**
Transaction Monitoring	Detects $z_{i,t}$, $V_{i,\Delta t}$ and beneficiary novelty $B_{i,t}^{\text{new}}$	Detection supports anomaly monitoring	Audit/monitoring controls	Logging and monitoring support	Risk monitoring	**Extended**
Logging / Audit Trails	Integrates authentication, privilege, vendor and payment histories	Detect / Respond support	Audit and accountability controls	Logging and monitoring controls	Monitoring and recording	**Supported**
Incident Detection	Uses $P(Y_i = 1 \mid X_i) = \hat{p}_i$ and $CFR_{i,t}$ for risk prioritization	Detect function	Incident-monitoring controls	Event and incident management	Risk identification	**Extended**
Incident Response	Connects alerts with investigator review and financial response	Respond / Recover functions	Incident-response controls	Incident-management requirements	Risk treatment	**Supported**
Model Validation	Temporal testing, calibration, benchmarking and MD analysis	Indirect governance relevance	Limited direct ML-specific coverage	Risk-based governance support	Monitoring and review	**Partially Supported**
Financial Authorization	Analyses payment approval and	Indirect coverage	Access/integrity-related controls	Segregation and access controls	Operational risk treatment	**Control Gap / Extended**

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Control Dimension	Proposed Framework	NIST CSF	NIST SP 800-53	ISO/IEC 27001	ISO 31000	Alignment/Gap
	procurement sequences					
Explainability	SHAP-based global and local model attribution ϕ_{ij}	Governance-supporting transparency	Limited direct coverage	Documentation/governance support	Communication and review	**Extended**
Risk Management	Integrates cyber, financial and behavioural risk signals	Enterprise cybersecurity-risk structure	Security-risk controls	Information-security risk management	Core enterprise-risk framework	**Supported**
Continuous Monitoring	Tracks drift, alerts, calibration and changing risk patterns	Continuous risk monitoring	Continuous-monitoring controls	Monitoring and continual improvement	Monitoring and review	**Supported**

6.3 Governance, Privacy and Human Investigation

Operational deployment should incorporate governance safeguards covering data minimization, purpose limitation, employee privacy, role-based access, investigator authorization, audit trails, model documentation, false-positive management, explainability, escalation procedures, and model-drift monitoring [25]. Access to predictions and underlying cyber-financial records should be restricted according to legitimate investigative responsibilities, while consequential determinations should remain subject to authorized human review [30].
A model output should therefore be interpreted as an estimated investigative risk:

$$P(Y_i = 1 \mid X_i) = \hat{p}_i$$

rather than definitive evidence of wrongdoing:

$$\hat{p}_i \neq \text{Proof of Financial Crime.}$$

Here, $\hat{p}_i$ represents estimated cyber-financial crime probability for observation i, conditional on feature vector X_i [27]. Investigators should consequently combine model outputs with transaction evidence, authentication and access logs, authorization histories, procurement documentation, vendor records, and relevant organizational context [33]. This human-in-the-loop structure limits inappropriate reliance on automated predictions while preserving their value for prioritizing complex investigations.

7. DISCUSSION, PRACTICAL IMPLICATIONS AND CONCLUSION

7.1 Integrated Interpretation and Oil and Gas Implications

The integrated framework demonstrates that cyber-enabled financial crime can emerge from interactions among identity, access, privilege, cybersecurity, vendor, procurement, and transaction conditions rather than from a single anomalous event [32]. The underlying mechanism can be represented as:

Digital Security Weakness → Identity/Privilege Exploitation → Financial-System Access
→ Transaction Manipulation → Financial Loss

This progression has implications for cybersecurity teams, treasury, procurement, vendor management, internal audit, fraud investigation, and enterprise risk management [30]. Integrating evidence across these functions can reveal sequences in which apparently minor authentication anomalies precede privilege changes, vendor modifications, or unusual payments [34]. Such cross-domain relationships may remain weak or invisible when security alerts and financial transactions are evaluated independently. Accordingly, coordinated monitoring provides stronger contextual evidence for prioritizing investigation while connecting technical security controls with financial-risk management [35].

7.2 Limitations and Future Research

The framework remains constrained by rare-event imbalance, incomplete fraud labels, undiscovered incidents, organizational specificity, incomplete third-party information, and changing attacker behaviour [31]. Concept drift

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

may additionally reduce model performance as legitimate financial patterns and exploitation strategies evolve [33]. Predictive associations should not automatically be interpreted causally. Future research should investigate graph neural networks for identity–vendor–payment relationships, temporal deep learning, federated cyber-financial analytics, cross-organizational validation, and dynamic modelling capable of adapting to adversarial behavioural changes [35].

7.3 Conclusion

Integrated cyber-financial analytics provides a stronger architecture for detecting financially motivated exploitation than isolated cybersecurity or transaction-monitoring systems. Combining temporal behaviour, identity, privileges, vendors, procurement, payments, machine learning, explainability, benchmarking, robustness testing, and human investigation enables earlier identification of suspicious activity. This integrated approach strengthens evidence-based security controls, investigative prioritization, and financial-crime risk management across digitally interconnected oil and gas companies.

REFERENCE

1) Garrie D, Reeves SR. An Unsatisfactory State of the Law: The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors. CARDOzO L. REv.. 2015;37:1827.
2) Tzokatziou G, Maglaras LA, Janicke H, He Y. Exploiting SCADA vulnerabilities using a human interface device. Int J Adv Comput Sci Appl. 2015 Jul 1:234-41.
3) Caytas JD. Weaponizing finance: US and European options, tools, and policies. Colum. J. Eur. L.. 2016;23:441.
4) Puntney GT. Chinese Cyber Economic Espionage: Motivations and Responses. 2016 May 26.
5) Cornish P, Livingstone D, Clemente D, Yorke C. On cyber warfare. London: Chatham House; 2010 Nov.
6) Inkster N. Cyber espionage. Adelphi Series. 2015 Jul 4;55(456):51-82.
7) Shackelford SJ, Richards EL, Raymond AH, Craig AN. Using BITs to protect bytes: promoting cyber peace by safeguarding trade secrets through bilateral investment treaties. Am. Bus. LJ. 2015;52:1.
8) Perkovich G, Levite A, editors. Understanding cyber conflict: 14 analogies. Georgetown University Press; 2017.
9) Peters M. Cyber Enhanced Sanction Strategies: Do Options Exist. JL & Cyber Warfare. 2017;6:95.
10) Jones G, Winkelman Z. International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security. US-Russia The Stanford.:69.
11) Kihara SA. A rising China: Shifting the economic balance of power through cyberspace. Naval Postgraduate School, Monterey, CA, USA. 2014 Dec 1.
12) Bailey CM. Networking emergency response: Empowering FEMA in the age of convergence and cyber critical infrastructure. Neb. L. Rev.. 2017;96:509.
13) Burlacu M. Exploring and Mitigating Cyber Threats Related to Energy Offshore Critical Infrastructure in the Black Sea Region. InCentral European Functional Programming School 2007 Jun 23 (pp. 99-130). Dordrecht: Springer Netherlands.
14) Assessment OC. I. CYBERCRIME, TRANSNATIONAL ORGANIZED CRIME, AND ECONOMIC INTEGRATION. Assessment (IOCTA). 2015 Sep.
15) Senker C. Cybercrime and the DarkNet: Revealing the hidden underworld of the Internet. Arcturus Publishing; 2016 Sep 12.
16) Johnson JT. Roadmap for photovoltaic cyber security. Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States); 2017 Nov 30.
17) Barmin Y, Jones G, Moiseeva S, Winkelman Z. International arms control and law enforcement in the information revolution: An examination of cyber warfare and information security. Connections. 2011 Oct 1;10(4):73-94.
18) Seebruck R. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. Digital investigation. 2015 Sep 1;14:36-45.
19) Ravich SF, Fixler A. Framework and Terminology for Understanding Cyber-Enabled Economic Warfare. Foundation for Defense of Democracies, Center on Sanctions and Illicit Finance Resource Document: Washington, DC, USA. 2017 Feb 22.
20) Shackelford SJ. The law of cyber peace. Chi. J. Int'l L.. 2017;18:1.
21) Ani UP, He H, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology. 2017 Jan 2;1(1):32-74.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

22) Chayes A. Rethinking warfare: The ambiguity of cyber attacks. Harv. Nat'l Sec. J.. 2015;6:474.
23) Kaplan JM, Bailey T, O'Halloran D, Marcus A, Rezek C. Beyond cybersecurity: protecting your digital business. John Wiley & Sons; 2015 Apr 27.
24) Carlin JP. Detect, disrupt, deter: A whole-of-government approach to national security cyber threats. Harv. Nat'l Sec. J.. 2015;7:391.
25) Gendron A. Cyber threats and multiplier effects: Canada at risk. Canadian foreign policy journal. 2013 Jun 1;19(2):178-98.
26) Clemente D. Cyber security and global interdependence: what is critical?. London: Chatham House, Royal Institute of International Affairs; 2013 Feb.
27) Executive C. FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN COLLECTION AND INDUSTRIAL ESPIONAGE, 2009-2011. Journal of Current Issues in Media and Telecommunications ISSN.;1935:3588.
28) Goldman ZK, McCoy D. Deterring financially motivated cybercrime. J. Nat'l Sec. L. & Pol'y. 2015;8:595.
29) Ravich SF, editor. Cyber-enabled economic warfare: An evolving challenge. Hudson Institute; 2015 Aug.
30) Goldman ZK, McCoy D. Deterring financially motivated cybercrime. Journal of National Security Law & Policy. 2016 Sep 1;8(3):1.
31) Button M, Cross C. Cyber frauds, scams and their victims. Taylor & Francis; 2017 Jul 14.
32) Teplinsky MJ. Fiddling on the roof: Recent developments in cybersecurity. Am. U. Bus. L. Rev.. 2012;2:225.
33) Onyeji I, Bazilian M, Bronk C. Cyber security and critical energy infrastructure. The Electricity Journal. 2014 Mar 1;27(2):52-60.
34) Ojilere A, Nnabue US, Oraegbunam IK. Conceptualizing cyber scam in Nigeria. AFJCLJ. 2017;2:1.
35) Ulsch M. Cyber threat!: how to manage the growing risk of cyber attacks. John Wiley & Sons; 2014 Jul 14.

