

RESEARCH ARTICLE

 OPEN ACCESS | Double-Blind Peer Reviewed

Cybersecurity Risk Management and Digital Trust in FinTech Organizations: A Critical Review of Threats, Frameworks, and Trust-Enabling Mechanisms

Jean Luc^{1*}, Andi Lynn²¹ Division of Information Technology & Sciences, Champlain College, USA² Division of Information Technology & Sciences, Champlain College, USA

*Corresponding author: Jean Luc | Email: jean.luc@champlain.edu |

ARTICLE INFO

Article History

Received: 12 June 2026**Revised:** 24 July 2026**Accepted:** 17 August 2026**Published:** 02 September 2026

Keywords

Cybersecurity,
Risk Management,
Digital Trust, Financial services.
Digitization, Fintech
Organizations,

How to Cite

J. Luc and A. Lynn, "Cybersecurity risk management and digital trust in FinTech organizations: A critical review of threats, frameworks, and trust-enabling mechanisms," J. Appl. Technol., Intell. Comput. Syst. (JATICS), vol. 2, no. 2, pp. 38–52, 2026.

ABSTRACT

The digitization of financial services has been transformed by FinTech which has introduced digital payments, platform lending, open banking and algorithmic advice. The same architectural characteristics that facilitate this speed and scale—API-centric design, cloud reliance and dependence on third parties—also expand the cyber attack surface. This review explores the relationship between cybersecurity risk management and digital trust in the context of FinTech organizations in a critical manner. It draws on peer reviewed studies, international standards, regulatory instruments and industry reports and combines (i) the structure of the FinTech attack surface and what is known about threats and losses, (ii) the main risk management frameworks and quantitative models, (iii) the consolidating regulatory landscape, and (iv) the behavioral and technical aspect of digital trust. The review then presents an integrated Risk – Trust Nexus framework that connects the governance, technical controls and assurance mechanisms to the customer, partner and regulatory trust beliefs of competence, integrity and benevolence. The synthesis shows that trust requires risk management maturity but is not the only factor in trust – transparency, demonstrated resilience and credible incident handling are also key to trust. There are still significant lack of elements in place, such as lack of loss data, insufficient measurement of third-party and concentration risk, empirical evidence on trust metrics is limited, and the governance of AI-powered security tooling. Finally, a research agenda for practitioners, regulators and scholars is outlined.

INTRODUCTION

Financial technology (FinTech), or FinTech for short, is now part of the core of the financial system, rather than just on the margins. Payment wallets, digital-only lenders, robo-advisers, crypto-asset exchanges, and embedded-finance platforms now take on roles that were once exclusive to licensed institutions and do it in ways that conventional institutions can't keep up with – both in speed and in costs [1], [2]. This evolution can be termed a post-crisis paradigm where technology, regulatory changes and changing consumer expectations all contribute [1]. Lee and Shin describe the FinTech ecosystem as a chain of start-ups, incumbents, technology developers, governments and customers whose business models rely on the use of data and platform effects [2].

The very elements that make FinTech appealing, such as API-first design, cloud-native systems, quick cycles of release and integration with third-party services, increase the attack surface. Supervisors have taken notice: the Basel Committee's evaluation of the FinTech developments has included the operational, cyber and third-party risk management as a priority for banks and supervisors in the face of increasingly widespread digital business models [3]. The economic impact is significant. According to the 2024 IBM study, the average financial-sector data breach cost is USD 6.08 million, which is approximately 22% higher than the industry average [4]. The density of interconnectedness between financial services can lead to an incident at one entity to spread to counterparties and, in some cases, to threaten the financial stability of the financial system [5].

But Cyber Risk of FinTech is not just a technical or financial issue. The users of these wherewithal cannot look into the systems in which they place their money and identity; they must trust on the sign of trustworthiness. Digital trust, defined as the trust that stakeholders have in the organization's capacity and willingness to secure data, transactions and identities is thus both a requirement for and a result of proven security and governance [6],[7]. Breaches undermine that trust and create expenses that go beyond remediation, including to customers, companies, the broader financial industry and, at the far end of the spectrum, to economies. [8].

In the existing literature, the relevant aspects are generally analyzed separately: Security standards and frameworks, economic and quantitative models of cyber risk, regulatory compliance, and trust theory in information systems. There are few contributions that link them in a FinTech-specific way. This article fills in that gap. It has four impacts:

- a structured map of the FinTech attack surface, together with the current evidence on threats and losses;
- a comparative assessment of the leading risk management frameworks, standards, and quantitative approaches;
- an analysis of the evolving regulatory regime, with emphasis on operational resilience and third-party oversight; and
- a synthesis of trust theory and technical trust enablers, culminating in an integrated Risk–Trust Nexus framework (previewed in Fig. 1), a set of testable propositions, and a research agenda.

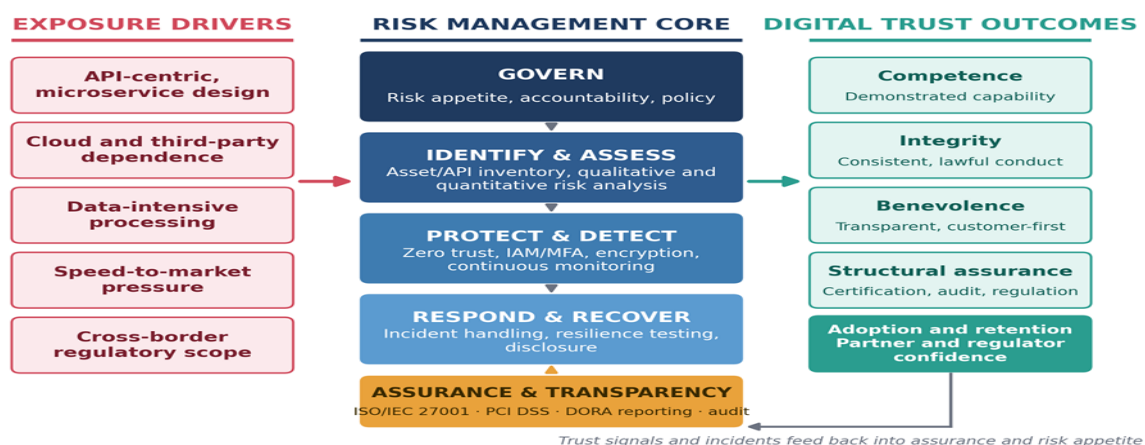


Fig. 1: The Risk–Trust Nexus framework developed in this review. Exposure drivers shape the risk management core; the core, reinforced by assurance mechanisms, generates the trust beliefs on which adoption and confidence depend, and trust signals feed back into governance.

The rest of the article is divided into the following sections. The review approach is detailed in Section II. Section III describes the FinTech ecosystem and attack surface and IV reviews the threat landscape, loss evidence. Section V contrasts risk management frameworks, Section VI discusses quantification and security economics, and Section VII looks at the regulatory landscape. Section VIII and IX discuss digital trust and its enabling technologies, while Section X introduces the integrated framework and Section XI and XII address open challenges and conclude.

REVIEW APPROACH

The article is of a structured narrative review design which is appropriate for a field where evidence is spread out among academic articles, technical standards, regulatory documents and industry telemetry. Four types of evidence streams were identified: (i) peer-reviewed research within the information systems, security economics, and financial technology fields; (ii) international and national standards and technical guidance; (iii) legislative and supervisory instruments; and (iv) industry and public-sector reports with empirical loss and incident data. The scope and the selection criteria are summarized in Table I.

Criterion	Description
Topical scope	Cybersecurity risk management, cyber resilience, and digital trust as they apply to FinTech and financial-services organizations.
Evidence types	Peer-reviewed articles, standards, regulations, supervisory guidance, and industry incident or loss reports.
Inclusion	Direct relevance to risk governance, assessment, control, resilience, regulation, or trust; authoritative issuing body or transparent method.
Exclusion	Vendor marketing without disclosed methodology; opinion pieces without evidence; documents superseded by a later edition of the same standard.
Analytical lens	Thematic synthesis across four themes: attack surface and threats; frameworks and quantification; regulation; digital trust and its enablers.
Temporal focus	Emphasis on 2014–2025, with foundational theoretical and economic works retained irrespective of date.

Table I: Scope And Selection Criteria Of The Review

Two cautions apply. Firstly, the figures reported by industry are often convenience or self-selected samples, and emphasis can be influenced by vendor incentives; these figures are used here to give an indication, but are not definitive [4, 9]. Second, there are differences in regulatory instruments from jurisdiction to jurisdiction. The discussion focuses on EU and international standard-setter materials as they are the clearest on operational resilience requirements for financial entities; readers should align the results with their country's requirements.

THE FINTECH ECOSYSTEM AND ITS ATTACK SURFACE

STRUCTURAL CHARACTERISTICS

There are many dimensions of FinTech firms, and they all have some structural characteristics that shape their cyber risk. The first is about API-centric integration. The revised Payment Services Directive (PSD2) imposes the obligations on ASIs to make account information and payment initiation available to the authorized third parties via interfaces [10]. The latter is reliance on cloud infrastructure and on specialist service providers, and translates many security concerns to contract, assurance, and concentration concerns. The third is data intensity: behavioral, transactional and sometimes biometric data are used for scoring and personalization, adding value to the data for attackers and elevating privacy concerns in the event of breach. The fourth is 'rapid iteration' where frequent releases reduce the amount of time available to conduct a security review. Partnerships, sponsor-bank deals, and marketplaces are examples of interdependence between ecosystems, the fifth of which is discussed.

All these attributes combine to create a new perimeter for security, one that is distributed across a series of identities, tokens, data streams and contractual relationships. The Basel Committee highlights that the rise of FinTech changes the risk profile of banks, including through reliance on third parties and new data flows, and encourages supervisors to adjust their approaches to reflect these changes [3].

SEGMENT-SPECIFIC EXPOSURE

Not all FinTech segments are created equal. Table II correlates the representative segments with their cyber exposure, and to illustrative controls discussed later in this article.

Segment	Representative activities	Dominant cyber exposure	Illustrative controls
Digital payments and wallets	Instant transfers, card-not-present payments, mobile wallets	Account takeover; payment fraud; cardholder-data compromise	Strong customer authentication [10]; PCI DSS controls [11]; ML fraud scoring [12]
Open banking and API platforms	Account aggregation, payment initiation	API abuse; token theft; authorization-flow weaknesses	Hardened OAuth 2.0 profiles [13]; consent management; rate limiting
Digital lending and marketplaces	Algorithmic credit scoring, peer-to-peer lending	Identity fraud; privacy breaches; manipulation of scoring models	Data protection by design [14]; model governance; identity proofing
Wealth, trading, and robo-advice	Brokerage applications, algorithmic advice	Credential stuffing; availability attacks; market-manipulation vectors	Multi-factor authentication; resilience testing [15]
Crypto-assets and ledgers	Exchanges, custody, smart-contract platforms	Private-key compromise; smart-contract flaws; insider misuse	Key management and multi-party custody; independent code audit [16]
Embedded finance and BaaS	Banking-as-a-service, insurtech, RegTech	Third-party concentration; supply-chain compromise	ICT third-party risk management [17]

Table II: Fintech Segments, Dominant Cyber Exposure, And Illustrative Controls

Two cross-cutting observations follow from this mapping. First, identity is the common denominator: across segments, the most frequent route to harm runs through the compromise or misuse of credentials, tokens, and privileged access. Second, the more a firm’s value proposition rests on integration, the more its risk posture is determined by parties it does not control. Both observations recur in the frameworks and regulations reviewed below.

THREAT LANDSCAPE AND EVIDENCE ON LOSSES

PRINCIPAL THREAT CATEGORIES

Attackers targeting FinTech organizations target them and do opportunistic attacks. There are five large groups in the literature and in the incident reporting. Phishing, session hijacking, credential stuffing, and credential theft are all examples of credential-based attacks, which target the weakest link in the identity chain. In fact, a non-malicious human element was involved in about two-thirds of all breaches (68%), highlighting the ongoing importance of social engineering and error [9]. The use of vulnerabilities is becoming more prevalent as an initial access point: according to the same report, exploiting vulnerabilities as an entry point has increased from roughly 77% in the year before to 14% of all breaches [9]. Ransomware and extortion merge encryption and data theft with availability and are a favorite attack against payment and trading platforms. A third party or supply chain compromise enables attackers to get to many downstream companies via one service provider. Loss due to insider misuse or error is still a significant issue. The potential to reduce the cost of convincing phishing and impersonation is also anticipated to add to the pressures at hand for identity verification and customer authentication as a result of the use of generative AI.

LOSS EVIDENCE

The financial services sector is a top culprit when it comes to losses resulting from breaches, according to a series of industry studies that have found evidence. Financial services is a top industry when it comes to losses stemming from breaches, according to evidence found in a series of industry studies. In 2021–2024, the financial industry had an average of 63% of its cost trends matching the cross-industry average for

that period (see Fig. 2(a)), and the breaches in that industry were on average 23% longer in 2024 than the breaches across all industries (see Fig. 2(b)). The average price of the financial industry increased from USD 5.72 million in 2021 to USD 6.08 million in 2024, staying above the global average for the period. Despite identifying breaches earlier (168 days compared to the global average of 194 days) and controlling them earlier (51 days compared to 64 days), exposures were still identified in near 6 months, a long time compared to the time taken by automated attacks to achieve their objectives [4]. In the same study, malicious attacks were responsible for roughly 50% of financial-sector breaches, with the remaining ones attributed to IT failures and human error [4].

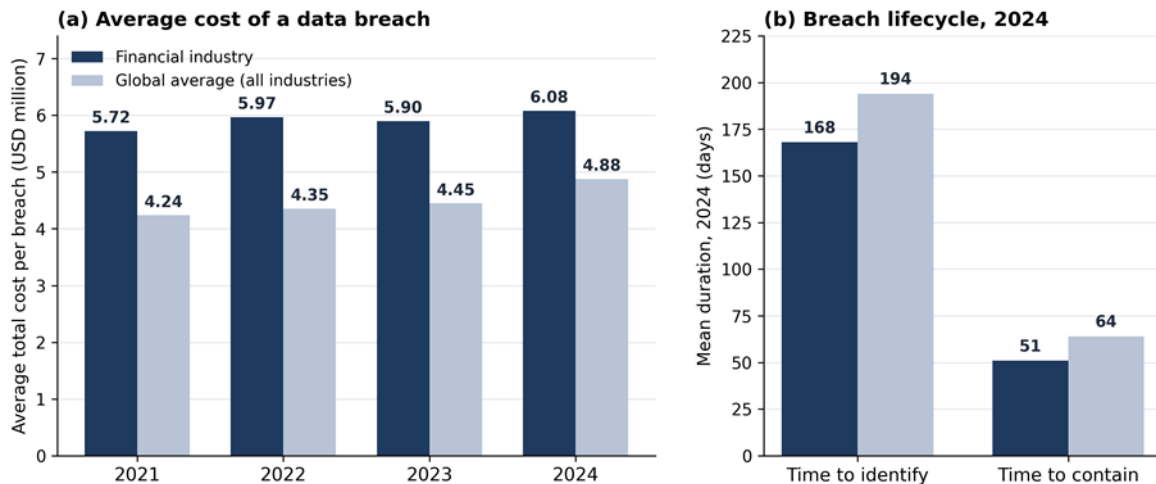


Fig. 2: Cost and duration of data breaches. (a) Average total cost per breach, financial industry versus global cross-industry average, 2021–2024. (b) Mean time to identify and contain a breach, 2024. Data: IBM Cost of a Data Breach Report 2024 [4].

The same study showed that the organizations that use AI and automation extensively in their security efforts had significantly lower average breach costs (USD 3.84 million, compared to USD 5.72 million for those that do not use them) — though this correlation is statistical and may be due to the fact that adopters are likely to be more security-mature on average.

SYSTEMIC AND MACRO-FINANCIAL DIMENSIONS

One of the aspects of financial-sector cyber risk that is unique is that it can have a systemic impact. Kopp et al. state that cyber risk has characteristics similar to other systemic risks: they depend on common factors, are highly interconnected, and they suffer from market failures like information asymmetry and underinvestment in security [5]. While noting the fragility of the underlying data, Bouveret's quantitative framework estimates possible average annual losses of 10% of the net income of banks around the world, significantly higher in extreme cases [18]. The authors in Lagazio et al. examine a multi-level perspective distinguishing the impact at the firm level, the financial sector level, and the national level economies, and demonstrate that the firm-level cost accounting approach underestimates the total impact [8]. The arguments of the FinTech companies—typically smaller and more focused than their corporate counterparts—suggest that the private incentives for investment in security could be sub-optimal, a subject which is explored further in Section VI.

CYBERSECURITY RISK MANAGEMENT FRAMEWORKS AND STANDARDS

Organizations seldom develop cyber risk management from the ground up; they have specific frameworks and standards to acquire that provide them a shared set of terminology, control catalogs, and assurance mechanisms. This section highlights those relevant to FinTech.

NIST CYBERSECURITY FRAMEWORK 2.0

The NIST Cybersecurity Framework (CSF) 2.0 breaks down cybersecurity outcomes into six functions: Govern, Identify, Protect, Detect, Respond and Recover [19]. Govern introduces the concept of risk strategy, risk roles, risk policy and supply-chain risk management as a cross-cutting function and marks the beginning of the transformation of cybersecurity from a technical function into an enterprise risk function [19]. The framework also includes Profiles (current and target outcomes) and Tiers (level of rigor for risk governance). The activities that are relevant to the FinTech field are displayed as functions in the

Fig. 3. It has an outcome-based, non-prescriptive nature that works well with a diverse set of FinTech organizations, but it is not certifiable and its control selection is left up to the adopting organization.

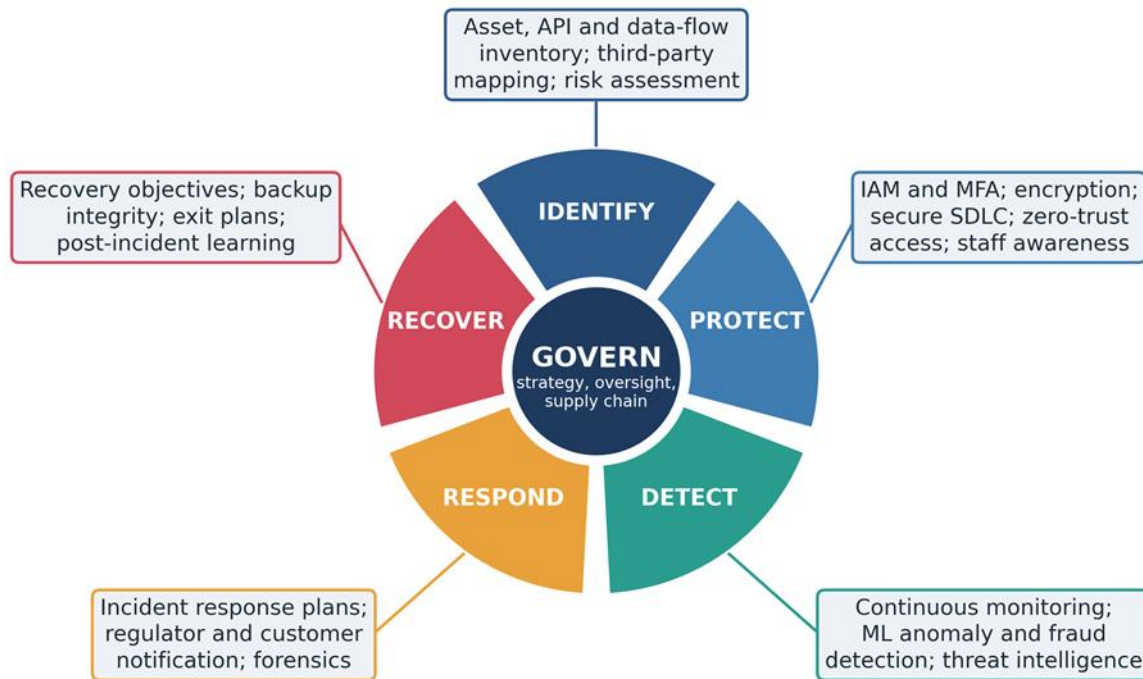


Fig. 3: NIST CSF 2.0 functions [19] with FinTech-relevant activities. Govern is depicted at the center because it informs every other function. Activity examples are the authors' illustration.

ISO/IEC 27001 AND ISO/IEC 27005

The ISO/IEC 27001:2022 gives the requirements for an information security management system (ISMS) and can be certified by an independent body. In a business-to-business FinTech partnership, where vendor due diligence is a frequent occurrence, certification serves as an outside endorsement of management-system maturity, particularly valuable. In 2022, the Annex A control set was merged into four themes (organizational, people, physical, and technological) [20]. The standard ISO/IEC 27005:2022 provides guidance for identifying, analyzing, evaluating and treating information security risks [21]. One recognized limitation is that certification scope can be drawn very tightly and a statement of scope should be read in conjunction with a certificate.

NIST SP 800-30 RISK ASSESSMENT

NIST SP 800-30 Revision 1 is a broadly accepted risk assessment process that consists of preparation, conduct, communication and maintenance, and defines risk as a function of threat events, vulnerabilities, likelihood and impact [22]. It is transparent and it is flexible: it can be used to represent qualitative, semi-quantitative and quantitative scales. The limitations of the method are that it is sensitive to the quality of the inputs for threat and impact assessment and might be subject to different rates from different assessors.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a contractual requirement for businesses that handle, process, or pass card information. Version 4.0 contains 12 main requirements, enhances the authentication requirements, and adds a customized approach which allows entities to satisfy the expressed purposes with other controls [11]. The standard is clear and measurable, but it is limited to include account data; compliance to the cardholder data environment does not guarantee the rest of the enterprise.

OPERATIONAL RESILIENCE PRINCIPLES

Basel Committee Principles for Operational Resilience define the concept of operational resilience as the ability to operate critical functions in the presence of disruption and outline expectations in relation to governance, operational risk management, business continuity and testing, mapping interdependencies, dependency management of third parties, incident management and cyber and ICT resilience [15]. The

principles move the focus from preventing all incidents to maintaining critical services within tolerances, a concept that is very similar to the value customers of digital financial services care about.

THIRD-PARTY AND SUPPLY-CHAIN RISK MANAGEMENT

The line between the enterprise and its service providers is also blurred for most FinTech companies, as cloud-hosting, payment processing, identity verification, data aggregation and core-banking services are generally provided by third parties. In line with this, CSF 2.0 positions the governance of supply-chain risk management under the Govern function [19] and the Basel principles call on firms to inform their operational resilience plans of interdependencies and manage third-party dependencies [15]. These expectations are translated to concrete commitments in the form of a register of information on contractual relationships with third-party information and communication technology providers, contractual commitments and exit strategies [17]. Here are three ‘real-world’ points. First, the level of due diligence must match the criticality of the provider, with a critical provider getting more rigorous examination, monitoring and audit rights than a peripheral provider. Second, focus should be on the level of the firm's critical services and not just on individual contracts as there can be multiple contracts utilizing the same infrastructure. Third, plans for exiting and substitutions require testing not just documentation because an untested plan will not provide much confidence during an actual outage. The Basel Committee's FinTech assessment already predicted that dependence on third parties will be a key characteristic of the new business models [3].

COMPARATIVE VIEW

Table III shows a comparison of the instruments in terms of nature, focus and suitability for FinTech. There is no single instrument that will do the job. In practice, companies integrate an outcome-based governance framework, a management system that can be certified for assurance, a methodology for identifying, assessing and prioritising risk and sector-specific needs for regulatory compliance.

Instrument	Nature	Primary focus	Strengths for FinTech	Limitations
NIST CSF 2.0 [19]	Voluntary framework	Outcome-based functions from Govern to Recover; Profiles and Tiers	Scalable; common language for boards and regulators	Not certifiable; control selection left to adopter
ISO/IEC 27001 and 27005 [20], [21]	Certifiable standard and risk guidance	ISMS, risk treatment, continual improvement	External assurance signal for partners and customers	Scope may be narrow; process-heavy for small firms
NIST SP 800-30 [22]	Risk assessment guide	Threat, vulnerability, likelihood, and impact analysis	Transparent; supports qualitative and quantitative scales	Dependent on quality of inputs and assessor judgment
PCI DSS v4.0 [11]	Contractual industry standard	Protection of payment account data	Concrete, testable requirements	Scope limited to account data; compliance is not security
BCBS operational resilience [15]	Supervisory principles	Delivery of critical operations through disruption	Focus on critical services and interdependencies	Principles-based; requires translation into metrics
DORA [17]	Binding EU regulation	ICT risk, incident reporting, testing, third-party oversight	Harmonized obligations; oversight of critical providers	Implementation burden; limited to EU-regulated entities

Table III: Comparison of Selected Frameworks, Standards, And Regulatory Instruments

QUANTIFICATION AND SECURITY ECONOMICS

QUANTITATIVE RISK MODELS

Although qualitative heat maps are still prevalent as they are easy to create and convey, they do not work well for investment decisions and board-level trade-offs. Factor Analysis of Information Risk (FAIR) does just the opposite, breaking the risk down into loss event frequency, loss event magnitude, each of which is further broken down into measurable factors, allowing the expression of scenarios as loss distributions in monetary terms [23]. Woods and Böhme bring together the literature to quantify cyber risk and point to

common issues: data scarcity and bias, inconsistent definitions of loss, and the challenge of model validation for rare events [24]. Bouveret's sector-level estimates show how much potential there is, and how fragile they are, particularly because they rely on assumptions regarding the distribution of losses and the level of reporting [18].

INVESTMENT AND INCENTIVES

There are two complementary insights contributed from the field of security economics. For a large class of probability functions for breaches, Gordon and Loeb prove that the optimum level of investment in protecting an information set is never more than a fixed fraction $1/e$ of the expected loss resulting from a breach [25]. In effect, it appears to be reasonable to allocate less resources to the most vulnerable resources, and to base investment decisions on the sensitivity of the vulnerability to spending, and not on vulnerability itself. Anderson and Moore highlight the fact that many security failures are not caused by a lack of technology, but by misaligned incentives, externalities and information asymmetry [26]. These arguments are relevant for FinTech, since customers have to absorb part of the cost of the breach, and since for smaller organizations it is a pressing budget problem.

RISK TRANSFER AND CYBER INSURANCE

Insurance is sometimes offered as an alternative way of investment control. In theory it removes some of the financial burden and, if offered for what security practices are actually observed, may offer an incentive to improve security practices. In fact the data problems which plague quantification also plague actuarial pricing [24] and the "information asymmetry" and "moral hazard" issues traditionally found in security economics are relevant as well [26]. Insurers are also exposed to aggregation risk as a vulnerability or a failure may lead to a correlated claim on many insureds, with parallels to systemic risk arguments in the financial sector [5]. In the case of FinTech, therefore, it is best to think of insurance as a way of covering tail and residual losses rather than replacing preventative and resilience controls and to review terms, exclusions and sub-limits with reference to the scenarios quantified in the risk assessment.

TOWARD A HYBRID PRACTICE

The literature/practice suggests a hybrid approach. A wide risk register can be screened using qualitative screening at low cost, both in terms of cost and in terms of time, as per NIST SP 800-30 or ISO/IEC 27005 [21] [22]. The most important and most severe scenarios (e.g. loss of critical payment rail, compromise of a signing key, failure of a concentrated cloud provider) can then be quantified, say with FAIR, with ranges and with explicit documentation of assumptions [23]. Quantification is most useful when it can inform decisions around risk appetite, insurance coverage and prioritizing control; least when it yields an unearthing of spurious precision.

REGULATORY AND COMPLIANCE LANDSCAPE

There is an overlapping set of legislative, supervisory and contractual requirements on which FinTech firms rely. This review is summarized in chronological order in Fig. 4.

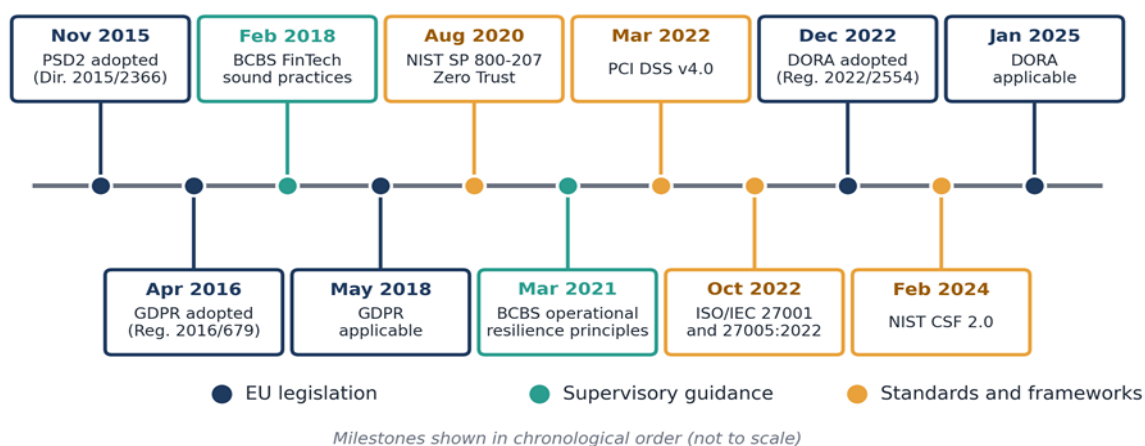


Fig. 4: Milestones in the regulatory, supervisory, and standards landscape relevant to FinTech cyber risk [10], [14], [3], [27], [15], [11], [20], [17], [19].

PAYMENT SERVICES AND DATA PROTECTION

The open banking market and the security requirements of APIs and strong customer authentication for electronic payments that came with it were based on the revised Payment Services Directive (PSD2) [10]. General Data Protection Regulation (GDPR) calls for appropriate technical and organizational measures for securing personal data, for favouring data protection by design and by default, as well as requiring that the controller notifies the supervisory authority in the event of a personal data breach, if one occurs, within a period of 72 hours after its occurrence [14]. Breach notification is not just a compliance requirement for FinTech companies; it is actually the time when trust with their stakeholders is at its highest risk.

DIGITAL OPERATIONAL RESILIENCE

The most recent, and most comprehensive instrument, is the Digital Operational Resilience Act (DORA). It sets a standard for ICT risk management, ICT-related incident management and reporting, digital operational resilience testing, managing ICT third-party risk and sharing information between financial entities [17]. In particular, it establishes an oversight mechanism for critical ICT third-party providers, recognising that concentration in shared providers is a system-level exposure which can only be addressed as a whole system and not by individual firms [17]. The regulation is in alignment with the Basel approach to operational resilience that is being discussed at the international level by the Basel Committee [15].

COMPLIANCE, SECURITY, AND TRUST

One of the constant challenges in practice is between compliance and risk-based security. Compliance creates a minimum standard and sets a common language for assurance, but a set of controls at any one moment cannot meet the pace of adversaries. This is evident in PCI DSS: If a business is compliant with PCI DSS, that doesn't mean they are secure outside of PCI DSS. Another barrier for cross-border Fintech enterprises is regulatory fragmentation, with multiple jurisdictions having different definitions of incidents, who is responsible for reporting, and who is required to test. When mapping controls to a single control library, and then to each regime, there is no duplication, and less risk of inconsistent evidence.

DIGITAL TRUST: THEORETICAL FOUNDATIONS

Trust research provides the conceptual link between security controls and stakeholder behavior. According to Mayer et al., trust is the willingness of a party to be vulnerable to the action of another party and they have identified 3 antecedents of perceived trustworthiness namely ability, benevolence, and integrity [6]. McKnight et al. further their study of ecommerce by adding on three categories of trusting beliefs (competence, benevolence, integrity), one category of trusting intentions, and two categories of general disposition to trust (structural assurance, situational normality) [7].

In the context of FinTech, these can be easily understood. Competence is the ability to avert, identify, and recover from an attack. Integrity is consistency with the security and privacy commitments that are made. Benevolence is the practice of customer-focused behavior, especially in the event of an incident. Structural assurance refers to certifications, regulatory oversight, and legal protections that enable stakeholders to trust a company without necessarily knowing the company inside and out, and situational normality to the expectation that the world operates in a predictable and familiar manner. These constructs are then connected with organizational manifestations, enablers and indicative measures in table IV.

Trust dimension	Organizational manifestation	Enablers	Indicative measures
Competence	Capacity to prevent, detect, and recover from attacks	Control maturity; zero-trust architecture [27]; resilience testing [15]	Control-maturity tier; recovery-time achievement; test coverage
Integrity	Consistent adherence to stated security and privacy commitments	Policy enforcement; independent audit; privacy by design [14]	Audit-finding closure rate; policy-exception volume
Benevolence	Customer-centered conduct during and after incidents	Timely notification; redress; transparency reporting	Notification latency; completeness of customer remediation
Structural assurance	Third-party attestations and legal safeguards	ISO/IEC 27001 certification [20]; PCI DSS validation [11]; supervision	Certification scope and currency; supervisory findings

Trust dimension	Organizational manifestation	Enablers	Indicative measures
Situational normality	Environment perceived as familiar and predictable	Consistent authentication experience; predictable alerts	Authentication abandonment; fraud-report rates

Table IV: Mapping Trust Dimensions To Organizational Enablers And Indicative Measures

The following are a few implications that should be highlighted. First, trust is asymmetric, it builds up organically over time, when it is done well, and can very quickly break down upon visible failure, so response quality after an incident is just as important as prevention. Second, there's a trade-off between security and usability. If not designed carefully, friction in authentication can threaten situational normality and lead customers to seek out other authentication methods that are less secure, so design friction must be "calibrated" not "maximal" [10]. Third, trust should be adjusted, not maximized: Trust in an organisation without substantive controls is a risk in itself and that is why credible and verifiable assurance mechanisms rather than reassuring messaging are important.

Trust repair deserves a special mention. Integrity and benevolence are assessed largely by how they are exhibited, so when there is a problem, others are making a judgment about whether the problem is incompetence, lack of interest or bad luck. A prompt, clear, factually accurate response – plus a concrete remediation – will be more likely to be read as integrity and benevolence, while a delayed, minimized, or blaming response will be read as the opposite [6]. A partial buffer is that of institution-based trust, as when customers believe that the institution is regulated and that its counterparties will be liable to them, a loss of trust may not be enough to cause them to stop buying or selling. A minimum standard of transparency is established through regulatory notification processes, such as the 72-hour window under the GDPR and the notification requirements under the DORA [14, 17] which is an opportunity lost for firms to demonstrate that they are being benevolent towards those affected.

TECHNICAL ENABLERS OF DIGITAL TRUST

ZERO TRUST ARCHITECTURE

Instead of trusting, verifying: Zero trust is a security strategy that assumes access is always denied until proven legitimate, even for users on the network's "trusted" perimeter. It is stated in terms of a policy engine and policy administrator which determine access to resources and a policy enforcement point which gates access to resources in NIST SP 800-207 [27]. Zero trust is a perfect match for the operating model for FinTech, where access is provided to employees, contractors, partners and customer applications from outside a fixed perimeter. It also restricts lateral movement following a credential compromise, an area that is considered to be the most common path to damage in Section IV.

IDENTITY, AUTHENTICATION, AND API SECURITY

Delegated authorization protocols are used for open banking and platform integration. The authors of Fett et al. carried out a formal security analysis of OAuth 2.0, uncovering a number of previously unknown attacks and offering solutions to counter them; they show that many common flows are vulnerable to subtle attacks. Together with other strong authentication requirements [10] they support hardened protocol profiles, short-lived and audience-restricted tokens, mutual authentication of parties and ongoing monitoring of the behaviour of the API.

DISTRIBUTED LEDGER AND CRYPTOGRAPHIC ASSURANCE

With DHT, there is a power of tamper-evident record-keeping, shared state with no single trusted operator, and programmable settlement logic. NISTIR 8202 presents a balanced overview of these properties and also emphasizes that they are dependent upon consensus design, key management and governance [16]. Cryptographic assurance requires operational controls and independent code review, and the trustworthiness of a ledger is contingent on immutability, that is, private keys should not be compromised and smart contracts should not contain bugs that lead to irreversible loss.

PRIVACY-PRESERVING ANALYTICS

The more information there is the better fraud and credit models become, but the more information that is shared across institutions, the greater the legal and trust issues. Federated learning is a training method that uses a shared model, which is updated by exchanging updates instead of raw data [28]. This provides a pathway towards a collaborative fraud detection approach that is aligned with the data minimization

and protection-by-design principles [14]. There are some caveats: Model updates may reveal information about training data sets, and federated learning should be used in conjunction with other protections and against the threat model of the deployment.

MACHINE LEARNING FOR FRAUD DETECTION

Real-time transaction scoring is common using machine learning. Realistic fraud detection is not a textbook classification due to the difficulty of class imbalance, changing fraud patterns (concept drift), late and partial labels and the interplay of automated alerts and human investigators and Dal Pozzolo et al. present a learning strategy that addresses these challenges [12]. False positives negatively impact trust, and false negatives allow fraud to go through the door, so model performance is a customer experience and risk measure, and model risk governance should consider detection models as controls that should be tested and change-managed.

INTEGRATED RISK-TRUST NEXUS FRAMEWORK

FRAMEWORK DESCRIPTION

The reviewed strands are combined in Fig. 1. Exposure drivers are listed in the left-hand column: API-centric design, cloud dependency, third-party reliance, data intensity, speed-to-market pressure and cross-border regulatory scope. These drivers trigger a risk management core that follows the core principles of CSF 2.0, which includes governance governing appetite and accountability, identification & assessment being a combination of qualitative and quantitative analysis, protection & detection being zero trust and monitoring controls, and response & recovery being a translation of resilience objectives to tested capability [19, 23, 27]. There are mechanisms of assurance and transparency that transform the internal capability into something external parties can observe such as certification, audit and regulatory reporting [17], [20]. The outcomes of the resulting trust beliefs, as well as adoption, retention and partner and regulator confidence, are presented in the right column and are based on trust theory [6] and [7]. The incidents and trust signals then feed back into to assurance and risk appetite, and creating a closed loop.

PROPOSITIONS FOR FUTURE RESEARCH

The framework produces propositions which can inform empirical studies. These are expressed as hypotheses based on the synthesis and not as facts.

- P1 (Governance moderation). Governance maturity moderates the effect of technical controls on incident likelihood and impact; equivalent controls yield weaker results where accountability and risk appetite are undefined.
- P2 (Demonstrated resilience). Demonstrated, tested recovery capability contributes more to stakeholder trust than the mere absence of publicly known incidents.
- P3 (Transparent response). Timely and transparent incident communication attenuates post-breach loss of trust, mediated by perceived benevolence and integrity.
- P4 (Structural assurance). For stakeholders with limited technical ability to evaluate security, structural assurance partly substitutes for direct evidence of competence, but only where certification scope is clearly disclosed.
- P5 (Concentration). Third-party concentration is a distinct determinant of ecosystem-level trust beyond firm-level controls, because it creates correlated failure modes [5], [17].

CONTROL COVERAGE AGAINST DOMINANT THREATS

A portfolio of controls is shown in relation to the threat categories of Section IV in Fig. 5. The figure is a qualitative synthesis by the authors of the literature and standards reviewed here, to represent a relative mitigating contribution and not measured effectiveness. The pattern supports a “defense in depth” perspective: identity controls are most important when it comes to account takeover, monitoring and detection is a key when it comes to API abuse and payment fraud, segmentation and tested recovery is essential with regards to ransomware, and third-party governance is the biggest for supply-chain compromise. There is no one column that is consistently strong, and no one control family is able to deal with every threat.

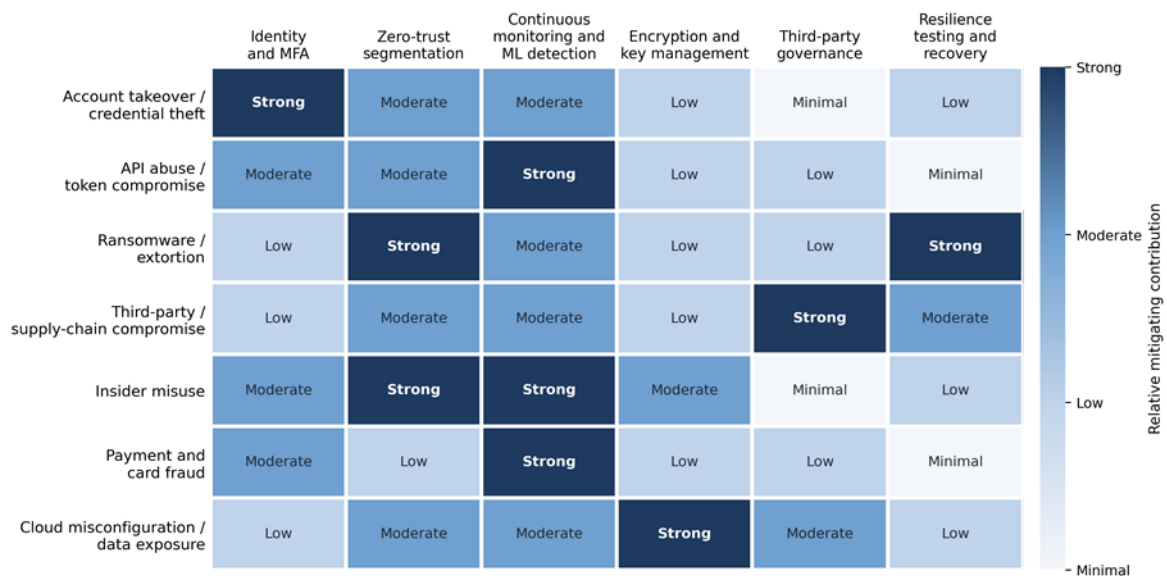


Fig. 5: Qualitative synthesis of the relative mitigating contribution of control families against dominant FinTech threat categories. Ratings are the authors' interpretive judgments drawn from the reviewed literature and standards, not empirical measurements.

ILLUSTRATIVE APPLICATION

As an example, imagine a payments FinTech with a mobile app and partner APIs that facilitate instant transfers taking place on a cloud-based platform. An attacker gets a partner's API credentials via phishing and starts to make fake payment initiation requests. As you read through the framework you will see which layers held during the incident. The speed of escalation occurs under Govern, based on the firm's appetite for payment fraud risk and the responsibility allocated to partner-access controls [19]. Limit blast radius/surface anomalies with short-lived, user-restricted tokens and behavioural monitoring of API calls under Protect and Detect. Respond and Recover is a set of pre-agreed playbooks that enable the firm to suspend the partner credential, freeze suspicious transfers and resume normal service within its 'tolerance' [15]. Outside the organization, it is important to notify customers, the partner and supervisors appropriately and specifically to show benevolence and integrity while a valid ISO/IEC 27001 certificate gives context, it does not excuse [14], [17], [20]. The outcome of trust is not a question of whether or not the attempt took place, but rather of the observable quality of each layer, and this is the core of the framework. This vignette is used to illustrate and is not a real event.

IMPLICATIONS FOR PRACTICE

- Govern explicitly. Assign accountable executives, define risk appetite in terms of critical services and tolerable disruption, and report a small set of forward-looking metrics to the board [15], [19].
- Treat identity as the primary perimeter. Combine strong authentication, least privilege, and continuous verification across employees, partners, and APIs [13], [27].
- Manage third parties as part of the control environment. Maintain a register of critical providers, test exit and substitution plans, and evidence concentration analysis [17].
- Prepare and rehearse disclosure. Pre-agree decision rights and templates for notification to regulators and customers, and exercise them alongside technical recovery [14], [29].
- Signal credibly. Pursue assurance mechanisms whose scope is meaningful, disclose that scope, and avoid conflating compliance certificates with security outcomes [11], [30].

OPEN CHALLENGES AND RESEARCH AGENDA

Several challenges emerge from the synthesis and define an agenda for future work.

- **Data scarcity and comparability.** Loss data are underreported, inconsistently defined, and skewed toward large firms, limiting the validity of quantitative models [18], [24]. Standardized incident taxonomies and privacy-preserving data-sharing arrangements are needed.
- **Third-party and concentration risk.** Methods for measuring correlated failure across shared providers remain immature, and firm-level assessments cannot capture ecosystem-level exposure [5], [31].

- **Empirical measurement of trust.** Trust constructs are well theorized [6], [7], but field evidence linking specific security investments and disclosure practices to trust outcomes in FinTech is sparse. Longitudinal and event-study designs around breach disclosures would be valuable.
- **Governance of AI in security and fraud.** AI raises both defensive capability [32], [12] and offensive potential, and it introduces model risk, explainability demands, and data-protection questions that current frameworks address only partially.
- **Regulatory convergence.** Divergent incident definitions and reporting timelines increase compliance cost for cross-border firms, and empirical comparison of regimes' effectiveness is lacking [14], [17].
- **Cryptographic agility and emerging technologies.** Preparation for advances in cryptanalysis, and secure integration of ledger-based infrastructure, will require inventory of cryptographic dependencies and agile migration planning [16].
- **Small and early-stage firms.** Resource-constrained FinTech start-ups need proportionate, low-cost paths to credible assurance; how frameworks scale down without losing substance is an open question [19], [20].

CONCLUSION

This review has addressed the cybersecurity risk management and digital trust as a mutual phenomenon within the context of a FinTech organization. The evidence demonstrates that the FinTech operating model (which is API driven, cloud and third party reliant, data rich) generates an attack surface in which identity and third party relationships are the primary lines of exposure [4], [9]. Existing governance and standards provide the language and structure for dealing with that exposure, including CSF 2.0 with governance; ISO/IEC 27001 with certifiable assurance; and DORA and Basel principles, which take operational supervision to operational resilience and third party oversight [15], [17], [19], [20]. Quantitative and economic methods complement prioritization and investment with rigor, but are still limited in their ability because of the quality of the data [29], [30].

The main thesis is that having a risk management capability is essential but not enough for establishing digital trust. The four conditions that must be met for trust to be established are competence, integrity, benevolence, and structural assurance [6], [7]. The proposed Risk-Trust Nexus framework provides a structure for matching the investments made in technology, governance and assurance with the values of the stakeholders that a FinTech business relies on. Empirical validation of its propositions, enhancement of measuring concentration risk, and responsible governance of AI-powered security tools are the most promising avenues for future directions in research and practice.

REFERENCES

- [1] U. A. Kithran, S. Ilyas, K. Amber, H. Abbas, and S. Zahid, "AI-based collision prediction and prevention systems in urban traffic," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 1907–1920, 2025.
- [2] M. R. Islam, I. A. Badhan, M. H. Rahman, and M. N. Hasnain, "The economics of global renewable energy supply chains: Opportunities and vulnerabilities for the U.S.," *International Journal of AI, Engineering and Management Studies (IJAIEMS)*, vol. 1, no. 1, pp. 108–136, 2026.
- [3] U. Imtiaz, "Ghost signals: Ethical RF adversarial testing of consumer alarm ecosystems," in *Data Science and Security*, S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds. Cham, Switzerland: Springer, 2026, *Lecture Notes in Networks and Systems*, vol. 1945, doi: 10.1007/978-3-032-24075-0_21.
- [4] S. M. Ali, M. Hadi, F. Usama, M. S. Khan, M. Iqbal, and S. Ahmad, "From artificial to quantum intelligence: The next frontier of low-carbon energy systems," in *Proc. 2026 Int. Conf. Integrated Intelligence and Cognitive Engineering (ICIICE)*, Dubai, United Arab Emirates, 2026, pp. 1–6, doi: 10.1109/ICIICE69672.2026.11565487.
- [5] A. Badhan, M. N. Hasnain, M. H. Rahman, I. Chowdhury, and M. A. Sayem, "Strategic deployment of advance surveillance ecosystems: An analytical study on mitigating unauthorized U.S. border entry," *Inverge Journal of Social Sciences*, vol. 3, no. 4, pp. 82–94, 2024.
- [6] M. Delshadi, N. Ahmad, M. D. Rasheed, M. S. Sardar, and U. Aslam, "Deep learning-based network traffic analysis for cyber threat detection," *Spectrum of Engineering Sciences*, vol. 3, no. 12, pp. 607–614, 2025.
- [7] K. Khaliq, M. S. Khan, S. Sajid, I. Shahbaz, M. W. Iqbal, K. S. Siddiqui, et al., "A study on the application of deep learning and machine learning in adaptive intelligent tutoring," *Spectrum of Engineering Sciences*, vol. 4, no. 3, pp. 818–835, 2026.
- [8] U. A. Kithran, A. Khanam, S. Ilyas, R. Yaqoob, and M. Hannan, "Demand forecasting in transportation networks using deep learning," *Spectrum of Engineering Sciences*, vol. 3, no. 11, pp. 687–700, 2025.

- [9] U. Iqbal and Y. Bhutto, "Digital transformation through artificial intelligence and advance business analytic in American operational management," *Journal of Theoretical and Applied Econometrics*, vol. 3, no. 1, pp. 37–50, 2026.
- [10] M. M. Islam, "AI-driven fraud detection and prevention using human behavior analysis to enhance U.S. social and financial security," *International Journal of Applied Mathematics*, vol. 38, no. 8S, pp. 861–871, 2025.
- [11] D. Safiullah, A. A. Khan, N. Ahmad, M. Danish, and S. Rana, "Integrating artificial intelligence and soil ecology to enhance plant resilience under environmental stress," *ASSAJ*, vol. 4, no. 2, pp. 3508–3516, 2025.
- [12] R. Singh, "Brønsted-acid-guided esterification: Mechanistic and kinetic insights for long-chain fatty acid to alkyl ester conversion on a heterogenized porous acid platform," *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 1, 2026, doi: 10.67231/rzakra50.
- [13] U. Iqbal, "AI-enhanced network optimization for electric vehicle charging infrastructure expansion in the United States using graph theory and demand analytics," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 2, pp. 112–129, 2024.
- [14] M. Chaudhari, "Hydrophilic nanofiber barrier coatings for aluminum: Waterborne crosslinking, microstructure–property links, and EIS-based protection," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3017, Jul. 2026, doi: 10.4238/rhd2k915.
- [15] R. Singh, "Smart prediction of molecular behavior in liquid chromatography for better compound detection," *International Journal of Clinical Research and Medical Sciences*, vol. 1, no. 1, 2026, doi: 10.67231/v3jyx227.
- [16] R. Parveen, "An explainable AI framework for ethical fraud prevention in U.S. federal welfare programs," *International Journal of Applied Mathematics*, vol. 38, no. 11S, pp. 1425–1435, 2025.
- [17] M. N. Amjad, "Machine learning for renewable energy forecasting and smart grid optimization," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 2, pp. 130–145, 2024.
- [18] U. Imtiaz, "Dynamic security certification framework for evolving distributed architectures," in *Data Science and Security*, S. Shukla, H. Sayama, K. Tiwari, J. P. George, and J. V. Kureethara, Eds. Cham, Switzerland: Springer, 2026, *Lecture Notes in Networks and Systems*, vol. 1947, doi: 10.1007/978-3-032-24360-7_32.
- [19] M. Chaudhari, "Epoxy barrier coatings reinforced with solidified-waste microfillers for aggressive acids," *Genetics and Molecular Research*, vol. 25, no. 3, Art. no. 3020, Jul. 2026, doi: 10.4238/96y1s945.
- [20] Kumar and K. K. S. Nair, "The impact of cloud-based business analytics on operational efficiency in U.S. small and medium-sized firms," *Spanish Journal of Innovation and Integrity*, vol. 49, pp. 303–318, 2025.
- [21] S. T. Hasan, "Labor market intelligence using natural language processing for the U.S. direct care workforce: Predicting skill gaps, recruitment needs, and emerging healthcare workforce demand," *American Journal of Multidisciplinary Knowledge Insights*, vol. 3, no. 1, pp. 1–16, 2024.
- [22] S. Mirza, S. Butt, A. Arif, and N. Jahangir, "COVID and post-COVID e-learning reforms in higher education institutions: A systematic review of literature," *Journal of Business Insight and Innovation*, vol. 5, no. 8, pp. 364–383, 2026.
- [23] M. N. Amjad, "Artificial intelligence-based voltage stability assessment in modern power systems: Edge intelligence for real-time monitoring of smart electrical networks," *Journal of Business Insight and Innovation*, vol. 3, no. 1, pp. 102–115, 2024.
- [24] M. A. Jawed, "Uncertainty-aware geostatistical reconstruction of regional groundwater hydraulics under sparse monitoring conditions: A case study of the Evergreen Underground Water Conservation District (EUWCD), Texas, USA," *Bishop International Journal of Mathematics and Computer Science*, vol. 1, no. 1, pp. 57–71, 2025.
- [25] W. Reese and D. Sinclair, "Bridging the digital divide: Digital inequality and socioeconomic outcomes in the United States," *American Journal of Multidisciplinary Knowledge Insights*, vol. 5, no. 1, pp. 1–8, 2026.
- [26] A. Kumar, "The role of banking credit access in healthcare analytics-driven practice growth: Implications for regional economic development in the U.S.," *Journal of Computational Systems & Engineering Insights*, vol. 2, no. 2, pp. 15–28, 2024.
- [27] N. J. Mercer, "Enhancing organizational performance through strategic cloud computing in management," *International Journal of Business Integrity and Technology Advancements*, vol. 1, no. 1, pp. 11–17, 2025.
- [28] K. Hamdan, "AI-powered cyber resilience strategies for modern organizations," *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 1, pp. 1–10, 2026.
- [29] R. M. Cachart, F. Ahmed, S. Pochincharla, V. Gummadavelli, R. S. Ganapathy, and A. Devineni, "Adaptive program governance platform using reinforcement learning and policy optimization," in *Proc. 2026 Int.*

Conf. Intelligent and Sustainable AI Systems (ICOSAAS), Bali, Indonesia, 2026, pp. 1563–1570, doi: 10.1109/ICOSAAS68663.2026.11648756.

[30] M. S. Uddin, A. Khan, I. Alim, and D. Khan, “The evolution of cybersecurity in the digital age: Contemporary threats, technologies, and future directions,” *Journal of Computational Systems & Engineering Insights*, vol. 4, no. 2, pp. 12–29, 2026.

[31] T. Boz et al., “Large-scale online science and engineering professional learning for rural elementary teachers,” *Research in Science Education*, vol. 56, no. 3, pp. 891–914, 2026.

[32] R. J. Hammack, J. Robinson, T. Boz, et al., “Supporting elementary engineering instruction in rural contexts through online professional learning and modest supports,” *Teaching, Leadership & Professional Practice Faculty Publications*, no. 40, 2024. [Online]. Available: <https://commons.und.edu/tlpp-fac/40>