Securing Cloud-Based FinTech: An Analysis of Evolving Cyber Threats

Cyber threats facing cloud-based FinTech companies exhibit diverse attack vectors, each characterized by unique attributes and potential consequences. These threats are not theoretical but represent genuine concerns in the contemporary cybersecurity landscape. This abstract encapsulates the primary attack methods and their associated impacts.

In typical attacks, API vulnerabilities have a high likelihood of unauthorized access or data extraction through insecure APIs, posing significant security risks for FinTech firms relying on these interfaces. Cloud-native threats, designed explicitly for cloud architectures, present a moderate threat level, introducing the potential for exploiting container vulnerabilities, manipulating serverless functions, or commandeering orchestrator dashboards—vulnerabilities unique to cloud-based FinTech entities. Advanced Persistent Threats (APTs) constitute a persistent menace by elite state-sponsored or highly adept criminal factions aiming to infiltrate cloud infrastructure clandestinely over an extended duration.

Cryptojacking schemes entail the deployment of malware to co-opt cloud resources for cryptocurrency mining, potentially evading detection due to the dynamic resource allocation in cloud settings.

Supply chain attacks, which target third-party service providers integrating with FinTech platforms, including cloud infrastructure vendors, introduce an indirect route to compromising security, yielding a high-level threat.

AI-powered attacks leverage artificial intelligence to automate attack processes or scale up social engineering tactics like spear phishing, representing a novel threat. While less probable, cross-cloud attacks entail exploits that leverage vulnerabilities in one cloud service to target another, capitalizing on the interconnected nature of cloud services. Financially motivated data breaches, characterized by innovative exfiltration methods, pose a severe risk, targeting the theft of substantial volumes of financial data stored in cloud environments for illicit purposes.

Misconfiguration exploitation introduces a unique menace by employing automated tools engineered to identify and exploit misconfigurations in real-time within complex cloud environments. Lastly, zero-day exploits, often featuring attacks against newly discovered vulnerabilities in cloud infrastructure or FinTech applications before patching, contribute to the spectrum of threats. More advanced attacks encompass further intricacies.

Adversarial AI and machine learning threats entail the potential usage of machine learning algorithms to orchestrate attacks capable of learning and adapting to the behavior of security systems, devising means to bypass anomaly detection mechanisms relied upon by numerous FinTech entities.

Side-channel attacks directed at cloud environments focus on leveraging information leakage inherent in shared cloud infrastructure, capitalizing on subtleties of resource sharing to glean sensitive information from co-tenants on the same cloud platform.

Quantum-inspired attacks, predating the actualization of quantum computing, potentially involve the development of quantum-inspired algorithms operating on classical computers yet capable of accelerating the breach of specific cryptographic protocols beyond traditional techniques.

Blockchain wallet vulnerabilities are likely to manifest as FinTech companies increasingly adopt blockchain technology, with attackers targeting integration points or the smart contracts governing wallet services, potentially leading to the theft of cryptocurrencies or tokens.

Deepfake technology, empowered by AI-generated audio and video, presents the prospect of impersonating key personnel to facilitate unauthorized financial transactions or manipulate stock prices through disinformation dissemination.

Cloud jacking and hyperjacking represent innovative attacks that wrest control over cloud management platforms (CMPs) or even cloud service hypervisors, potentially resulting in comprehensive control over cloud resources and data.

The manipulation of estimative models introduces a risk wherein attackers poison the data streams upon which AI models rely, thereby inducing erroneous outcomes advantageous to the attacker's objectives. Swarm-based attacks involve the coordinated deployment of compromised IoT devices or cloud instances to execute a distributed and adaptable attack, distinguishing themselves from conventional botnets.

Protocol poisoning aims to exploit lesser-known protocols or proprietary extensions inherent in cloud services, permitting subtle manipulation or the establishment of enduring backdoors. Attacks directed at intra-cloud communications target the communication between services and microservices within the cloud infrastructure, which may lack robust defense compared to external traffic.

Memory corruption attacks via just-in-time (JIT) compilers present a threat, with attackers targeting JIT compilation processes commonly employed in cloud environments, potentially resulting in arbitrary code execution. Attacks leveraging encrypted traffic capitalize on the increasing prevalence of encryption to conceal attack patterns or insert malicious code activated post-decryption by the endpoint.

AI-powered autonomous attack drones exemplify cyber-physical attacks under AI control, potentially used for physically infiltrating data centers or intercepting data transmissions, including satellite uplinks. Exploiting quantum cryptography as an emerging threat involves attacking theoretical vulnerabilities in quantum cryptography, including side-channel assaults on quantum critical distribution systems.

Manipulating AI-based financial advice bots involves subtly influencing the decision-making processes of AI-driven robo-advisors to manipulate market positions or perpetrate fraudulent activities. A separate category of attacks exhibits some overlap.

Algorithm manipulation attacks involve advanced techniques to manipulate machine learning algorithms relied upon by the platform for fraud detection, potentially causing these algorithms to overlook fraudulent transactions or incorrectly flag legitimate activities. As an autonomous testing approach, AI fuzzing scrutinizes cloud platform interfaces and services using AI to uncover intricate vulnerabilities that conventional fuzzing techniques may overlook.

Chain reaction attacks encompass the potential for exploiting vulnerabilities within one aspect of the suite, such as the expense management module, to trigger a domino effect, culminating in a comprehensive compromise of interconnected systems, including accounts payable.

Economic denial of sustainability (EDoS) attacks may exploit cloud services' auto-scaling feature, incurring financial loss by provoking substantial scaling events that result in exorbitant charges. If executed successfully, model inversion attacks grant attackers access to the AI models used for analytics and decision-making, potentially allowing them to reverse-engineer these models to unveil sensitive business insights or reconstruct private datasets.

Shadow API attacks involve the exploitation of undocumented or rogue APIs, potentially created during development or integration, offering backdoor access to the system. Data pipeline poisoning attacks involve injecting malicious data into information streams that feed the platform's analytics and reporting tools, leading to tainted business insights and sabotaging decision-making processes.

Business logic attacks, a distinct avenue of attack, do not target conventional security vulnerabilities but instead exploit the cloud-based suite's business logic to perpetrate unauthorized transactions or data breaches. Service mesh hijacking

introduces innovative attacks that compromise the service mesh layer, facilitating inter-service communications within the cloud infrastructure thereby enabling eavesdropping or tampering with internal traffic.

Cryptographic flaw exploitation hinges on using cutting-edge cryptanalysis techniques against platforms' non-standard cryptographic implementations, potentially revealing encrypted data. Adaptive compression attacks involve exploiting data compression algorithms employed in cloud networks to deduce sensitive information from encrypted packet sizes.

Quantum computing threats revolve around using emerging quantum capabilities to compromise prevailing encryption standards, potentially exposing all data transmitted or stored by the platform. Supply chain compromise schemes involve multi-stage attacks that commence with the compromise of a suite supplier or integration partner, subsequently leveraging this access to assail the platform itself. Cloud service misconfigurations introduce the prospect of exploiting intricate and frequently overlooked misconfigurations unique to cloud environments, thereby gaining unauthorized access or escalating privileges within the platform.

Container and lateral movement attacks involve escaping containerized environments and acquiring access to the underlying cloud infrastructure, ultimately facilitating lateral movement throughout the platform. Homomorphic encryption exploitation encompasses the potential exploitation of homomorphic encryption weaknesses, a relatively recent cryptographic system adopted by FinTech companies for performing computations on encrypted data.

Quantum timing attacks leverage emerging quantum technologies to execute timing attacks with unparalleled precision, potentially jeopardizing cryptographic keys or sensitive operations. Blockchain rollback attacks, affecting the foundational technology underpinning cryptocurrencies, entail innovative attacks that manipulate the blockchain to 'rollback' transactions, undermining the integrity of the blockchain ledger.

Zero-knowledge proof exploitation, if FinTech applications incorporate zero-knowledge proofs for privacy-preserving transactions, may involve the exploitation of theoretical vulnerabilities in these protocols. AI model theft or subversion attacks entail the theft or subtle alteration of AI models used for trading, risk assessment, or fraud detection, resulting in malfunction or information leakage. Interconnectivity exploits manifest as attacks that capitalize on the intricate interconnections among financial services and institutions facilitated by FinTech platforms, potentially initiating cascading failures or infiltrating multiple systems.

Biometric data breaches target biometric authentication systems, seeking to steal biometric data or engineer sophisticated spoofing attacks. If and when QKD technology is employed, attacks via quantum key distribution (QKD) may focus on exploiting practical implementation flaws rather than the underlying quantum mechanics. Federated learning poisoning, in a cloud environment employing federated learning, may involve the injection of malicious updates to compromise the shared model. Super-app exploits pertain to attacks that target integration points between different services within a FinTech 'super-app,' seeking to exploit trust relationships.

Manipulating AI-based regulatory compliance tools may entail innovative attacks that manipulate these systems to induce non-compliance or mask illicit activities. Exploiting decentralized finance (DeFi) protocols concerns the emergence of DeFi platforms within FinTech, with unique attacks potentially targeting smart contract vulnerabilities or liquidity pools.

Attacks via embedded finance explore the vulnerability of integration points between FinTech and non-financial platforms, susceptible to exploitation due to less robust security measures in non-financial ecosystems. Digital identity fraud schemes represent advanced methods to compromise digital identity verification systems, pivotal for KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance. The following is a listing of typical, advanced, and unique innovative attacks relevant to the FINTECH industry:

Typical attacks

- API Vulnerabilities: As FinTech companies heavily rely on APIs for integration with other services and data exchange, novel attacks exploit undocumented or insecure APIs to gain unauthorized access or extract sensitive data.
- Cloud-Native Threats: Attacks explicitly designed for cloud architectures, such as exploiting container vulnerabilities, serverless function manipulations, or orchestrator dashboard takeovers, be unique to cloud-based FinTech companies.
- Advanced Persistent Threats (APTs): Tailored and sustained attack campaigns by state-sponsored or highly sophisticated criminal groups that aim to infiltrate cloud infrastructure over a long period without detection.
- Cryptojacking: Attackers deploy malware that hijacks cloud resources for cryptocurrency mining, which may be hard to detect due to the dynamic resource allocation in cloud environments.
- Supply Chain Attacks: Targeting third-party service providers that integrate with your FinTech platform, such as cloud infrastructure vendors, is a novel way to compromise security indirectly.
- AI-Powered Attacks: Using artificial intelligence to automate attack processes or conduct social engineering attacks at scale, such as spear phishing, presents a novel threat.
- Cross-Cloud Attacks: Novel attacks might include cross-cloud exploits that leverage vulnerabilities in one cloud service to attack another, using the interconnected nature of cloud services.
- Financially Motivated Data Breaches: Innovative exfiltration techniques to steal large volumes of financial data stored in cloud environments, often for fraud or selling on the dark web.
- Quantum Computing Threats: Although emerging, the potential use of quantum computing to break encryption that secures financial transactions is a future novel threat.
- Insider Threats: With the cloud enabling remote access to sensitive systems, novel attacks involve social engineering or coercion of insiders to gain access to or compromise cloud-based financial systems.
- Misconfiguration Exploitation: Novel automated tools designed to detect and exploit misconfigurations in real-time pose a unique threat, as cloud environments are complex and often misconfigured.
- Bypassing Multi-Factor Authentication (MFA): Novel techniques for bypassing MFA, a common security measure in FinTech platforms employed by attackers.
- Zero-Day Exploits: Novel attacks often include zero-day exploits against newly discovered vulnerabilities in cloud infrastructure or FinTech applications before they are patched.

- Mobile Platform Attacks: With the increase in mobile FinTech services, organizations should expect novel attacks on mobile platforms, such as malicious apps or compromising mobile device management (MDM) systems.

Innovative and unique cyber attacks evolve rapidly, leveraging emerging technologies and sophisticated techniques often ahead of current defense measures. The most likely cyber attacks to target cloud-based FinTech companies, along with their estimated likelihood:

Attack	**Likelihood**
API Vulnerabilities	High
Cloud-Native Threats	Moderate
Advanced Persistent Threats (APTs)	Moderate
Cryptojacking	Moderate
Supply Chain Attacks	High
AI-Powered Attacks	Moderate
Cross-Cloud Attacks	Low
Financially Motivated Data Breaches	High
Misconfiguration Exploitation	High
Zero-Day Exploits	Moderate

More Advanced Attacks

Adversarial AI and Machine Learning: Cybercriminals use machine learning algorithms to craft attacks that can learn and adapt to the behavior of security systems, effectively finding ways to bypass anomaly detection that many FinTech companies rely on.

Side-Channel Attacks on Cloud Environments: Novel side-channel attacks target information leaked from shared cloud infrastructure, exploiting the subtleties of cloud resource sharing to glean sensitive information from other tenants on the same cloud platform.

Quantum-Inspired Attacks: Even before the advent of quantum computing, attackers might have developed quantum-inspired algorithms that ran on classical computers but broke specific cryptographic protocols faster than traditional methods.

Blockchain Wallet Vulnerabilities: As more FinTech companies adopt blockchain technology, innovative attacks may target the integration points or the smart contracts that handle the wallet services, leading to the theft of cryptocurrency or tokens.

Deepfake Technology: Cybercriminals impersonate key personnel to initiate unauthorized financial transactions or to manipulate stock prices by spreading disinformation by using AI-generated audio and video,

Cloud Jacking and Hyperjacking: Innovative forms of attacks that take over control of cloud management platforms (CMPs) or even the hypervisors that underpin cloud services, leading to broad control over cloud resources and data.

Manipulation of Predictive Models: If your FinTech company relies on predictive modeling for trading or credit scoring, an innovative attack might involve subtly poisoning the data streams the models rely on, leading to flawed outcomes that benefit the attacker.

Swarm-based Attacks: Using a swarm of compromised IoT devices or cloud instances, attackers launch a distributed and coordinated attack that is more adaptable and resilient than traditional botnets.

Protocol Poisoning: Exploiting lesser-known protocols or proprietary extensions in cloud services for subtle manipulation. This type of poisoning may try to establish persistent backdoors.

Interception of Intra-Cloud Communications: Innovative attacks target the communication between services and microservices within the cloud infrastructure, which might not be as heavily defended as external traffic.

Memory Corruption Attacks via JIT Compilers: Targeting just-in-time (JIT) compilation processes that are common in cloud environments, which, if exploited, lead to arbitrary code execution.

Attacks via Encrypted Traffic: Leveraging the increasing volume of encrypted traffic to mask attack patterns or to inject malicious code that is only activated after decryption by the endpoint.

AI-Powered Autonomous Attack Drones: Cyber-physical attacks using AI-controlled drones for physical infiltration of data centers or interception of data transmission, including satellite uplinks.

Exploiting Quantum Cryptography: Future attacks may exploit theoretical weaknesses in quantum cryptography, such as side-channel attacks on quantum critical distribution systems.

Manipulation of AI-based Financial Advice Bots: By subtly influencing the decision-making process of AI-based robo-advisors, attackers manipulate market positions or conduct fraudulent activities.

These attacks are complex and would likely require substantial resources and expertise, making them more common among nation-state actors or highly sophisticated criminal syndicates. The defense against such attacks is equally complex, requiring cutting-edge countermeasures, continuous monitoring, and adaptive security postures.

Other Attacks with Some Overlap

- Algorithm Manipulation Attacks: Attackers use advanced techniques to manipulate machine learning algorithms that the platform uses for fraud detection, causing them to miss fraudulent transactions or flag legitimate activities erroneously.
- AI Fuzzing: This involves using AI to autonomously test the cloud platform's interfaces and services to uncover complex vulnerabilities that can be exploited in ways traditional fuzzing might not reveal.
- Chain Reaction Attacks: An attacker exploits a vulnerability in one part of the suite, such as the expense management module, to trigger a domino effect, leading to a broader compromise of interconnected systems, including accounts payable.
- Economic Denial of Sustainability (EDoS): This type of attack exploits the auto-scaling feature of cloud services, causing financial loss by triggering massive scaling events that lead to exorbitant charges.
- Model Inversion Attacks: If attackers gain access to the AI models used for analytics and decision-making, they reverse-engineer these models to discover sensitive business insights or reconstruct private datasets.
- Shadow API Attacks: Exploiting undocumented or rogue APIs created during development or integration processes and can provide backdoor access to the system.
- Data Pipeline Poisoning: Injecting malicious data into the information streams feeds the platform's analytics and reporting tools, leading to tainted business insights and potentially sabotaging decision-making processes.
- Business Logic Attacks: Rather than targeting traditional security vulnerabilities, attackers exploit the business logic of the cloud-based suite to conduct unauthorized transactions or data leaks.
- Service Mesh Hijacking: Innovative attacks target the service mesh layer that facilitates inter-service communications within the cloud infrastructure, allowing attackers to eavesdrop on or tamper with internal traffic.
- Cryptographic Flaws Exploitation: Leveraging cutting-edge cryptanalysis techniques against platforms' non-standard cryptographic implementations, potentially revealing encrypted data.
- Adaptive Compression Attacks: Exploiting the data compression algorithms used in cloud networks to infer sensitive information from the size of encrypted packets.
- Quantum Computing Threats: Using emerging quantum computing capabilities to break current encryption standards, potentially exposing all data transmitted or stored by the platform.
- Supply Chain Compromise: Conducting a multi-stage attack by compromising a suite supplier or integration partner and leveraging that access to attack the platform.

- Cloud Service Misconfigurations: Exploiting complex and often overlooked misconfigurations unique to cloud environments to gain unauthorized access or escalate privileges within the platform.
- Container Escape and Lateral Movement: Breaking out of a containerized environment to gain access to the underlying cloud infrastructure, leading to the possibility of lateral movement
- Homomorphic Encryption Exploitation: As FinTech companies might adopt homomorphic encryption to perform computations on encrypted data, novel attacks aim to exploit weaknesses in these relatively new cryptographic systems.
- Quantum Timing Attacks: Using emerging quantum technologies to perform timing attacks at an unprecedented precision, potentially compromising cryptographic keys or sensitive operations.
- Blockchain Rollback Attacks: Targeting the blockchain technology that underpins cryptocurrencies, an innovative attack involves manipulating the blockchain to 'rollback' transactions, undermining the integrity of the blockchain ledger.
- Zero-Knowledge Proof Exploitation: If FinTech applications use zero-knowledge proofs for privacy-preserving transactions, novel attacks might aim to exploit theoretical weaknesses in these protocols.
- AI Model Theft or Subversion: Stealing or subtly altering AI models used for trading, risk assessment, or fraud detection, causing them to malfunction or leak information.
- Interconnectivity Exploits: As FinTech platforms increasingly interconnect with various financial services and institutions, novel attacks exploit these complex interdependencies to cascade failures or infiltrate multiple systems.
- Biometric Data Breaches: Innovatively targeting biometric authentication systems to steal biometric data or develop sophisticated spoofing attacks.
- Attack via Quantum Key Distribution (QKD): When used, QKD attackers might focus on exploiting practical implementation flaws rather than the underlying quantum mechanics.
- Federated Learning Poisoning: In a cloud environment with federated learning, attackers inject malicious updates to corrupt the shared model.
- Super-app Exploits: If a FinTech platform functions as a 'super-app' offering multiple services, unique attacks might target the integration points between different services to exploit trust relationships.
- Manipulating AI-based Regulatory Compliance Tools: Using AI for regulatory compliance, innovative attacks might focus on manipulating these systems to either cause non-compliance or mask illicit activities.
- Exploiting Decentralized Finance (DeFi) Protocols: DeFi platforms are emerging in FinTech, and unique attacks might target smart contract vulnerabilities or liquidity pools.
- Attacks via Embedded Finance: As FinTech integrates finance into non-financial platforms, attacks target these integration points to exploit the less secure elements of the ecosystem.
- Digital Identity Frauds: Advanced methods to compromise digital identity verification systems, crucial for KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance.

The impact assessment tables for various cyber-attack methods reveal that the likelihood of such events occurring within the next year ranges from low to high. Events resulting in data breaches or loss of data availability present substantial risks, with some methods posing a very high likelihood of compromising data. Financial damages from potential attacks are estimated to span from tens of thousands to tens of millions of dollars, reflecting the severe consequences these incidents harbor. Data unavailability due to these attacks lasts from a few hours to several days, with costs per hour of downtime varying significantly depending on the nature of the attack. Notably, methods involving quantum technology remain unpredictable, with their impacts currently unknown due to the emergent state of the technology. The assessments underscore the need for organizations to prepare robust cyber defenses against a spectrum of threats to mitigate risks of data breaches, financial losses, and operational disruptions.

The table below presents below offers a comprehensive analysis of various cyber attack methods, assessing their likelihood of occurrence within the next year, the potential for data compromise resulting from these attacks, the extent of financial damage they may inflict, the potential duration of data unavailability, and the associated cost per hour. This analysis serves as a valuable resource for understanding the evolving cyber threat landscape, enabling organizations, particularly those in the financial technology (FinTech) sector, to prioritize their cybersecurity efforts and allocate resources effectively. By quantifying the risks associated with each attack method, organizations can make informed decisions to bolster their defenses and mitigate potential cyber threats proactively. This proactive approach is vital in an era where cyberattacks are becoming increasingly sophisticated and frequent, posing significant challenges to data security and financial stability.

Attack Method	Likelihood (Next Year)	Likelihood of Data Compromise	Financial Damage Potential	Data Unavailability (Hours)	Cost Per Hour
Advanced Persistent Threats (APTs)	High	Very High	$1M-$10M	96	$10K
Biometric Data Breaches	High	Very High	$1M-$10M	96	$10K
Digital Identity Frauds	High	Very High	$1M-$10M	96	$10K
Financially Motivated Data Breaches	High	Very High	$1M-$10M	96	$10K
Adversarial AI and Machine Learning	Moderate	High	$100K-$500K	24	$2K
AI Model Theft or Subversion	Moderate	High	$1M-$5M	72	$3K
AI-Powered Attacks	Moderate	High	$100K-$1M	24	$1K
AI-Powered Autonomous Attack Drones	Moderate	High	$1M-$10M	96	$10K
API Vulnerabilities	Moderate	High	$100K-$1M	24	$1K
Attacks via Encrypted Traffic	High	High	$500K-$5M	24	$2K
Business Logic Attacks	High	High	$100K-$500K	24	$2K
Bypassing Multi-Factor Authentication (MFA)	Moderate	High	$100K-$1M	24	$2K
Chain Reaction Attacks	Moderate	High	$1M-$10M	96	$5K
Cloud Service Misconfigurations	High	High	$500K-$5M	48	$2.5K
Cloud-Native Threats	High	High	$500K-$5M	48	$2.5K
Container Escape and Lateral Movement	Moderate	High	$500K-$1M	48	$3K
Cross-Cloud Attacks	Moderate	High	$1M-$5M	72	$4K
Cryptographic Flaws Exploitation	Moderate	High	$500K-$5M	72	$3K
Data Pipeline Poisoning	Moderate	High	$100K-$1M	48	$2K
Deepfake Technology	Moderate	High	$50K-$250K	12	$1K
Economic Denial of Sustainability (EDoS)	Moderate	High	$1M-$10M	96	$10K
Exploiting Decentralized Finance (DeFi) Protocols	High	High	$1M-$10M	96	$5K
Federated Learning Poisoning	Moderate	High	$500K-$5M	48	$3K
Insider Threats	Moderate	High	$50K-$500K	24	$1K
Interception of Intra-Cloud Communications	Moderate	High	$100K-$500K	48	$2K
Interconnectivity Exploits	High	High	$500K-$5M	96	$4K
Manipulation of AI-based Financial Advice Bots	Moderate	High	$100K-$1M	24	$1K
Manipulation of Predictive Models	Moderate	High	$100K-$1M	24	$2K
Memory Corruption Attacks via JIT Compilers	Moderate	High	$500K-$1M	48	$3K

Attack Method	Likelihood (Next Year)	Likelihood of Data Compromise	Financial Damage Potential	Data Unavailability (Hours)	Cost Per Hour
Misconfiguration Exploitation	High	High	$100K-$1M	24	$1K
Mobile Platform Attacks	High	High	$100K-$1M	48	$1.5K
Protocol Poisoning	High	High	$100K-$1M	24	$2K
Service Mesh Hijacking	High	High	$500K-$5M	48	$2.5K
Shadow API Attacks	High	High	$100K-$1M	24	$1K
Super-app Exploits	High	High	$1M-$10M	72	$5K
Supply Chain Attacks	High	High	$1M-$10M	72	$5K
Supply Chain Compromise	High	High	$1M-$10M	72	$5K
Zero-Day Exploits	Low	High	$1M-$10M	48	$5K
Cryptojacking	High	Low	$10K-$100K	0	$500.00
Swarm-based Attacks	Low	Low	$10K-$100K	0	$500.00
Adaptive Compression Attacks	Low	Moderate	$10K-$100K	0	$500.00
AI Fuzzing	Low	Moderate	$10K-$100K	0	$500.00
Algorithm Manipulation Attacks	Low	Moderate	$100K-$1M	48	$1K
Attacks via Embedded Finance	Moderate	Moderate	$100K-$500K	48	$2K
Blockchain Rollback Attacks	Low	Moderate	$100K-$1M	48	$2K
Blockchain Wallet Vulnerabilities	Moderate	Moderate	$10K-$100K	24	$500.00
Cloud Jacking and Hyperjacking	Low	Moderate	$1M-$10M	72	$5K
Manipulating AI-based Regulatory Compliance Tools	Moderate	Moderate	$100K-$1M	24	$2K
Model Inversion Attacks	Low	Moderate	$100K-$1M	0	$500.00
Side-Channel Attacks on Cloud Environments	Moderate	Moderate	$50K-$500K	48	$1K
Zero-Knowledge Proof Exploitation	Low	Moderate	$100K-$1M	48	$2K
Attack via Quantum Key Distribution (QKD)	Low	Unknown	Unknown	Unknown	Unknown
Exploiting Quantum Cryptography	Low	Unknown	Unknown	Unknown	Unknown
Homomorphic Encryption Exploitation	Low	Unknown	Unknown	Unknown	Unknown
Quantum Computing Threats	Low	Unknown	Unknown	Unknown	Unknown
Quantum Computing Threats	Low	Unknown	Unknown	Unknown	Unknown
Quantum Timing Attacks	Low	Unknown	Unknown	Unknown	Unknown
Quantum-Inspired Attacks	Low	Unknown	Unknown	Unknown	Unknown

The likelihood of occurrence, potential data compromise, financial damage, and data unavailability are marked as "Unknown" for quantum computing threats and quantum-inspired attacks. The "Unknown" identifier indicates these threats' current uncertainty and evolving nature. The financial damage potential, data unavailability, and cost per hour for each attack type reflect these events' varied impacts on an organization.

The potential for a data breach or loss of data availability is predominantly high, with financially motivated data breaches and APTs being very high due to the targeted nature of these attacks. The extent of financial damage varies, with the highest potential damage estimated between $1 million to $10 million. The potential number of hours that data will be unavailable ranges from 24 to 96 hours, and the cost per hour of this unavailability ranges from $1,000 to $10,000.

Cryptojacking, while having a high probability of occurrence, typically results in lower financial damage and does not directly cause data unavailability. Conversely, cloud jacking and chain reaction attacks have lower likelihoods, resulting in significant economic damage and extended data unavailability. The cost per hour of data unavailability varies, indicating the different levels of operational impact these events have.

For attacks via Quantum Key Distribution (QKD), the likelihood of occurrence, potential data compromise, financial damage, and data unavailability are marked as "Unknown," reflecting these threats' nascent and speculative nature. The table shows these events' varied impact on an organization, with the highest potential financial damage and data unavailability associated with biometric data breaches and digital identity frauds, indicating their potentially severe implications. The financial damage potential, data unavailability, and cost per hour for each attack type suggest these events' varied impact on an organization.

These figures are assumptions and should be refined based on specific organizational data, threat intelligence, and expert assessment.