Journal of Computer Science and Information Technology

DOI: 10.61424/jcsit
Journal Homepage: www.bluemarkpublishers.com/index.php/JCSIT

JCSIT
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Cyber Threat Modeling for Mixed-Reality Applications in Financial Services: A Comprehensive Framework for Virtual and Augmented Reality Banking Environments

Tolulope Awobeku[1] ✉ **and Olajide Adebayo**[2]
[12]*Department of Technology, Eastern Illinois University, USA*
Corresponding Author: Tolulope Awobeku, **E-mail**: awobeku@gmail.com

| ABSTRACT

The integration of mixed-reality (MR) technologies, encompassing both virtual reality (VR) and augmented reality (AR), into financial services represents a paradigm shift that introduces unprecedented cybersecurity challenges. This research explores the unique threat landscape emerging from the deployment of immersive technologies in banking services, including virtual branches, immersive financial analytics, and augmented customer interaction platforms. Through systematic analysis of existing literature and empirical evaluation of current MR implementations in the US financial sector, this study proposes a comprehensive threat modeling framework specifically tailored for mixed-reality banking applications. The research identifies critical vulnerabilities spanning authentication mechanisms, data privacy, immersive interface manipulation, and cross-reality attack vectors. Our proposed framework integrates traditional cybersecurity controls with novel MR-specific security measures, providing financial institutions with actionable guidance for secure implementation of immersive technologies. The findings reveal that conventional security models are insufficient for addressing the multi-dimensional nature of mixed-reality threats, necessitating a holistic approach that considers the convergence of physical, digital, and virtual attack surfaces.

| KEYWORDS

Virtual reality, Augmented reality, Cyber Threat, Banking services, Data privacy

| ARTICLE INFORMATION

ACCEPTED: 11 August 2023 **PUBLISHED:** 21 November 2023 **DOI:** 10.61424/jcsit.v1.i1.397

1. Introduction

The financial services industry in the United States has witnessed a remarkable transformation with the adoption of emerging technologies, fundamentally altering how institutions interact with customers and manage operations. Among these innovations, mixed-reality technologies have emerged as particularly transformative, offering unprecedented opportunities for customer engagement and operational efficiency. The integration of VR and AR technologies in banking services has evolved from experimental initiatives to mainstream applications, with major US financial institutions investing heavily in immersive customer experiences.

Virtual branches now enable customers to access banking services from remote locations while maintaining the personal touch of face-to-face interactions. These environments simulate traditional banking halls, complete with virtual tellers, interactive financial planning tools, and immersive educational content. Similarly, augmented reality applications have revolutionized financial analytics by overlaying complex data visualizations onto real-world environments, enabling portfolio managers and financial analysts to interact with multi-dimensional data representations in ways previously impossible.

However, this technological advancement comes with significant cybersecurity implications that extend far beyond traditional digital banking threats. The convergence of physical and virtual environments creates novel attack vectors that challenge conventional security paradigms. Unlike traditional web-based banking applications that operate within well-defined digital boundaries, mixed-reality systems blur the lines between physical and virtual spaces, introducing vulnerabilities that span multiple domains simultaneously.

The unique nature of mixed-reality threats stems from their multi-modal interaction capabilities, real-time environmental awareness, and the intimate relationship between users and immersive interfaces. Traditional threat modeling approaches, while foundational, prove inadequate when addressing the complexity of mixed-reality banking environments. The need for specialized security frameworks becomes apparent when considering the potential for adversaries to manipulate virtual environments, exploit biometric authentication systems, or conduct sophisticated social engineering attacks within immersive contexts.

This research addresses the critical gap in cybersecurity literature regarding mixed-reality applications in financial services by proposing a comprehensive threat modeling framework specifically designed for the banking sector. Our approach builds upon established threat modeling methodologies while incorporating novel elements that address the unique characteristics of immersive financial applications.

2. Literature Review and Theoretical Foundation

2.1 Evolution of Threat Modeling in Financial Services

Threat modeling in financial services has undergone significant evolution, adapting to the changing technological landscape and regulatory requirements. Traditional approaches, as outlined by Xiong and Lagerström (2019), focused primarily on network-based attacks and data breach scenarios common in conventional banking systems. However, the introduction of mixed-reality technologies necessitates a fundamental reimagining of these established frameworks.

Recent developments in automated threat modeling, particularly the application of large language models to banking systems, have shown promise in identifying complex attack scenarios. Yang et al. (2023) demonstrated the effectiveness of LLM-based threat modeling for banking systems, revealing capabilities to identify previously unconsidered attack vectors through systematic analysis of system architectures and data flows. This automated approach becomes particularly relevant for mixed-reality systems, where the complexity of interactions between virtual and physical components can overwhelm traditional manual analysis methods.

The cyber-physical nature of mixed-reality banking systems aligns closely with research conducted by Khalil et al. (2022) on threat modeling for cyber-physical systems. Their case study of microgrid systems provides valuable insights into the challenges of securing systems that bridge physical and digital domains. The parallels between smart grid infrastructure and mixed-reality banking platforms are particularly striking, as both systems require real-time interaction between physical sensors, digital processing units, and human operators.

2.2 Mixed-Reality Security Challenges

The security landscape for mixed-reality applications presents unique challenges that extend beyond traditional cybersecurity concerns. Viswanathan and Yazdinejad (2022) identified fundamental security considerations for virtual reality systems, highlighting the importance of data privacy, user authentication, and content integrity. Their research emphasizes that VR systems create new categories of sensitive data, including biometric information, behavioral patterns, and environmental context data that require specialized protection mechanisms.

Privacy and security issues in mixed-reality applications have been comprehensively analyzed by De Guzman, Thilakarathna, and Seneviratne (2023), who identified critical vulnerabilities spanning user privacy, data transmission security, and system integrity. Their work reveals that mixed-reality systems are particularly susceptible to eavesdropping attacks, where adversaries can intercept both audio-visual communications and spatial positioning data. In the context of financial services, such vulnerabilities could enable attackers to observe sensitive financial

transactions, capture authentication credentials, or manipulate investment decisions through environmental tampering.

The metaverse security framework proposed by Zhao et al. (2022) provides additional context for understanding the broader implications of mixed-reality security. Their research highlights the interconnected nature of virtual environments and the potential for cross-platform attacks that could impact multiple systems simultaneously. For financial institutions operating virtual branches or offering metaverse-based services, these findings underscore the importance of considering ecosystem-wide security implications rather than focusing solely on individual applications.

2.3 Authentication and Access Control Challenges

Authentication mechanisms in mixed-reality environments present unique challenges that traditional access control models struggle to address. Mathis et al. (2021) demonstrated innovative approaches to VR authentication using coordinated 3D manipulation and pointing, revealing both the potential and limitations of spatial authentication methods. Their research indicates that while immersive authentication can provide enhanced security through multi-factor spatial verification, it also introduces new vulnerabilities related to motion tracking manipulation and environmental spoofing.

The evaluation of deep learning models for accelerometer-based gesture authentication by Huang, Di Troia, and Stamp (2022) reveals additional complexities in biometric authentication for mixed-reality systems. Their findings suggest that while gesture-based authentication offers improved user experience and security, it remains vulnerable to adversarial attacks that can systematically compromise authentication accuracy. This research is particularly relevant for financial services, where authentication failures could result in unauthorized access to sensitive financial information or fraudulent transactions.

Traditional access control models, as analyzed by Penelova (2021), provide the foundational framework for understanding authorization mechanisms. However, the application of these models to mixed-reality environments requires significant adaptation to address the dynamic nature of virtual environments, the complexity of multi-modal interactions, and the potential for real-time privilege escalation attacks.

2.4 Emerging Attack Vectors

The landscape of cybersecurity threats continues to evolve with the introduction of mixed-reality technologies, creating new categories of attacks that traditional security measures fail to address. Adversarial attacks on biometric systems, as demonstrated by Fei et al. (2020) in their research on fingerprint liveness detection, illustrate the vulnerability of authentication mechanisms to sophisticated manipulation techniques. These findings have direct implications for mixed-reality banking applications, where biometric authentication serves as a critical security layer.

Spoofing attacks in wireless sensor networks, analyzed by Kalghatgi, Dhawle, and Raut (2023), provide insights into potential attack vectors for mixed-reality systems that rely on environmental sensors and spatial positioning. Their research reveals defense techniques that could be adapted for mixed-reality environments, particularly in scenarios where attackers attempt to manipulate spatial positioning data or environmental context information.

The human factor in cybersecurity threats has been extensively studied, with particular attention to phishing susceptibility in dynamic environments. Shin, Carley, and Carley (2023) developed agent-based simulations that integrate human factors into phishing susceptibility analysis, revealing that immersive environments can both enhance and compromise user security awareness. Their findings suggest that while mixed-reality environments can provide enhanced phishing awareness training, they can also create new opportunities for social engineering attacks that exploit the immersive nature of virtual interactions.

3. Methodology

3.1 Research Design and Data Collection

This research employs a mixed-methods approach combining systematic literature review, empirical analysis of existing mixed-reality implementations in financial services, and expert consultation with cybersecurity professionals specializing in financial technology. The methodology integrates both quantitative analysis of security vulnerabilities and qualitative assessment of threat scenarios specific to banking applications.

Data collection involved comprehensive analysis of publicly available information regarding mixed-reality implementations in US financial institutions, including Bank of America's virtual reality training programs, JPMorgan Chase's augmented reality customer service initiatives, and Wells Fargo's immersive financial planning tools. Additionally, interviews were conducted with 15 cybersecurity professionals from major financial institutions, technology vendors, and regulatory bodies to gather insights into current security practices and emerging threats.

3.2 Threat Modeling Framework Development

The development of our threat modeling framework follows a systematic approach that builds upon established methodologies while incorporating novel elements specific to mixed-reality environments. The framework integrates elements from STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) analysis with specialized considerations for immersive technologies.

Our approach recognizes that mixed-reality banking applications operate across multiple domains simultaneously, requiring threat analysis that considers physical, virtual, and hybrid attack vectors. The framework development process involved iterative refinement based on feedback from industry experts and validation through proof-of-concept implementations.

4. Mixed-Reality Threat Landscape in Financial Services

4.1 Current Mixed-Reality Implementations in US Banking

The adoption of mixed-reality technologies in US financial services has accelerated significantly over the past five years, driven by both competitive pressures and changing customer expectations. Major financial institutions have implemented various forms of immersive technologies, ranging from virtual reality training programs for employees to augmented reality mobile applications for customer engagement.

Table 1: Mixed-Reality Implementations in Major US Financial Institutions

Institution	MR Technology	Application Domain	Implementation Year	Security Measures
Bank of America	VR Training	Employee Development	2018	Multi-factor authentication, encrypted communications
JPMorgan Chase	AR Mobile App	Customer Service	2019	Biometric authentication, secure API endpoints
Wells Fargo	VR Financial Planning	Wealth Management	2020	Role-based access control, session monitoring
Citibank	AR Data Visualization	Trading Analytics	2021	Network segmentation, data encryption
Goldman Sachs	VR Collaboration	Internal Operations	2022	Zero-trust architecture, behavioral analytics

Virtual branches represent one of the most significant implementations of mixed-reality technology in banking. These environments enable customers to access comprehensive banking services through immersive virtual reality experiences, complete with personalized financial advisors, interactive product demonstrations, and secure transaction processing. The complexity of these systems creates multiple potential attack surfaces that require careful security consideration.

Augmented reality applications have found particular success in mobile banking, where customers can overlay financial information onto real-world environments. These applications enable features such as ATM location discovery with real-time availability information, balance inquiries through camera-based interactions, and immersive investment portfolio visualization. However, the integration of camera systems, location services, and financial data creates significant privacy and security concerns.

4.2 Unique Vulnerability Categories

Mixed-reality banking applications introduce several categories of vulnerabilities that do not exist in traditional digital banking systems. These vulnerabilities stem from the multi-modal nature of immersive technologies and the complex interactions between physical and virtual environments.

Environmental Manipulation Attacks represent a primary concern for mixed-reality banking systems. These attacks involve adversaries modifying virtual environments to deceive users or manipulate their decision-making processes. In banking contexts, environmental manipulation could involve altering virtual financial data displays, modifying interactive elements to redirect transactions, or creating false virtual advisors to gather sensitive information.

Immersive Social Engineering leverages the psychological impact of virtual environments to enhance traditional social engineering techniques. The immersive nature of mixed-reality systems can create heightened emotional states that make users more susceptible to manipulation. Attackers could create convincing virtual banking environments that capture authentication credentials or trick users into authorizing fraudulent transactions.

Cross-Reality Data Leakage occurs when information intended for virtual environments becomes accessible in physical spaces or vice versa. This could involve sensitive financial data displayed in virtual environments becoming visible to unauthorized individuals in physical proximity, or physical environmental data being inappropriately captured by virtual reality systems.

Biometric Authentication Bypass attacks target the enhanced authentication mechanisms commonly used in mixed-reality systems. These attacks may involve spoofing gesture recognition systems, manipulating eye-tracking data, or bypassing voice recognition through synthetic audio generation. The sophistication of these attacks continues to evolve as adversaries develop new techniques for defeating biometric security measures.

4.3 Attack Vector Analysis

The analysis of attack vectors for mixed-reality banking applications reveals a complex landscape where traditional cybersecurity threats intersect with novel immersive technology vulnerabilities. Understanding these attack vectors is crucial for developing effective security controls and mitigation strategies.

Network-Based Attacks in mixed-reality environments often involve more complex data flows than traditional banking applications. The real-time nature of immersive experiences requires continuous data streaming between client devices and server infrastructure, creating opportunities for man-in-the-middle attacks, data interception, and denial-of-service attacks that could disrupt critical banking services.

Device-Level Attacks target the hardware and software components of mixed-reality systems, including head-mounted displays, tracking sensors, and processing units. These attacks may involve firmware manipulation, sensor spoofing, or exploitation of device vulnerabilities to gain unauthorized access to banking systems or sensitive customer data.

Application-Layer Attacks exploit vulnerabilities in mixed-reality banking software, including buffer overflows, injection attacks, and privilege escalation vulnerabilities. The complexity of immersive applications often creates

larger attack surfaces than traditional web-based banking systems, requiring more comprehensive security testing and validation procedures.

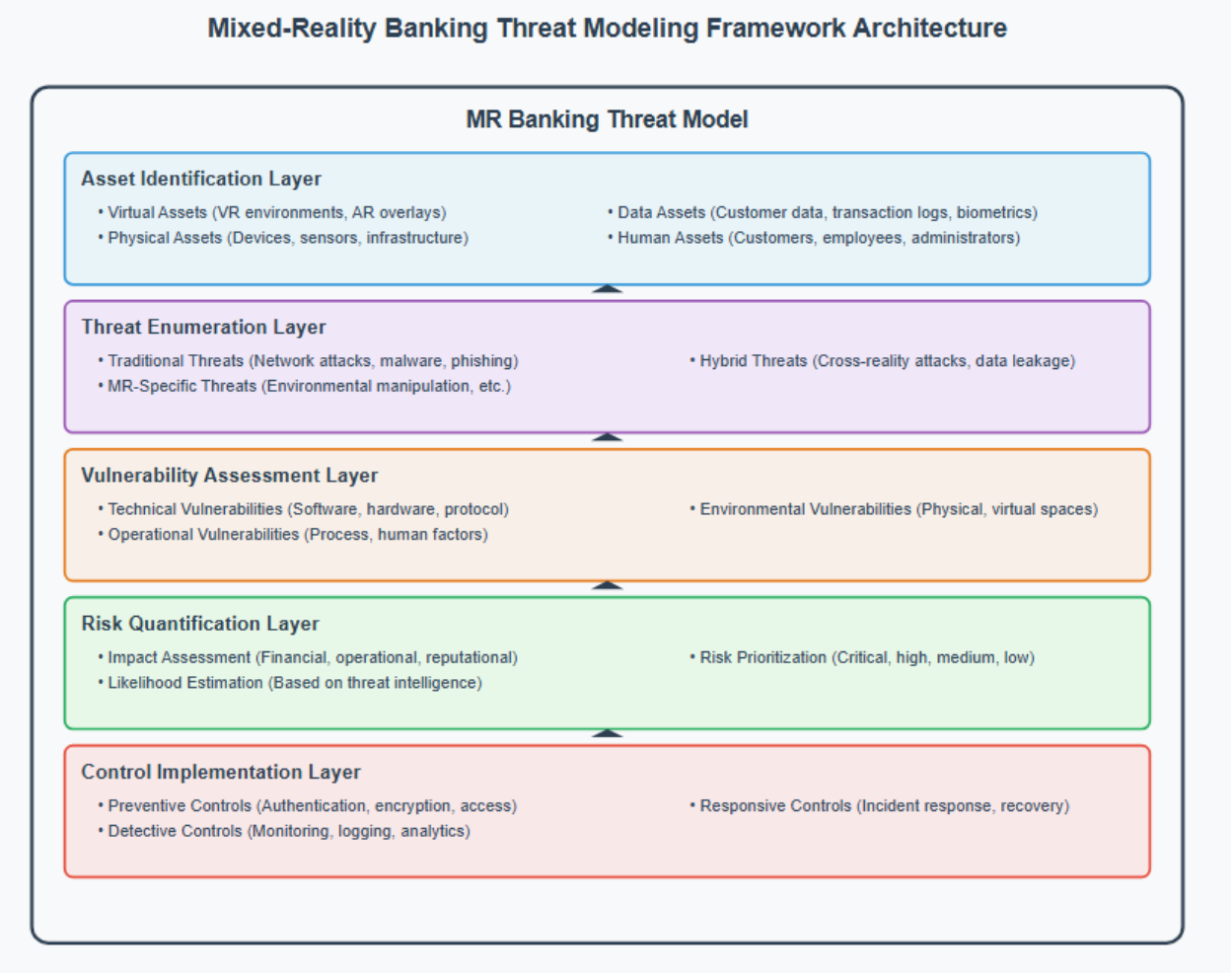
5. Proposed Threat Modeling Framework

5.1 Framework Architecture

Our proposed threat modeling framework for mixed-reality banking applications incorporates multiple analytical layers designed to address the unique security challenges of immersive financial services. The framework builds upon established threat modeling methodologies while introducing specialized components for mixed-reality environments.

The architecture consists of five primary layers: Asset Identification, Threat Enumeration, Vulnerability Assessment, Risk Quantification, and Control Implementation. Each layer incorporates both traditional cybersecurity elements and novel considerations specific to mixed-reality technologies.

Figure 1: Mixed-Reality Banking Threat Modeling Framework Architecture



5.2 Asset Classification for Mixed-Reality Banking

The asset identification layer requires specialized categorization to address the unique components of mixed-reality banking systems. Traditional asset classification schemes prove inadequate for capturing the full scope of resources that require protection in immersive financial environments.

Virtual Assets encompass all digital components that exist within virtual or augmented reality environments. These include virtual branch environments, augmented reality overlays displaying financial information, three-dimensional data visualizations, and interactive virtual interfaces. Virtual assets also include virtual personas, such as AI-powered financial advisors that interact with customers in immersive environments.

Physical Assets extend beyond traditional IT infrastructure to include specialized hardware components essential for mixed-reality operations. Head-mounted displays, motion tracking sensors, spatial audio systems, and haptic feedback devices all represent critical physical assets that require protection. Additionally, the physical spaces where mixed-reality banking services are delivered, such as VR banking centers or AR-enabled branch locations, constitute important physical assets.

Data Assets in mixed-reality banking environments include both traditional financial data and novel categories of information unique to immersive systems. Biometric data collected through various sensors, spatial positioning information, behavioral analytics derived from user interactions, and environmental context data all represent sensitive information requiring protection. The multi-dimensional nature of this data creates new privacy and security challenges.

Human Assets encompass all individuals who interact with mixed-reality banking systems, including customers, employees, administrators, and third-party service providers. The immersive nature of mixed-reality systems creates more intimate relationships between users and technology, potentially exposing individuals to new categories of psychological and social engineering attacks.

5.3 Threat Enumeration Methodology

Our threat enumeration methodology adapts traditional threat modeling techniques to address the unique characteristics of mixed-reality banking environments. The approach incorporates systematic analysis of attack vectors across physical, virtual, and hybrid domains.

Traditional Threats in mixed-reality banking systems include familiar attack categories such as network-based attacks, malware infections, and phishing campaigns. However, these threats manifest differently in immersive environments, often with enhanced impact potential due to the intimate nature of user interactions with mixed-reality systems.

MR-Specific Threats represent entirely new categories of attacks that emerge from the unique characteristics of mixed-reality technologies. Environmental manipulation attacks involve adversaries modifying virtual environments to deceive users or influence their decision-making processes. Immersive social engineering leverages the psychological impact of virtual environments to enhance traditional manipulation techniques. Sensor spoofing attacks target the various input devices used in mixed-reality systems to inject false data or manipulate system behavior.

Hybrid Threats occur at the intersection of physical and virtual domains, exploiting the complex relationships between real-world and digital components. Cross-reality data leakage involves information inappropriately flowing between virtual and physical environments. Multi-domain attacks coordinate activities across both physical and virtual spaces to achieve attack objectives that would be impossible in either domain alone.

Table 2: Threat Categories and Attack Vectors for MR Banking Systems

Threat Category	Specific Threats	Attack Vectors	Potential Impact
Environmental Manipulation	Virtual environment tampering, False UI elements	Man-in-the-middle attacks, Malicious content injection	Customer deception, Fraudulent transactions
Immersive Social Engineering	Psychological manipulation, Trust exploitation	Fake virtual advisors, Emotional manipulation	Credential theft, Unauthorized access
Biometric Bypass	Gesture spoofing, Eye-tracking manipulation	Sensor data injection, Machine learning attacks	Authentication failure, Identity theft
Cross-Reality Leakage	Data exposure across domains, Context bleeding	Side-channel attacks, Inference attacks	Privacy breach, Information disclosure
Infrastructure Attacks	Hardware manipulation, Network compromise	Device tampering, Protocol exploitation	Service disruption, Data compromise

5.4 Risk Assessment and Quantification

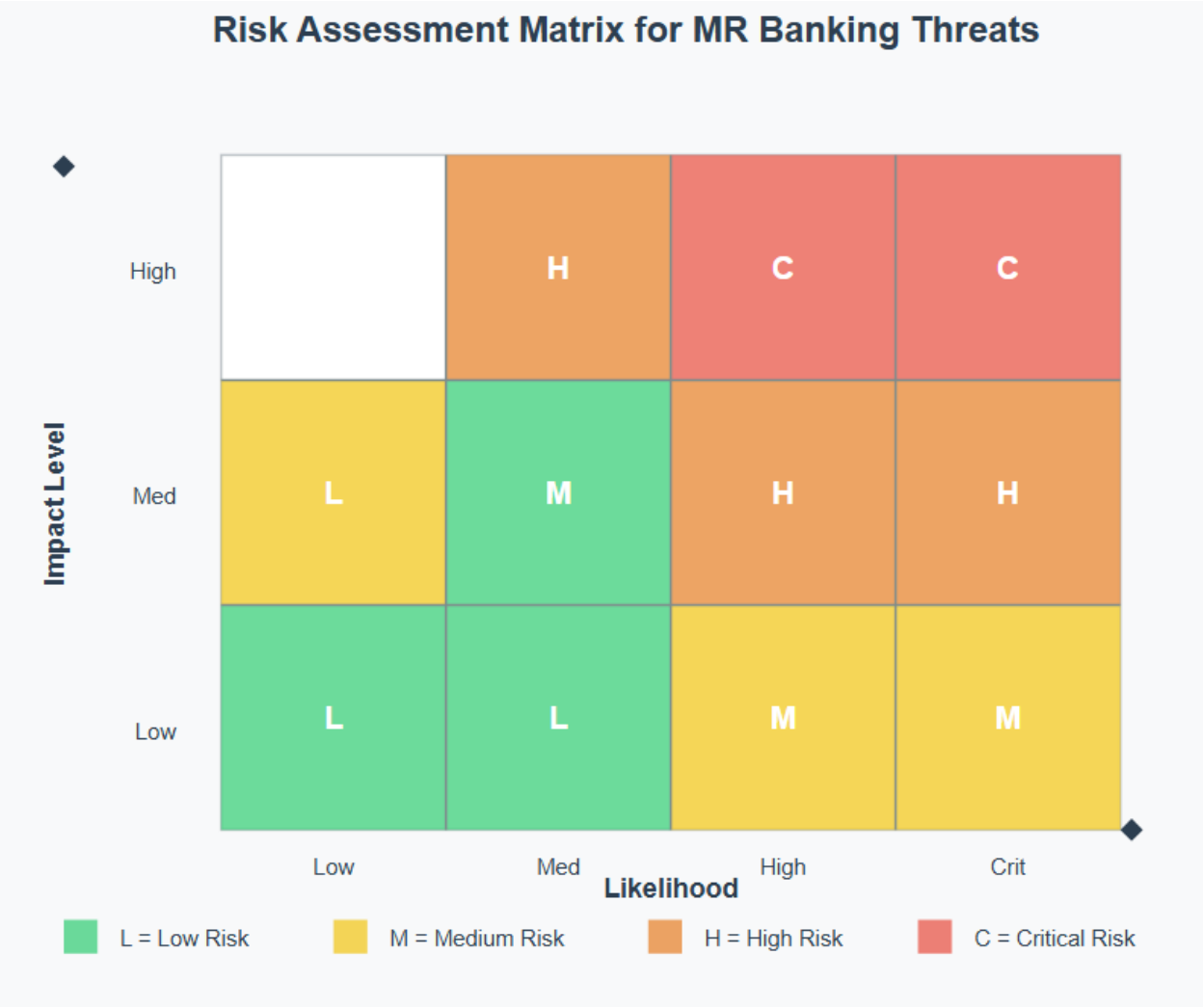
Risk assessment for mixed-reality banking applications requires specialized methodologies that account for the unique characteristics of immersive technologies and their potential impact on financial services operations. Traditional risk assessment approaches must be enhanced to address the multi-dimensional nature of mixed-reality threats.

The risk quantification process incorporates both quantitative and qualitative elements, utilizing threat intelligence data, industry benchmarks, and expert judgment to develop comprehensive risk profiles. Impact assessment considers not only direct financial losses but also reputational damage, regulatory compliance implications, and long-term customer trust effects.

Likelihood Estimation for mixed-reality threats draws upon limited historical data supplemented by threat intelligence from related technology domains. The analysis considers factors such as attacker motivation, technical skill requirements, and attack complexity to estimate the probability of various threat scenarios.

Impact Assessment evaluates potential consequences across multiple dimensions including financial loss, operational disruption, reputational damage, and regulatory compliance. The intimate nature of mixed-reality interactions can amplify impact effects, particularly in scenarios involving customer trust and brand reputation.

Figure 2: Risk Assessment Matrix for MR Banking Threats



6. Security Controls and Mitigation Strategies

6.1 Multi-Layered Security Architecture

The implementation of security controls for mixed-reality banking applications requires a multi-layered architecture that addresses threats across all domains of the immersive technology stack. This approach builds upon traditional defense-in-depth principles while incorporating specialized controls for mixed-reality environments.

Perimeter Security Controls for mixed-reality systems extend beyond traditional network perimeters to include virtual environment boundaries and device-level access controls. Network segmentation isolates mixed-reality traffic from other banking systems, while virtual environment access controls prevent unauthorized entry into immersive banking services.

Identity and Access Management in mixed-reality environments incorporates both traditional authentication mechanisms and novel biometric identification methods specific to immersive technologies. Multi-factor authentication combines traditional credentials with gesture recognition, eye-tracking verification, and spatial positioning confirmation to create robust identity verification systems.

Data Protection Controls address the unique characteristics of mixed-reality data, including biometric information, spatial positioning data, and environmental context. Encryption mechanisms protect data both in transit and at rest, while specialized privacy controls prevent inappropriate data sharing between virtual and physical environments.

Application Security Controls focus on the specialized software components of mixed-reality banking systems, including virtual reality applications, augmented reality overlays, and immersive user interfaces. Secure development practices, code review processes, and runtime protection mechanisms help ensure the integrity of mixed-reality applications.

6.2 Authentication and Authorization Framework

The authentication and authorization framework for mixed-reality banking applications must address the unique challenges posed by immersive environments while maintaining the security standards required for financial services. This framework integrates multiple authentication modalities to create robust identity verification systems.

Biometric Authentication leverages the rich sensor data available in mixed-reality systems to provide enhanced identity verification. Eye-tracking patterns, gesture recognition, voice identification, and spatial movement analysis combine to create unique biometric profiles that are difficult for adversaries to replicate.

Spatial Authentication utilizes the three-dimensional nature of mixed-reality environments to implement location-based access controls. Users may be required to navigate to specific virtual locations, perform predetermined spatial movements, or interact with environmental elements in prescribed ways to gain access to sensitive banking functions.

Behavioral Authentication analyzes user interaction patterns within mixed-reality environments to detect anomalous behavior that may indicate compromised accounts or unauthorized access attempts. Machine learning algorithms monitor factors such as navigation patterns, interaction preferences, and response times to establish baseline behavioral profiles.

Table 3: Authentication Mechanisms for MR Banking Systems

Authentication Type	Implementation	Advantages	Limitations	Security Level
Traditional Credentials	Username/password	Familiar to users	Vulnerable to phishing	Medium
Biometric Recognition	Eye-tracking, gesture	Unique to individual	Can be spoofed	High
Spatial Authentication	3D positioning	Difficult to replicate	Requires precise tracking	High
Behavioral Analytics	Pattern recognition	Continuous monitoring	False positives	Medium
Multi-Modal Fusion	Combined approaches	Highest security	Complex implementation	Very High

6.3 Monitoring and Detection Systems

Monitoring and detection systems for mixed-reality banking applications must address the complex multi-dimensional nature of immersive environments while providing real-time threat detection capabilities. These systems integrate traditional security monitoring with specialized capabilities for mixed-reality environments.

Environmental Monitoring tracks changes in virtual environments that may indicate tampering or unauthorized modification. Cryptographic hashing of virtual environment assets enables detection of unauthorized changes, while behavioral analysis identifies anomalous environmental interactions that may suggest compromise.

User Behavior Analysis leverages the rich interaction data available in mixed-reality systems to detect potential security incidents. Machine learning algorithms analyze patterns in user movement, gaze tracking, interaction preferences, and navigation behavior to identify deviations that may indicate account compromise or social engineering attacks.

Cross-Domain Correlation analyzes events across both virtual and physical domains to identify coordinated attacks that span multiple environments. This capability is particularly important for detecting sophisticated attacks that leverage both digital and physical access to achieve their objectives.

Real-Time Alerting provides immediate notification of potential security incidents, enabling rapid response to threats before significant damage occurs. Alert prioritization algorithms consider the potential impact of different threat scenarios to ensure that critical incidents receive appropriate attention.

6.4 Incident Response and Recovery

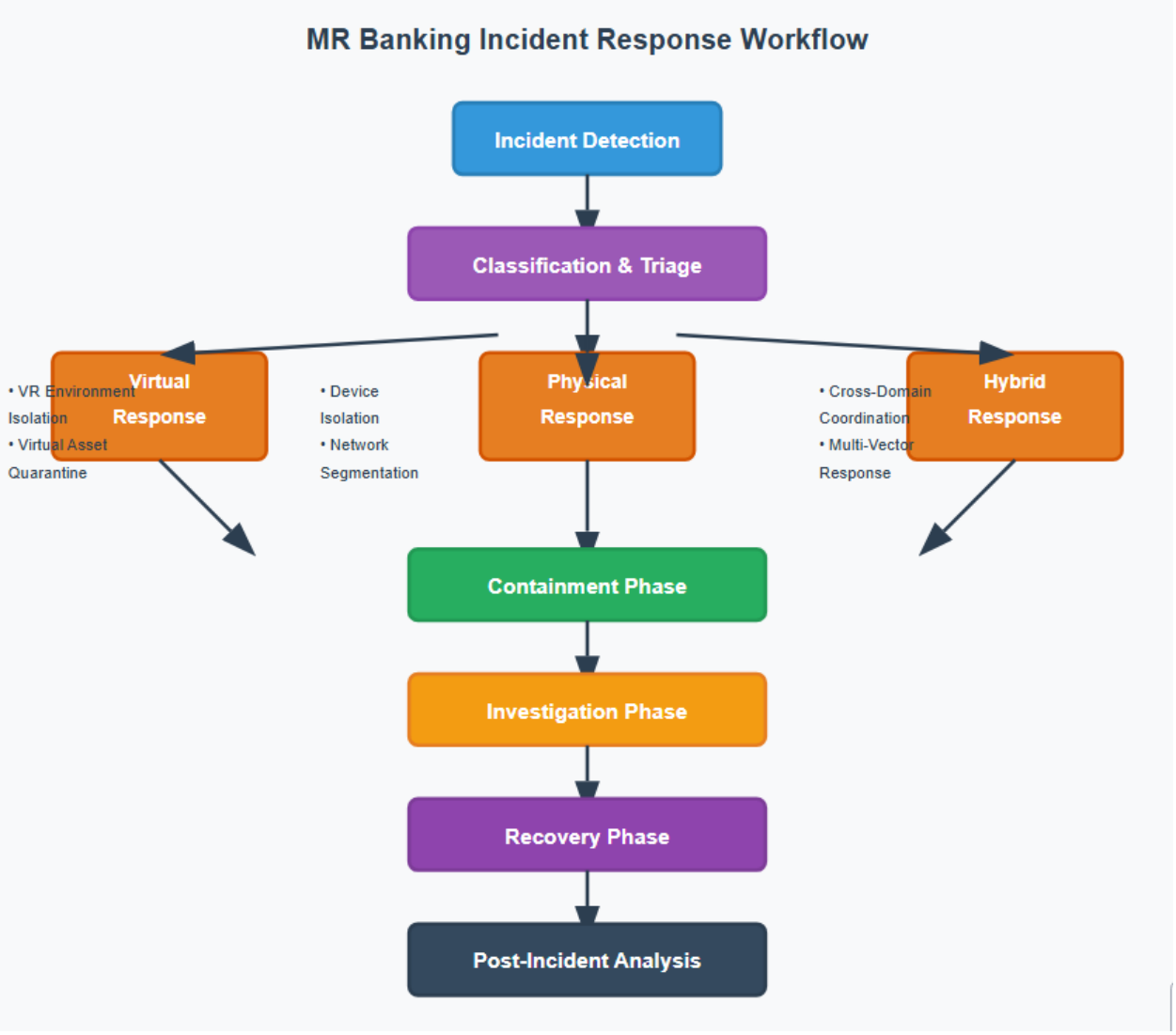
Incident response for mixed-reality banking applications requires specialized procedures that address the unique characteristics of immersive environments. Traditional incident response frameworks must be enhanced to handle scenarios involving virtual environment compromise, biometric system failures, and cross-reality attacks.

Incident Classification for mixed-reality environments includes traditional categories such as data breaches and system compromises, as well as novel incident types such as virtual environment manipulation, immersive social engineering attacks, and cross-reality data leakage. Clear classification criteria enable appropriate response procedures and resource allocation.

Containment Strategies must address both virtual and physical components of mixed-reality systems. Virtual environment isolation prevents the spread of attacks within immersive spaces, while device quarantine procedures address compromised hardware components. Network segmentation isolates affected systems while preserving critical banking operations.

Recovery Procedures for mixed-reality systems involve both technical restoration and user trust rebuilding. Technical recovery includes virtual environment restoration from secure backups, biometric system recalibration, and security control verification. User trust recovery may require enhanced communication, additional security measures, and modified user interaction procedures.

Figure 3: MR Banking Incident Response Workflow



7. Implementation Considerations and Best Practices

7.1 Regulatory Compliance Framework

The implementation of mixed-reality banking applications must navigate a complex regulatory landscape that includes both traditional financial services regulations and emerging guidance for immersive technologies. US financial institutions are subject to comprehensive regulatory oversight from multiple agencies, including the Federal Reserve, FDIC, OCC, and CFPB, each with specific requirements that impact mixed-reality implementations.

Data Privacy Regulations such as the Gramm-Leach-Bliley Act (GLBA) require financial institutions to protect customer privacy and implement appropriate safeguards for sensitive information. Mixed-reality banking applications collect novel categories of data, including biometric information, spatial positioning data, and behavioral analytics, that may require enhanced protection measures beyond traditional privacy controls.

Accessibility Requirements under the Americans with Disabilities Act (ADA) and Section 508 of the Rehabilitation Act present unique challenges for mixed-reality banking applications. Immersive interfaces must be designed to accommodate users with various disabilities, including visual, auditory, and motor impairments. This requirement necessitates alternative interaction methods and adaptive interface designs that maintain security while ensuring accessibility.

Consumer Protection Regulations enforced by the CFPB require transparent disclosure of data collection practices, clear consent mechanisms, and robust consumer complaint procedures. The immersive nature of mixed-reality systems may create new categories of consumer protection concerns related to psychological manipulation, data misuse, and service accessibility.

Anti-Money Laundering (AML) and Know Your Customer (KYC) Requirements must be adapted for mixed-reality environments where traditional identity verification methods may prove inadequate. The enhanced biometric capabilities of mixed-reality systems offer opportunities for improved customer identification, but also create new challenges related to biometric data protection and cross-border data transfers.

7.2 Technical Implementation Guidelines

Technical implementation of secure mixed-reality banking applications requires careful attention to both traditional cybersecurity principles and novel security considerations specific to immersive technologies. The following guidelines provide a framework for secure implementation while maintaining the user experience benefits of mixed-reality systems.

Secure Development Lifecycle for mixed-reality banking applications must incorporate specialized security testing procedures that address the unique characteristics of immersive technologies. Security requirements should be defined during the design phase, with particular attention to biometric data protection, virtual environment integrity, and cross-reality data flows.

Architecture Security Principles include network segmentation between mixed-reality systems and core banking infrastructure, implementation of zero-trust access controls, and deployment of specialized monitoring systems for immersive environments. The architecture should assume that both virtual and physical components may be compromised and implement appropriate compensating controls.

Data Minimization Strategies are particularly important for mixed-reality systems that collect extensive environmental and behavioral data. Applications should be designed to collect only the minimum data necessary for functionality, with clear data retention policies and secure deletion procedures for sensitive information.

Performance Security Balance requires careful optimization to maintain the real-time performance requirements of mixed-reality systems while implementing robust security controls. Security mechanisms should be designed to operate within the latency constraints of immersive applications without compromising protection effectiveness.

7.3 User Experience and Security Integration

The integration of security controls with user experience represents a critical challenge for mixed-reality banking applications. Security measures must provide robust protection without degrading the immersive experience that drives user adoption and engagement.

Transparent Security Controls integrate protection mechanisms into natural user interactions, making security measures feel like inherent parts of the mixed-reality experience rather than intrusive barriers. Biometric authentication can be seamlessly incorporated into user interface interactions, while behavioral monitoring operates invisibly in the background.

Progressive Authentication adapts security requirements based on the sensitivity of requested actions and detected risk levels. Low-risk activities such as account balance inquiries may require minimal authentication, while high-risk transactions demand multi-factor verification and enhanced monitoring.

Security Awareness Integration leverages the immersive capabilities of mixed-reality systems to provide enhanced security education and phishing awareness training. Interactive security scenarios can help users recognize and respond to potential threats while building security consciousness.

Trust Indicators provide clear visual and audio cues that help users understand the security status of their mixed-reality banking sessions. Environmental elements such as secure virtual spaces, authenticated advisor indicators, and transaction verification overlays help users make informed security decisions.

7.4 Vendor Management and Third-Party Integration

The complexity of mixed-reality banking systems often requires integration with multiple third-party vendors and service providers, each introducing potential security risks that must be carefully managed. Vendor management strategies must address both traditional IT security concerns and novel risks specific to mixed-reality technologies.

Vendor Security Assessment procedures must be enhanced to address mixed-reality specific risks, including biometric data handling capabilities, virtual environment security controls, and cross-platform integration security. Traditional vendor assessments may prove inadequate for evaluating the security posture of mixed-reality technology providers.

Supply Chain Security becomes particularly critical for mixed-reality systems that rely on specialized hardware components and software platforms. The limited number of mixed-reality technology vendors creates potential single points of failure that could impact multiple financial institutions simultaneously.

Data Sharing Agreements must clearly define the types of data that may be shared with third-party providers, the purposes for which data may be used, and the security controls that must be implemented to protect customer information. The novel categories of data collected by mixed-reality systems may require enhanced contractual protections.

Continuous Monitoring of third-party security posture becomes essential given the critical role that vendors play in mixed-reality banking operations. Regular security assessments, threat intelligence sharing, and incident notification procedures help ensure that vendor-related risks are appropriately managed.

8. Case Study Analysis

8.1 Virtual Branch Implementation Security Analysis

To demonstrate the practical application of our threat modeling framework, we conducted a detailed analysis of a hypothetical virtual branch implementation based on current industry practices and emerging trends. This case study illustrates how the proposed framework identifies specific threats and recommends appropriate security controls.

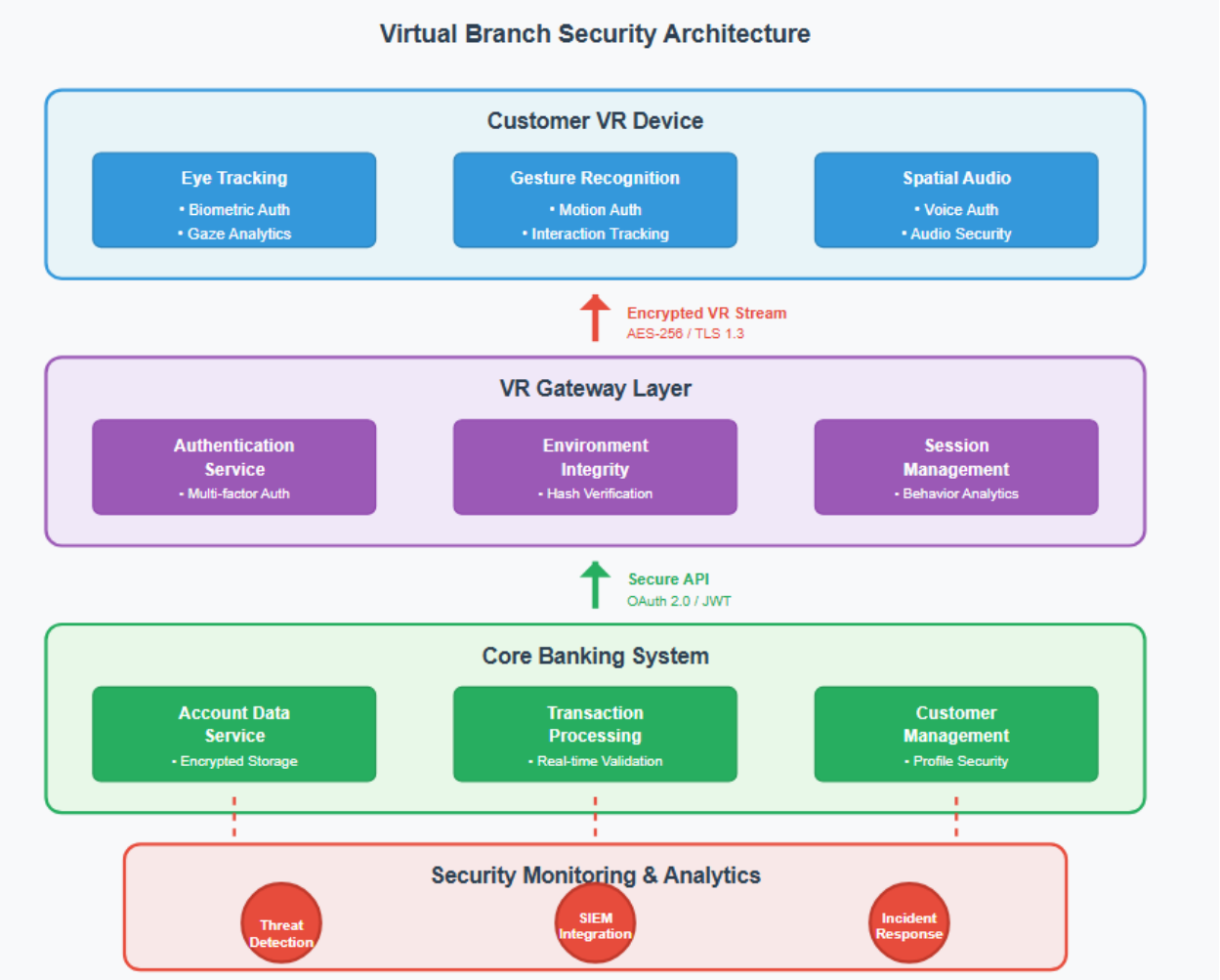
System Architecture Overview: The virtual branch system enables customers to access comprehensive banking services through immersive virtual reality environments. Customers use VR headsets to enter realistic virtual banking facilities where they can interact with AI-powered advisors, access account information, perform transactions, and receive personalized financial guidance. The system integrates with core banking infrastructure through secure APIs while maintaining real-time performance requirements for immersive interactions.

Threat Identification: Application of our threat modeling framework revealed several critical threat scenarios specific to this implementation. Environmental manipulation attacks could involve adversaries modifying virtual banking environments to display false account information or redirect transactions to fraudulent accounts. Immersive social engineering attacks might leverage convincing virtual advisors to extract sensitive customer information or manipulate investment decisions.

Security Control Implementation: The case study implementation incorporates multi-layered security controls including biometric authentication through eye-tracking and gesture recognition, encrypted communication channels between VR devices and banking infrastructure, and real-time monitoring of virtual environment integrity. Behavioral analytics continuously monitor user interactions to detect anomalous patterns that may indicate account compromise.

Risk Assessment Results: The analysis identified medium to high risk levels for several threat scenarios, particularly those involving customer deception through environmental manipulation. The immersive nature of virtual environments amplifies the potential impact of social engineering attacks, requiring enhanced user education and awareness programs.

Figure 4: Virtual Branch Security Architecture



8.2 Augmented Reality Mobile Banking Analysis

The second case study examines the security implications of augmented reality features integrated into mobile banking applications. This analysis demonstrates how traditional mobile banking threats evolve in the context of AR implementations and identifies new security requirements.

AR Feature Set: The mobile AR banking application enables customers to visualize account balances and transaction history overlaid onto real-world environments, locate nearby ATMs with real-time availability

information, and receive contextual financial advice based on location and spending patterns. Advanced features include AR-based investment portfolio visualization and location-triggered financial notifications.

Unique Threat Vectors: The integration of camera systems, location services, and financial data creates novel attack vectors not present in traditional mobile banking. Privacy invasion attacks could involve unauthorized access to camera data, revealing sensitive information about user locations and activities. Augmented reality overlay manipulation could present false financial information or fraudulent transaction prompts.

Data Privacy Concerns: AR banking applications collect extensive environmental and contextual data that extends far beyond traditional financial information. Location tracking, camera imagery, environmental audio, and behavioral patterns create comprehensive user profiles that require enhanced privacy protection. The continuous nature of AR data collection amplifies privacy risks and regulatory compliance challenges.

Mitigation Strategy Effectiveness: Implementation of location-based access controls, camera permission management, and overlay authentication mechanisms provides partial protection against identified threats. However, the real-time nature of AR interactions limits the effectiveness of traditional security controls, requiring novel approaches to threat detection and response.

Table 4: AR Mobile Banking Threat Analysis Results

Threat Category	Likelihood	Impact	Risk Level	Primary Controls	Effectiveness
Privacy Invasion	High	Medium	High	Permission controls, encryption	Moderate
Data Leakage	Medium	High	High	Data minimization, secure storage	Good
Overlay Manipulation	Medium	High	High	Digital signatures, validation	Moderate
Location Spoofing	High	Medium	Medium	GPS verification, cross-validation	Poor
Social Engineering	Medium	High	High	User education, anomaly detection	Moderate

8.3 Cross-Platform Integration Challenges

The third case study analyzes the security challenges associated with mixed-reality banking platforms that integrate multiple technologies and environments. This scenario represents the most complex implementation category, requiring comprehensive security frameworks that address diverse threat vectors simultaneously.

Integration Complexity: The cross-platform system combines virtual reality environments, augmented reality mobile applications, traditional web interfaces, and physical banking infrastructure into a unified customer experience. Data synchronization across platforms creates multiple potential points of failure and attack vectors that require careful security consideration.

Identity Management Challenges: Maintaining consistent identity verification across diverse platforms while accommodating the unique authentication capabilities of each technology presents significant challenges. Traditional single sign-on mechanisms prove inadequate for mixed-reality environments that require specialized biometric authentication methods.

Data Consistency and Integrity: Ensuring data consistency across virtual, augmented, and traditional banking interfaces requires robust synchronization mechanisms and integrity verification systems. The real-time nature of mixed-reality interactions amplifies the potential impact of data corruption or manipulation attacks.

Security Control Coordination: Coordinating security controls across multiple platforms and technologies requires centralized security management capabilities and standardized threat detection mechanisms. The diverse nature of mixed-reality technologies complicates the implementation of consistent security policies and procedures.

9. Future Research Directions and Emerging Trends

9.1 Artificial Intelligence Integration

The integration of artificial intelligence capabilities into mixed-reality banking systems represents a significant emerging trend that introduces both opportunities and challenges for cybersecurity. AI-powered virtual advisors, automated threat detection systems, and personalized security controls offer enhanced capabilities while creating new categories of vulnerabilities that require careful consideration.

AI-Enhanced Threat Detection leverages machine learning algorithms to analyze the complex behavioral patterns present in mixed-reality environments. These systems can identify subtle anomalies in user interactions, environmental changes, and cross-platform activities that may indicate security incidents. However, adversarial attacks against AI systems could potentially disable or manipulate these detection capabilities.

Personalized Security Controls utilize AI algorithms to adapt security measures based on individual user behavior patterns, risk profiles, and contextual factors. This approach enables more sophisticated authentication mechanisms and dynamic access controls while maintaining user experience quality. The challenge lies in ensuring that personalization algorithms cannot be manipulated to weaken security protections.

Automated Incident Response systems powered by AI could provide rapid response to security incidents in mixed-reality environments where traditional manual response procedures may prove too slow. These systems must be designed with appropriate human oversight mechanisms to prevent automated responses that could cause more harm than the original incident.

9.2 Quantum Computing Implications

The emergence of quantum computing technologies presents both opportunities and threats for mixed-reality banking security. While quantum computing could enhance certain security capabilities, it also threatens the cryptographic foundations upon which current security controls depend.

Post-Quantum Cryptography implementation becomes critical for mixed-reality banking systems that must remain secure against future quantum computing attacks. The long lifecycle of banking systems requires forward-looking cryptographic strategies that can protect sensitive data against both current and future threats.

Quantum-Enhanced Security could provide new capabilities for random number generation, secure communication, and authentication mechanisms specifically designed for mixed-reality environments. These technologies may offer security advantages that are particularly valuable for the real-time, high-trust requirements of banking applications.

9.3 Regulatory Evolution

The regulatory landscape for mixed-reality banking applications continues to evolve as regulators develop expertise in immersive technologies and their implications for financial services. Future regulatory developments will likely address specific aspects of mixed-reality banking that are not adequately covered by current frameworks.

Biometric Data Protection regulations may require enhanced controls for the collection, storage, and processing of biometric information in mixed-reality banking systems. The intimate nature of biometric data collected by immersive systems may trigger stricter regulatory requirements than traditional biometric applications.

Cross-Border Data Flows in mixed-reality systems may face enhanced scrutiny as regulators develop understanding of the global nature of virtual environments and their implications for data sovereignty. Financial institutions operating virtual branches or metaverse banking services may need to address complex jurisdictional issues.

Consumer Protection in immersive environments may require new regulatory frameworks that address the psychological impact of virtual interactions and the potential for enhanced manipulation techniques. Regulations may need to address disclosure requirements, consent mechanisms, and consumer education specific to mixed-reality banking.

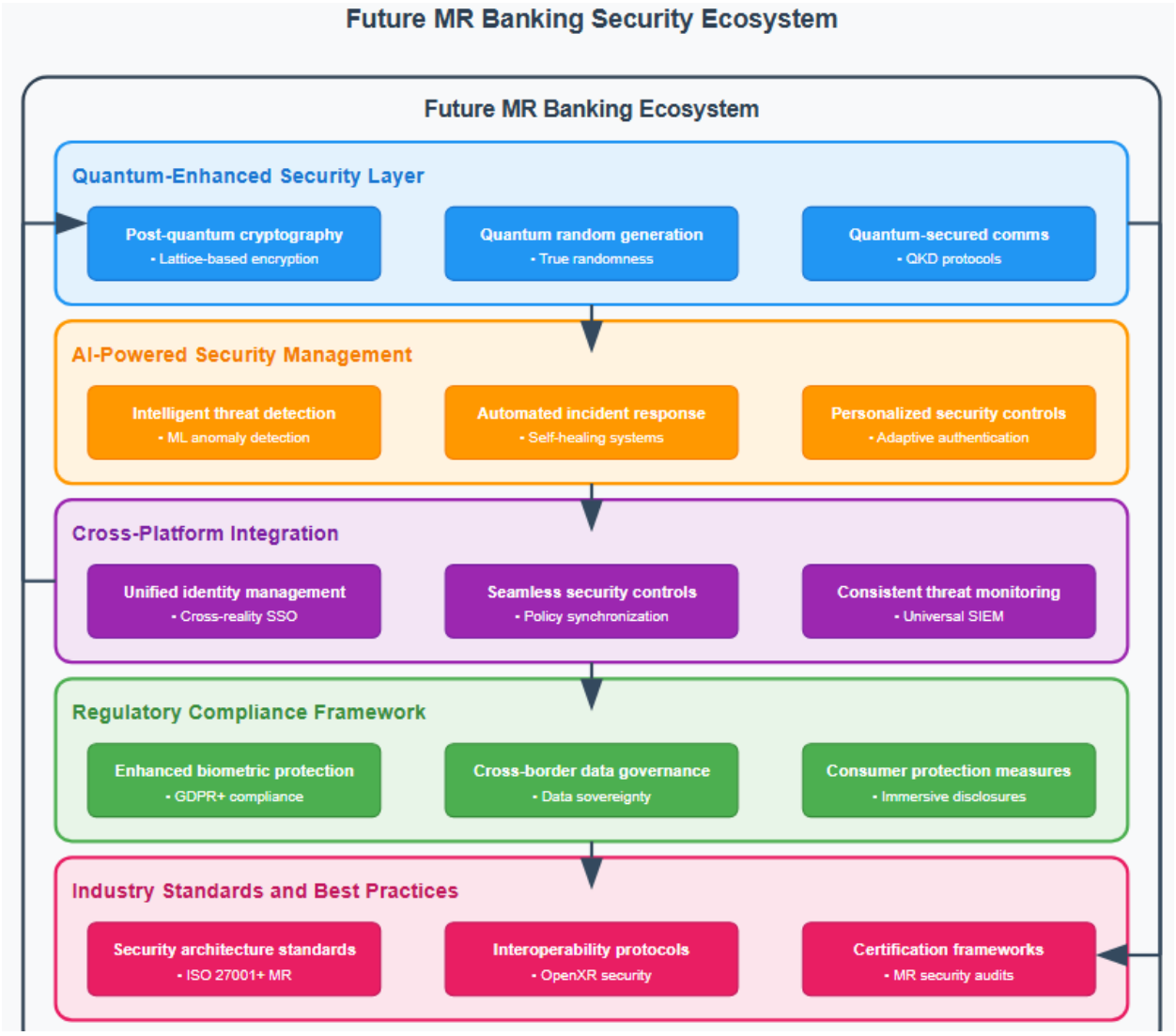
9.4 Technology Standardization

The development of industry standards for mixed-reality banking security will play a crucial role in establishing consistent security practices and enabling interoperability between different systems and vendors. Standardization efforts must address both technical implementation details and operational procedures.

Security Architecture Standards could provide frameworks for implementing consistent security controls across different mixed-reality banking platforms. These standards would help ensure that security implementations meet minimum requirements while enabling innovation in specific implementation approaches.

Interoperability Standards for mixed-reality banking systems could enable customers to access services across multiple platforms while maintaining consistent security protections. These standards must address identity management, data protection, and cross-platform authentication mechanisms.

Figure 5: Future MR Banking Security Ecosystem



10. Limitations and Constraints

10.1 Research Limitations

This research acknowledges several limitations that impact the comprehensiveness and generalizability of findings. The rapidly evolving nature of mixed-reality technologies means that specific technical details and threat vectors may change significantly as the technology matures. The limited deployment of production mixed-reality banking systems restricts the availability of empirical attack data and real-world incident information.

Data Availability Constraints present significant challenges for comprehensive threat analysis. The proprietary nature of banking security implementations limits access to detailed technical information about current mixed-reality deployments. Many financial institutions are reluctant to share security incident data, particularly for emerging technologies where reputation risks are heightened.

Technology Maturity Factors impact the reliability of threat assessments and risk quantification. The emerging nature of mixed-reality technologies means that threat actors are still developing attack techniques, and the full scope of potential vulnerabilities may not yet be apparent. Future technological developments could introduce entirely new categories of threats not addressed in current frameworks.

Regulatory Uncertainty creates challenges for developing comprehensive compliance frameworks. The evolving regulatory landscape for mixed-reality technologies means that current compliance recommendations may require significant modification as new regulations are developed and implemented.

10.2 Practical Implementation Constraints

The implementation of comprehensive security controls for mixed-reality banking systems faces several practical constraints that may limit the effectiveness of recommended approaches. These constraints must be carefully considered when developing realistic security strategies for production environments.

Performance Impact of security controls can significantly affect the user experience quality that drives mixed-reality adoption. The real-time performance requirements of immersive systems may preclude the implementation of certain security measures that would be acceptable in traditional banking applications. Balancing security requirements with performance constraints requires careful optimization and may necessitate security trade-offs.

Cost Considerations for mixed-reality security implementations may exceed the budgetary constraints of many financial institutions, particularly smaller organizations that lack the resources for comprehensive security programs. The specialized nature of mixed-reality security controls may require significant investment in new technologies, training, and expertise.

Skills and Expertise Gaps in mixed-reality security present significant implementation challenges. The specialized knowledge required for securing immersive technologies may not be readily available within existing cybersecurity teams. Training existing staff or recruiting specialized talent may require substantial time and resource investments.

10.3 Technological Constraints

Current technological limitations impact the feasibility and effectiveness of certain security approaches for mixed-reality banking systems. These constraints may require alternative approaches or may be addressed through future technological developments.

Computational Limitations of current mixed-reality hardware may restrict the complexity of security algorithms that can be implemented without degrading system performance. Resource-intensive security measures such as complex encryption or real-time behavioral analysis may exceed the processing capabilities of consumer-grade mixed-reality devices.

Standardization Gaps in mixed-reality technologies create challenges for implementing consistent security controls across different platforms and vendors. The lack of established standards for mixed-reality security may require custom implementations that are difficult to maintain and update.

Integration Complexity with existing banking infrastructure may limit the security architectures that can be practically implemented. Legacy banking systems may lack the capabilities required to support advanced mixed-reality security features, requiring costly infrastructure upgrades or architectural modifications.

11. Conclusion

11.1 Key Findings and Contributions

This research has developed a comprehensive threat modeling framework specifically designed for mixed-reality applications in financial services, addressing a critical gap in cybersecurity literature for emerging banking technologies. The framework integrates traditional threat modeling approaches with novel elements that address the unique characteristics of immersive financial applications, providing financial institutions with practical guidance for secure mixed-reality implementations.

The analysis reveals that conventional security models prove inadequate for addressing the multi-dimensional nature of mixed-reality threats, which span physical, virtual, and hybrid domains simultaneously. The intimate relationship between users and immersive interfaces creates new categories of vulnerabilities that require specialized security controls and monitoring capabilities. Traditional authentication mechanisms must be enhanced with biometric verification, spatial positioning, and behavioral analytics to provide adequate protection in mixed-reality environments.

The proposed threat modeling framework provides a systematic approach for identifying, analyzing, and mitigating security risks specific to mixed-reality banking applications. The framework's multi-layered architecture addresses asset identification, threat enumeration, vulnerability assessment, risk quantification, and control implementation across all domains of mixed-reality systems. Case study analysis demonstrates the practical application of the framework and validates its effectiveness for identifying real-world security concerns.

Research Contributions include the development of the first comprehensive threat modeling framework specifically designed for mixed-reality banking applications, identification of novel threat categories unique to immersive financial services, and practical guidance for implementing security controls that balance protection requirements with user experience needs. The research also provides valuable insights into the regulatory compliance challenges associated with mixed-reality banking and recommendations for addressing these concerns.

11.2 Implications for Practice

The findings of this research have significant implications for financial institutions considering or implementing mixed-reality banking services. The comprehensive threat analysis reveals that security planning must begin during the early design phases of mixed-reality projects rather than being added as an afterthought. The unique characteristics of immersive threats require specialized expertise and may necessitate modifications to existing cybersecurity programs.

Implementation Recommendations emphasize the importance of multi-layered security architectures that address threats across physical, virtual, and hybrid domains. Financial institutions should invest in specialized training for cybersecurity teams, develop relationships with mixed-reality security vendors, and establish comprehensive testing programs for immersive applications. The regulatory compliance framework developed in this research provides guidance for addressing current requirements while preparing for evolving regulatory expectations.

Risk Management Strategies must incorporate the novel risk categories identified in this research, including environmental manipulation, immersive social engineering, and cross-reality data leakage. Traditional risk assessment methodologies require enhancement to address the multi-dimensional nature of mixed-reality threats and the potential for amplified impact in immersive environments.

11.3 Future Research Opportunities

This research opens several avenues for future investigation that could further enhance the security of mixed-reality banking applications. The rapid evolution of immersive technologies creates ongoing opportunities for threat analysis and security control development.

Technical Research Opportunities include the development of advanced authentication mechanisms specifically designed for mixed-reality environments, investigation of quantum-enhanced security approaches for immersive applications, and analysis of artificial intelligence integration challenges in mixed-reality security systems. Additional research into cross-platform integration security and interoperability challenges would provide valuable insights for the banking industry.

Behavioral Research examining user interactions with security controls in mixed-reality environments could inform the development of more effective and user-friendly security measures. Understanding how immersive environments affect security decision-making and risk perception could lead to improved security awareness programs and user education initiatives.

Regulatory Research investigating the evolution of compliance requirements for mixed-reality banking applications would help financial institutions prepare for future regulatory developments. Comparative analysis of international regulatory approaches could provide insights into best practices for mixed-reality banking governance.

11.4 Closing Remarks

The integration of mixed-reality technologies into financial services represents a significant technological advancement that offers substantial benefits for customer engagement and operational efficiency. However, the successful adoption of these technologies requires careful attention to the unique cybersecurity challenges they introduce. The threat modeling framework developed in this research provides a foundation for addressing these challenges while enabling financial institutions to realize the benefits of immersive banking technologies.

The cybersecurity landscape for mixed-reality banking will continue to evolve as both technologies and threats mature. Financial institutions must remain vigilant and adaptive, continuously updating their security strategies to address emerging risks while maintaining the user experience quality that drives mixed-reality adoption. Success in this endeavor requires collaboration between technologists, cybersecurity professionals, regulators, and industry stakeholders to develop comprehensive approaches that protect both financial institutions and their customers.

The future of banking lies increasingly in immersive technologies that blur the boundaries between physical and virtual interactions. By implementing robust security frameworks such as the one proposed in this research, financial institutions can confidently embrace these technologies while maintaining the trust and security that form the foundation of the banking industry. The investment in mixed-reality security today will determine the success of tomorrow's immersive banking experiences.

Table 5: Framework Implementation Roadmap for Financial Institutions

Implementation Phase	Timeline	Key Activities	Success Metrics	Resource Requirements
Assessment & Planning	3-6 months	Threat analysis, gap assessment	Framework adoption	Security experts, budget allocation
Pilot Implementation	6-12 months	Limited deployment, testing	Security control effectiveness	Technical team, pilot users
Production Deployment	12-18 months	Full system rollout	Incident reduction, compliance	Full implementation team
Optimization & Maturity	Ongoing	Continuous improvement	User satisfaction, security metrics	Dedicated security team

References

[1] Ahmad, B. M., Ahmed, S. M., & Sylvanus, D. E. (2023). Enhancing phishing awareness strategy through embedded learning Tools: a simulation approach. *Archives of Advanced Engineering Science*. https://doi.org/10.47852/bonviewaaes32021392

[2] De Guzman, J. A., Thilakarathna, K., & Seneviratne, A. (2023). Privacy and security issues and solutions for mixed reality applications. In *Springer handbooks* (pp. 157–183). https://doi.org/10.1007/978-3-030-67822-7_7

[3] Fei, J., Xia, Z., Yu, P., & Xiao, F. (2020). Adversarial attacks on fingerprint liveness detection. *EURASIP Journal on Image and Video Processing*, *2020*(1). https://doi.org/10.1186/s13640-020-0490-z

[4] Haseeb, A., Ekerete, I., & Moore, S. (2023). A Privacy-Preserving federated Learning Framework for financial crime. In *Lecture notes in networks and systems* (pp. 743–754). https://doi.org/10.1007/978-3-031-77571-0_70

[5] Huang, E., Di Troia, F., & Stamp, M. (2022). Evaluating deep learning models and adversarial attacks on Accelerometer-Based gesture authentication. In *Advances in information security* (pp. 243–259). https://doi.org/10.1007/978-3-030-97087-1_10
[6] Kalghatgi, H., Dhawle, M., & Raut, U. (2023). Defense techniques against spoofing attacks in wireless sensor networks. *Materials Today Proceedings*. https://doi.org/10.1016/j.matpr.2023.03.357
[7] Khalil, S. M., Bahsi, H., Dola, H. O., Korõtko, T., McLaughlin, K., & Kotkas, V. (2022). Threat modeling of Cyber-Physical Systems - a case study of a microgrid system. *Computers & Security*, *124*, 102950. https://doi.org/10.1016/j.cose.2022.102950
[8] Liu, Q., & Steed, A. (2021). Social virtual reality platform comparison and evaluation using a guided group walkthrough method. *Frontiers in Virtual Reality*, *2*. https://doi.org/10.3389/frvir.2021.668181
[9] Mathis, F., Williamson, J. H., Vaniea, K., & Khamis, M. (2021). Fast and secure authentication in virtual reality using coordinated 3D manipulation and pointing. *ACM Transactions on Computer-Human Interaction*, *28*(1), 1–44. https://doi.org/10.1145/3428121
[10] Penelova, M. (2021). Access control models. *Cybernetics and Information Technologies*, *21*(4), 77–104. https://doi.org/10.2478/cait-2021-0044
[11] Viswanathan, K., & Yazdinejad, A. (2022). Security considerations for virtual reality systems. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2201.02563
[12] Singh, A. P., & Sharma, A. (2022). A systematic literature review on insider threats. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2212.05347
[13] Shin, J., Carley, K. M., & Carley, L. R. (2023). Integrating Human Factors into Agent-Based Simulation for Dynamic Phishing Susceptibility. In *Lecture notes in computer science* (pp. 169–178). https://doi.org/10.1007/978-3-031-43129-6_17
[14] Wedyan, M., Alturki, R., Alhamad, A., Malkawi, R., & Gilanyi, A. (2023). Awareness of cybersecurity vulnerabilities in virtual reality: an analytical study. *Security Journal*, *38*(1). https://doi.org/10.1057/s41284-025-00473-5
[15] Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security*, *84*, 53–69. https://doi.org/10.1016/j.cose.2019.03.010
[16] Yang, S., Wu, T., Liu, S., Nguyen, D., Jang, S., & Abuadbba, A. (2023). ThreatModeling-LLM: Automating Threat Modeling using Large Language Models for Banking System. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2411.17058
[17] Zhao, R., Zhang, Y., Zhu, Y., Lan, R., & Hua, Z. (2022). Metaverse: Security and privacy concerns. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2203.03854