International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 25s,2025
https://theaspd.com/index.php

Zero Trust in Mobile Applications: Security Without Sacrificing Usability

Swapnil Kale
RTM Nagpur University, India

Abstract
Zero Trust architecture in mobile applications represents a major shift in how companies approach security. Instead of trying to build walls around networks that no longer have clear boundaries, organizations are learning to verify everything and trust nothing by default. This comprehensive review shows how companies can successfully deploy Zero Trust frameworks without disrupting user experiences or operational effectiveness while actually strengthening their security posture. Mobile environments bring their own challenges that make them different from traditional desktop security—device diversity, network mobility, limited computing resources, and users who expect things to just work. Through detailed analysis of adaptive authentication processes, microsegmentation methods, continuous trust scoring, and context-based security controls, this review demonstrates that Zero Trust principles work well in mobile platforms without sacrificing usability. Real-world case studies from financial services, healthcare, and manufacturing show that successful implementations share common characteristics: comprehensive risk assessment models, integrated identity management solutions, and user-focused design patterns. Looking ahead, emerging technologies like AI-driven risk assessment, edge computing, quantum-resistant cryptography, and advanced behavioral biometrics will define the next generation of mobile Zero Trust deployments. Organizations that get this right gain significant competitive advantages through better security, improved user experiences, and increased operational agility.
Keywords: *Zero Trust Architecture, Mobile Security, Adaptive Authentication, Behavioral Biometrics, Microsegmentation*

1. INTRODUCTION

Mobile devices have completely transformed how businesses think about security. What used to be straightforward—protecting a network with clear boundaries—has become incredibly complex as smartphones and tablets took over both personal and professional lives. Today's organizations find themselves in a tough spot: employees expect to work from anywhere on any device, but this flexibility creates security headaches that traditional approaches simply can't handle. The numbers tell the story—smartphone adoption continues to climb year after year, and enterprise mobile app usage shows no signs of slowing down. This shift has forced companies to rethink everything about how they protect their data and systems [1].

The COVID-19 pandemic accelerated this transformation, pushing remote work adoption at breakneck speed across knowledge-intensive industries. Companies went from traditional office-based operations to distributed workforce models practically overnight, completely reshaping security perimeters from well-defined corporate boundaries to device-centric protection. This shift brought a wave of mobile-first security incidents, with breach detection times getting significantly longer when mobile endpoints are involved [2].

Zero Trust architecture breaks away from traditional security approaches that assume anything inside the network can be trusted. Instead, this security model operates on the principle that every access request needs constant verification, regardless of where it comes from or whether the user was previously authenticated. Implementing this approach requires evaluating multiple environmental factors: user identity validation, device security posture analysis, geographic location verification, network characteristics assessment, and behavior pattern identification.

Mobile environments create unique challenges for Zero Trust that set them apart from desktop-focused security models. Mobile devices constantly move between different network environments—jumping from enterprise-managed Wi-Fi to cellular networks with varying security requirements to public hotspots with little to no control. This constant connectivity change creates shifting risk profiles that traditional static security controls struggle to handle effectively.

Mobile users also have different expectations than desktop users. They want instant access and seamless experiences, which security requirements often compromise. Authentication steps that take too long lead to

high abandonment rates for enterprise apps, while multi-factor authentication can significantly extend task completion times. This tension between security and usability represents one of the key challenges organizations must balance to maintain operational security while keeping users satisfied.

Current market research shows that mobile security has become the top technology priority for enterprises, with organizations making substantial annual investments in mobile security infrastructure. However, implementation success rates remain challenging, with relatively few organizations successfully deploying comprehensive mobile security frameworks that meet productivity benchmarks. This implementation gap highlights the critical need for security architectures specifically designed to support mobile-first operational models while maintaining user experiences that drive adoption and deliver business value.

The economic impact of this security-usability tension is substantial. Businesses lose significant productivity each year due to mobile security friction, yet they also face considerable breach costs when mobile security architectures prove inadequate. These competing pressures demand sophisticated solutions that can dynamically balance security requirements with operational effectiveness, responding to threat conditions in real-time while preserving seamless user experiences that align with business objectives.

2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Mobile Security Paradigms Evolution

Mobile security didn't start where it is today—it went through several distinct phases as companies figured out what actually works. In the early days, when smartphones first entered the workplace, IT departments focused on controlling the entire device through Mobile Device Management (MDM) solutions. During this phase, organizations applied security policies to entire devices, and MDM solutions became widely adopted in enterprises for managing corporate mobile deployments.

Early mobile security solutions concentrated on device configuration control, application installation restrictions, and remote wipe capabilities for compromised devices. What companies learned during this time was that while basic security policies achieved high compliance rates, users pushed back hard due to privacy concerns about monitoring personal devices. This approach became increasingly inadequate as Bring Your Own Device (BYOD) policies gained popularity, creating complex scenarios that required enterprise security controls without violating user privacy.

Application-based security emerged when organizations recognized the limitations of device-level security solutions. This led to Mobile Application Management (MAM) technology and application wrapping solutions that provided more granular security at the application level without compromising device autonomy. The results during this transition period showed impressive improvements in enterprise mobility management capabilities.

Detailed security incident analysis from multiple enterprise deployments confirmed that application-level security controls offered better protection than device-only approaches. Application-based security implementations demonstrated significant reductions in data breach incidents along with improved user satisfaction on enterprise mobility platforms [3].

Today's identity-focused security era represents a fundamental redefinition of mobile security architecture. This approach recognizes that effective security requires integrating user identity authentication, contextual risk analysis, and adaptive policy enforcement into a unified framework rather than relying solely on device or application attributes. Identity-centric solutions have shown measurable improvements in security effectiveness, with better breach detection rates and fewer false positives compared to previous models.

2.2 Zero Trust Architecture Foundations

Zero Trust architecture represents a comprehensive security philosophy built on foundational principles that fundamentally distinguish it from traditional perimeter-based security models. The architecture emerged from the recognition that traditional network security assumptions became less valid in distributed computing environments. Early Zero Trust thinking focused on explicit verification requirements, least-privilege access implementation, and operating principles that assume breaches will occur.

Modern Zero Trust models have evolved significantly from these early concepts, incorporating sophisticated risk-based assessment techniques and dynamic policy management systems. Analysis of enterprise Zero Trust implementations shows dramatic reductions in security incident severity without compromising system performance to unacceptable levels.

Current Zero Trust deployments incorporate core principles that guide architectural design choices and policy development. These principles establish end-to-end protection requirements for computing services and data sources, mandate that all communications be encrypted and authenticated, enforce per-session authorization, implement dynamic policies through real-time risk assessment, maintain continuous asset monitoring, require dynamic authentication processes, and enable informed security policy decisions through comprehensive data collection [4].

2.3 Mobile-Specific Zero Trust Challenges

Mobile computing environments present unique implementation challenges that distinguish them from traditional enterprise Zero Trust deployments. Device heterogeneity creates complex management scenarios requiring support for multiple operating systems, hardware configurations, and emerging form factors. Modern enterprise environments must accommodate diverse mobile device ecosystems while maintaining consistent security policies.

Network mobility presents a fundamental challenge that separates mobile Zero Trust deployments from fixed enterprise implementations. Mobile endpoints move between network environments with different security profiles, requiring dynamic policy adjustments and continuous risk re-evaluation. Enterprise mobile clients frequently connect to diverse network infrastructures with varying security postures.

Computational resource limitations significantly influence mobile Zero Trust implementation approaches. Battery life requirements and processing power constraints demand optimized security algorithms and careful use of resource-intensive security controls. Mobile user behavior patterns differ substantially from desktop computing environments, creating different security considerations including location-based access requirements and context-dependent usage patterns.

Security Paradigm	Core Technologies & Approaches	Key Characteristics & Outcomes
Device-Centric Security (2007-2012)	Mobile Device Management (MDM), device configuration control, and remote wipe capabilities	High compliance rates for basic policies, but significant user resistance due to privacy concerns, inadequate for BYOD environments
Application-Centric Security (2013-2018)	Mobile Application Management (MAM), application wrapping solutions, and granular app-level controls	Superior protection compared to device-only approaches, significant reductions in data breach incidents, and improved user satisfaction
Identity-Centric Security (2019-present)	User identity verification, contextual risk assessment, dynamic policy enforcement	Enhanced breach detection capabilities, reduced false positive rates, and integration of behavioral and contextual factors
Zero Trust Implementation	Explicit verification, least-privilege access, continuous monitoring, dynamic authentication processes	Substantial reductions in security incident severity, comprehensive protection for distributed computing environments, and real-time risk assessment

Table 1: Mobile Security Architecture Progression: From Device-Centric to Zero Trust Models [3, 4]

3. Zero Trust Architecture Principles in Mobile Environments

3.1 Adaptive Authentication Mechanisms

Adaptive authentication sits at the heart of mobile Zero Trust. Rather than asking for the same login credentials every time, these systems get smarter—they look at the situation and decide how much verification is really needed. Mobile banking applications demonstrate successful adaptive authentication implementation through sophisticated risk assessment systems that evaluate contextual variables and environmental conditions to determine appropriate security controls.

Modern mobile banking applications use multi-factor risk-scoring algorithms that analyze extensive contextual parameters including device fingerprinting attributes, geolocation analysis, behavioral biometrics, and

network security assessments. These systems apply minimal authentication requirements when users access from known devices and established locations, typically using primary credentials or standard biometric identification methods.

When unusual conditions are detected—such as access attempts from unfamiliar geographic locations, unknown devices, or suspicious network environments—systems proportionally increase authentication requirements. Enhanced verification might include additional factors like SMS-based one-time passwords, hardware token verification, or advanced biometric authentication using voice recognition and behavior pattern analysis.

Implementation results across various financial institutions demonstrate that adaptive authentication dramatically reduces authentication friction for routine transactions without compromising security effectiveness. The sophistication of risk assessment algorithms and granular contextual data collection represent key success factors for effective adaptive authentication deployment [5].

3.2 Microsegmentation and Least-Privilege Access

Microsegmentation in mobile environments enforces granular access controls that restrict user permissions to the minimum required for specific task completion. This approach allows employees in similar organizational roles to have different access levels based on their specific responsibilities and operational context.

Enterprise mobile applications implement microsegmentation through role-based access control and attribute-based access control technologies that evaluate multiple authorization criteria in real-time. Access control implementations consider user role hierarchies, device security posture, network environmental conditions, time-based access constraints, and data sensitivity classifications. Advanced microsegmentation implementations use policy engines that evaluate access requests in real-time, considering user credentials, device trust indicators, network security ratings, and current data sensitivity labels. These systems must support offline operational modes where devices function in isolated environments while maintaining security boundaries through cached permissions and locally maintained policy hierarchies.

3.3 Continuous Trust Scoring and Context Assessment

Zero Trust mobile frameworks implement continuous trust evaluation mechanisms that monitor risk conditions throughout entire user sessions, recognizing that threat environments change dynamically and require constant reassessment. Continuous trust scoring systems collect and analyze multiple data streams including device health indicators, behavioral analysis patterns, network security attributes, and location-based context information.

Device health assessment examines operating system compliance, installed application integrity, security software status, and compromise indicators. Behavioral analysis tracks user interaction patterns, application usage behaviors, and deviations from established baseline profiles. Network assessment analyzes environmental security characteristics including encryption protocols and threat intelligence correlation.

Advanced deployments use machine learning algorithms to process contextual data and generate accurate dynamic trust scores for risk determination while maintaining computational efficiency compared to traditional rule-based systems [6].

3.4 Context-Aware Security Controls

Context-aware security controls adjust authentication requirements based on requested action sensitivity and current risk conditions. Healthcare applications demonstrate sophisticated context-aware implementation through multi-tiered access systems that support clinical workflow requirements while ensuring regulatory compliance.

Medical personnel accessing patient records for routine operations experience minimal authentication overhead, while high-risk activities like controlled substance prescriptions or critical medical record modifications require more stringent verification processes involving biometric validation and supervisor authorization workflows.

Implementing context-aware controls requires robust classification systems that categorize data sensitivity levels and action risk types, establishing security policy frameworks that balance protection requirements with operational efficiency needs.

Zero Trust Principle	Implementation Approach	Key Features & Applications
Adaptive Authentication Mechanisms	Multi-factor risk scoring algorithms analyzing device fingerprinting, geolocation, behavioral biometrics, and network security assessments	Dynamic security protocols that adjust verification requirements based on risk; minimal authentication for recognized devices/locations, escalated verification for anomalous conditions
Microsegmentation and Least-Privilege Access	Role-based access control (RBAC) and attribute-based access control (ABAC) with policy engines evaluating real-time access requests	Granular access controls restricting user permissions to minimum task requirements; considers user roles, device posture, network environment, and data sensitivity classifications
Continuous Trust Scoring and Context Assessment	Machine learning algorithms process device health, behavioral patterns, network characteristics, and location-based context information	Real-time monitoring throughout user sessions; evaluates operating system compliance, application integrity, user interaction patterns, and environmental security characteristics
Context-Aware Security Controls	Multi-tiered access systems with comprehensive classification of data sensitivity levels and action risk categories	Authentication requirements adapt based on action sensitivity; healthcare applications demonstrate minimal overhead for routine access, enhanced verification for high-risk actions like controlled substance prescriptions

Table 2: Mobile Zero Trust Security Framework: Core Components and Operational Characteristics [5, 6]

4. Implementation Strategies and Case Studies

4.1 Implementation of Financial Services

Banks and financial companies have been the early adopters of mobile Zero Trust, and for good reason—they're sitting on exactly the kind of sensitive data that hackers want most, plus regulators are breathing down their necks. Large-scale banking deployments have focused on building integrated identity and access management platforms that extend and integrate with existing core banking environments while providing enhanced security capabilities for mobile channels.

Financial institution deployments utilize sophisticated device fingerprinting technologies that can identify unique devices with high accuracy, even when users attempt to obscure device characteristics. Risk assessment algorithms analyze comprehensive contextual factors in real-time, including transaction pattern analysis, geographic consistency verification, device security posture assessment, and behavioral biometric validation.

Behavioral biometric integration has become a cornerstone of modern mobile banking security, analyzing user interaction patterns including typing rhythm, touch pressure, device handling, and navigation behaviors to create individual user profiles. These systems continuously monitor user behavior during sessions, detecting anomalous behaviors that might indicate account compromise or fraudulent access. Deployment results show substantial improvements in fraud detection with minimal impact on legitimate user experiences [7].

Major implementation challenges include complex integration requirements with existing legacy core banking systems, multi-jurisdictional regulatory compliance management, and comprehensive training programs for customer service representatives. Financial institutions address these challenges through carefully planned phased rollout strategies, extensive testing programs, and comprehensive staff training initiatives.

4.2 Healthcare Enterprise Deployment

Healthcare organizations face unique mobile security implementation challenges due to regulatory compliance requirements, clinical workflow constraints, and the mission-critical nature of patient care operations. Large health system implementations demonstrate industry-specific considerations that address healthcare operational requirements.

Healthcare deployments implement mobile Zero Trust architectures that integrate with Electronic Health Record systems, medical device management platforms, and clinical communication applications. Solutions use federated identity management approaches that provide single sign-on access to clinical applications while maintaining granular access controls based on roles, locations, and patient care relationships.

Clinical workflow analysis reveals that traditional authentication methods can significantly impact patient interaction efficiency. Advanced implementations use innovative biometric authentication technologies including palm vein scanning and behavioral keystroke analysis to provide seamless authentication experiences that minimize time requirements for routine clinical interactions.

Privacy protection capabilities include dynamic data masking functionality that automatically adjusts information visibility based on user roles and care relationships. Clinicians receive complete patient information for their assigned patients while accessing summary data for other patients, significantly reducing potential privacy violations while maintaining workflow efficiency [8].

4.3 Manufacturing and Industrial Implementation

Manufacturing environments present challenges requiring operational technology integration, industrial device constraints, and production continuity requirements. Global manufacturing deployments have developed hybrid Zero Trust architectures that support both traditional information technology systems and industrial control systems.

Manufacturing deployments accommodate mobile devices used by maintenance technicians, quality inspectors, and production supervisors who require access to administrative systems and real-time production data from manufacturing equipment. Device management policies vary based on operational roles and facility locations, with enhanced security controls for devices accessing critical production systems.

4.4 Performance and Scalability Considerations

Mobile Zero Trust deployments must address performance and scalability challenges that affect user experience and system reliability. Large-scale deployments require comprehensive architectural planning to prevent security controls from negatively impacting performance characteristics or increasing latency and resource consumption beyond acceptable levels. Performance optimization strategies include leveraging edge computing for latency-sensitive operations, implementing intelligent policy decision caching, and using adaptive compression techniques that balance security requirements with bandwidth efficiency.

Implementation Sector	Key Technologies & Approaches	Primary Challenges & Outcomes
Financial Services	Unified identity and access management platforms, sophisticated device fingerprinting, behavioral biometric integration, analyzing typing rhythm, touch pressure, and navigation behaviors	Complex legacy system integration, multi-jurisdictional regulatory compliance, and substantial improvements in fraud detection while maintaining seamless user experiences for legitimate users
Healthcare Enterprise	Electronic Health Record system integration, federated identity management with single sign-on capabilities, palm vein scanning, behavioral keystroke analysis, and dynamic data masking	Clinical workflow constraints, regulatory compliance requirements, patient care efficiency, minimized authentication time for routine interactions, while reducing privacy violations through role-based information visibility
Manufacturing and Industrial	Hybrid Zero Trust architectures accommodating IT and industrial control systems, role-based device management policies, and operational technology integration	Industrial device constraints, production continuity demands, operational technology integration, enhanced security controls for critical production system access, while supporting diverse mobile workforce roles

Table 3: Industry Case Studies: Mobile Zero Trust Deployment Approaches and Key Characteristics [7, 8]

5. Future Directions

5.1 Emerging Trends and Technologies

Several emerging technological developments are set to transform mobile Zero Trust deployments in enterprise environments. Machine learning and artificial intelligence capabilities continue experiencing rapid advancement, enabling far more accurate risk assessment frameworks with significantly reduced false positives. Modern machine learning models show dramatic accuracy improvements over traditional rule-based systems, using neural network architectures that analyze behavioral patterns and threat indicators with sophisticated pattern recognition capabilities that continuously evolve to address changing threat landscapes. Edge computing deployment represents a transformative shift in mobile security architecture, relocating security decision-making capabilities closer to end-users and significantly reducing authentication latency while improving offline operational scenarios. Edge-based security solutions can process authentication requests with exceptional response times while maintaining security effectiveness even during network connectivity disruptions. Distributed edge computing architectures support localized policy enforcement and risk analysis, reducing dependency on centralized security infrastructure while maintaining consistent security postures across geographically distributed mobile workforces.

Quantum-resistant cryptographic algorithms are undergoing intensive testing and preparation for mobile deployment scenarios as quantum computing threats transition from theoretical concerns to practical challenges requiring immediate attention. Post-quantum cryptography research focuses on developing encryption technologies that maintain computational efficiency suitable for resource-constrained mobile devices while providing long-term security against quantum computing attacks. Deployment planning for quantum-resistant algorithms must consider mobile device computational limitations, battery life impacts, and performance requirements for real-time security operations [9].

Behavioral biometrics technologies are advancing beyond traditional keystroke analysis to encompass sophisticated recognition capabilities including gait pattern analysis, voice characteristic identification, and cognitive behavioral assessment. Modern behavioral biometric systems can identify users through distinctive walking patterns captured by smartphone sensors, voice pattern recognition during communications, and cognitive response patterns during application interactions.

5.2 Research Opportunities

Future research initiatives present significant opportunities for enhancing mobile Zero Trust effectiveness. Developing standardized metrics for quantifying Zero Trust effectiveness in mobile environments represents a high-priority research area, as organizations currently lack standardized approaches for measuring security improvements and operational benefits. Research into privacy-preserving techniques for behavioral analysis addresses growing user privacy concerns while maintaining security effectiveness.

Quantum-resistant security protocols specifically designed for resource-limited mobile devices constitute an immediate research priority as quantum computing capabilities advance. Research must address computational and energy efficiency challenges of post-quantum cryptographic algorithms without sacrificing security effectiveness equivalent to current encryption standards [10].

5.3 Industry Implications

Successful mobile Zero Trust architecture deployment has broad implications for industry practices, compliance frameworks, and competitive positioning across multiple sectors. Organizations achieving comprehensive Zero Trust implementations can realize competitive advantages through superior security postures, enhanced user experiences, and increased operational agility that enables rapid response to changing business requirements. Regulatory bodies are incorporating Zero Trust principles into compliance frameworks, with several jurisdictions considering mandatory Zero Trust implementation requirements for specific industry sectors. This regulatory evolution will accelerate adoption timelines and standardization across industries while creating market pressures for widespread Zero Trust deployment.

Future Direction Category	Key Technologies & Developments	Impact & Implementation Considerations
Artificial Intelligence &	Neural network architectures with sophisticated pattern recognition capabilities, advanced risk assessment	Significant accuracy improvements over traditional rule-based systems, continuous adaptation to evolving threat

Machine Learning	mechanisms with reduced false positive rates	landscapes, and enhanced behavioral pattern processing
Edge Computing Deployment	Distributed edge computing architectures, localized policy enforcement and risk assessment, proximity-based security decision-making	Transformative shift relocating security processes closer to end-users, exceptional authentication response times, improved offline operational capabilities during network disruptions
Quantum-Resistant Cryptography	Post-quantum cryptographic algorithms designed for resource-constrained mobile devices, computational efficiency optimization for real-time operations	Preparation for quantum computing threats, transitioning from theoretical to practical concerns, consideration of mobile device limitations, battery life impacts, and performance requirements
Advanced Behavioral Biometrics	Gait pattern analysis through smartphone sensors, voice characteristic identification, cognitive behavioral assessment beyond keystroke analysis	Sophisticated recognition capabilities enabling continuous authentication without explicit user actions, unique user identification through walking patterns, and cognitive response analysis
Research Opportunities & Industry Implications	Standardized Zero Trust effectiveness metrics, privacy-preserving behavioral analysis techniques, and mandatory regulatory compliance frameworks	Critical research priorities for evaluation methodologies, competitive advantages through comprehensive implementations, and accelerated adoption timelines driven by regulatory evolution

Table 4: Mobile Zero Trust Evolution Framework: Technological Advances and Industry Transformation [9, 10]

CONCLUSION

The move from traditional network security to Zero Trust isn't just an upgrade—it's a completely different way of thinking about protection. The old approach of building digital walls doesn't work when everyone's working on phones and tablets from coffee shops and home offices. This comprehensive review demonstrates that Zero Trust principles can be successfully implemented in mobile environments through sophisticated adaptive authentication systems that dynamically adjust security requirements based on contextual risk assessment, microsegmentation approaches that implement granular access controls limiting user permissions to minimum operational requirements, continuous trust scoring mechanisms that monitor risk conditions throughout entire user sessions, and context-aware security controls that balance protection needs with operational efficiency requirements.

Real-world implementation experiences across diverse industry sectors including financial services, healthcare, and manufacturing show that organizations can achieve substantial security improvements while maintaining or enhancing user satisfaction through carefully planned deployment strategies that emphasize user-centered design principles alongside comprehensive security frameworks. Emerging technologies including artificial intelligence-powered risk assessment capabilities, edge computing architectures that relocate security decision-making closer to end-users, quantum-resistant cryptographic approaches optimized for resource-constrained mobile devices, and advanced behavioral biometric solutions incorporating gait recognition and voice pattern identification will continue driving innovation in mobile Zero Trust implementations.

Regulatory authorities are increasingly incorporating Zero Trust principles into compliance frameworks, creating market pressures for comprehensive deployment across industry sectors. Organizations that excel in these implementations gain competitive advantages through enhanced security postures, improved user experiences, and increased operational agility that enables rapid adaptation to evolving business requirements and threat environments.

REFERENCES

1. Josh Howarth, "How Many People Own Smartphones? (2025-2029)," Exploding Topics, 2025. Available: https://explodingtopics.com/blog/smartphone-stats
2. Lund S, et al., "The future of work after COVID-19. San Francisco, CA: McKinsey Global Institute, 2021. Available: https://lmic-cimt.ca/future-of-work/lund-s-madgavkar-a-manyika-j-smit-s-ellingrud-k-meaney-m-robinson-o-2021-february-18-the-future-of-work-after-covid19-san-francisco-ca-mckinsey-global-institute-2/
3. Asaf Shabtai, et al., "Google Android: A Comprehensive Security Assessment," ResearchGate, 2010. Available: https://www.researchgate.net/publication/224107182_Google_Android_A_Comprehensive_Security_Assessment
4. Scott Rose (NIST), et al., "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020. Available: https://csrc.nist.gov/pubs/sp/800/207/final
5. N.L. Clarke AND S.M. Furnell, "Advanced user authentication for mobile devices," Computers & Security, 2007. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404806001428
6. Anam Sajid and Haider Abbas, "Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges," J Med Syst, 2016. Available: https://pubmed.ncbi.nlm.nih.gov/27155893/
7. Oceano Be, "Integrating Behavioral Biometrics into Mobile Banking," 2025. Available: https://oceanobe.com/news/integrating-behavioral-biometrics-into-mobile-banking/1662
8. Abdullah Alabdulatif, "Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users," Information, 2025. Available: https://www.mdpi.com/2078-2489/16/3/219
9. Sebastian Paul and Patrik Scheible, "Towards Post-Quantum Security for Cyber-Physical Systems: Integrating PQC into Industrial M2M Communication," Computer Security – ESORICS, 2020. Available: https://link.springer.com/chapter/10.1007/978-3-030-59013-0_15
10. Sherali Zeadally, et al., "Design architectures for energy harvesting in the Internet of Things," Renewable and Sustainable Energy Reviews, 2020. Available: https://www.sciencedirect.com/science/article/abs/pii/S136403212030188X