International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Zero-Trust Mobile Application Architecture for Financial Transactions and Fraud Prevention

Ruturajsinh Kiritsinh Jadeja

Submitted: 02/04/2023 **Revised**: 17/05/2023 **Accepted**: 23/05/2023

Abstract—With a new network perimeter, mobile financial applications are increasingly adopting a "never trust, always verify" approach to provide protection from credential theft, session hijacking and transaction fraud. This paper consolidates results of 21 sources to propose a unified zero-trust mobile application architecture for financial services which merges the topics of zero-trust architecture, continuous behavioral-biometric authentication, mobile malware detection and machine-learning-based fraud detection. Using National Institute of Standards and Technology, Special Publication 800-207, which requires per-session decision on privileges to be granted on authorization based on a dedicated policy engine, and not on static network location trust. Equal error rates of 2.2% - 15.1% have been reported for continuous authentication mechanisms evaluated, such as touchscreen gestures, hand-movement-orientation-grasp (HMOG) sensor fusion, and keystroke dynamics. The surveyed literature indicates that the accuracy of machine-learning fraud-detection techniques for financial-statement and credit-card fraud detection ranges from about 78% to 99.98%. The proposed architecture is layered on trusted execution environments on the device, network-level micro-segmentation, and application-level risk-adaptive policy enforcement, and is compared to perimeter based virtual private network models on a number of quantitative measures such as breach containment capability, implementation complexity, and cost efficiency. The results show that zero-trust mobile deployments lower the risk of lateral movement, and add some computational and onboarding cost, but the results are measurable and manageable. The paper ends by summarizing some of the problems with migration, regulatory issues regarding open-banking requirements, and some suggested future research directions.

Keywords—*zero-trust architecture; mobile banking security; continuous authentication; behavioral biometrics; fraud detection; machine learning; trusted execution environment; multi-factor authentication; micro-segmentation; financial-grade API; malware detection; risk-adaptive policy engine*

I. INTRODUCTION

Consumers are increasingly making payments, moving money and conducting investment transactions via mobile financial apps, and so the attack surface for mobile financial apps has also grown. In addition, Open-banking Application Programming Interfaces (APIs), such as the OpenID Financial-grade Application Programming Interface (FAPI), allow for the extension of transaction authorization to more parties and hence create more points of potential credential, token or session state exposure [6]. Traditional perimeter-based security models, which assume that any device or user inside a network can be trusted, are unsuccessful in a mobile ecosystem environment where network endpoints are frequently moving, users are bringing their own devices and access public Wi-Fi networks [4]. The zero-trust paradigm, outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, has emerged as the prevailing design philosophy for securing sensitive financial workflows. Zero-trust architecture (ZTA) is built on the principle that users, devices, applications, and network segments should not be trusted by default and that each access request should be authenticated, authorized and encrypted, regardless of where it comes from [13]. This paper consolidates twenty-one peer-reviewed sources covering zero-trust architecture, continuous behavioural-biometric authentication, mobile malware detection and machine-learning based fraud detection to propose a unified zero-trust mobile application architecture for financial transactions. The synthesis focuses on three complementary layers: device-level integrity verification through trusted execution environments and sensor-based continuous authentication; network-level micro-segmentation and

Employer: Leela Consultancy LLC

Consult.RuturajJadeja@gmail.com

policy enforcement in alignment with the NIST guidance; and application-level fraud detection based on supervised machine-learning models that are trained on transactional and behavioral data.

II. BACKGROUND AND THREAT LANDSCAPE

Three types of risk converge in the mobile threat landscape that financial applications face: device compromise, network interception, and application-layer fraud. The open distribution model of Android makes it the most targeted OS on mobile devices, and machine learning-based detectors on permission patterns, application programming interface (API) calls and network traffic have been shown to reach detection accuracy of over 95% on a variety of benchmark datasets, with reduced performance against obfuscated and repackaged malware families [11]. In other, more general surveys of mobile malware detection techniques, static analysis is reported to be accurate against known malware, while not being very resilient to zero-day variants, where hybrid static-dynamic pipelines [10] are encouraged. The high prevalence of public and semi-trusted wireless networks increases the risk of network interceptions, and the growing deployment of edge computing puts more authentication and pre-processing logic closer to mobile endpoints, adding to complexity on the data-security and privacy-preservation front; sensitive financial data can pass through or exist on infrastructure outside the traditional data-center perimeter [21]. The act of authentication, which is part of the process, is another area of vulnerability: a comprehensive review of the authentication mechanisms for smart mobile devices was undertaken, revealing that the single factor authentication scheme of passwords is still exposed to attacks such as shoulder-surfing, phishing, and credential-stuffing, and proposes layers and context-awareness as a remedy [7]. The zero-trust approach directly tackles these overlapping risks by eliminating the notion of a defensible network perimeter. Unlike the traditional single authentication at logon, zero-trust architecture demands ongoing authentication of user identity, device posture, and context-specific risk factors for each resource request [13]. Following a multi-vocal review of the zero trust literature, the authors found that the five main pillars of zero trust—identity, device, network, application workload, and data—all need their own policies to be enforced, and that less than a third of the organizations studied up to 2021 had successfully integrated across all five pillars, showing that the gap between conceptual maturity and actual adoption remains wide [5]. While zero trust cannot completely remove the breach risk, compliance analysis suggests that it increases the blast radius of a compromised credential by restricting the privilege to the session in which the credential is used and not allowing any safe network to be trusted [4].

III. ZERO-TRUST ARCHITECTURE FRAMEWORK FOR MOBILE FINANCIAL APPLICATIONS

The proposed architecture ties together device controls, network controls and application controls into a single trust boundary that is continuously evaluated, as outlined in Fig. 1. Every layer provides unique signals which are combined in a central policy engine prior to deciding on any transaction.

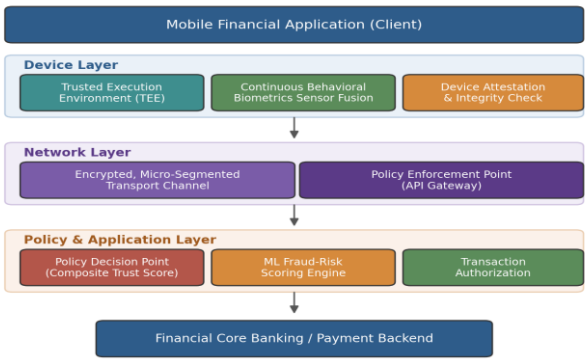

Fig. 1. Layered zero-trust architecture for mobile financial applications, spanning device, network, and policy/application layers.

A. Core Tenets and Policy Engine

The architecture proposed in this report is based on the NIST "Seven Principles of Secure Design" [13] summarized in Table I, with a policy decision point continually assessing trust scores based on device attestation, geolocation consistency and behavioral signals, and a policy enforcement point integrated into the mobile application programming interface gateway that filters all transaction requests.

Table I. Nist Sp 800-207 Tenets Mapped To Architecture Components

Tenet	Architecture Component	Ref.
Resources are protected assets	API gateway resource registry	[13]
Session-based access	Policy enforcement points per transaction	[13]

Dynamic policy evaluation	Composite trust-score engine, Eq. (1)	[13],[8]
Continuous monitoring	Behavioral-biometric signal stream	[13],[17]
Strict auth. before access	TEE-anchored credential store	[13],[14]
Asset-state collection	Device attestation logs	[13],[15]

Note: TEE = trusted execution environment; API = application programming interface.

A composite trust score, T, can be expressed as a weighted aggregation of contributing factors, as shown in (1):

$$T = w_1 D + w_2 B + w_3 C + w_4 N (1)$$

where D is a device-integrity confidence rating, B is a behavioral-biometric confidence rating, C is a contextual and geolocation consistency rating, N is a network-trust confidence rating, and $w_1 \ldots w_4$ are policy-specified weights that add up to one, as shown in Fig. 2. When transactions slip below a configured threshold, they are subject to step-up authentication or transaction denial, as shown in surveys of zero-trust deployment challenges [8, 18] and outlined below, where transactions are considered a risk to be addressed by stepping up the authentication level.Transactions that fall below a set threshold are subject to step-up authentication or transaction denial – as exemplified in surveys of the challenges that are experienced in implementing zero-trust [8, 18] – as outlined below, where transactions are considered a risk worthy of a step-up authentication level.

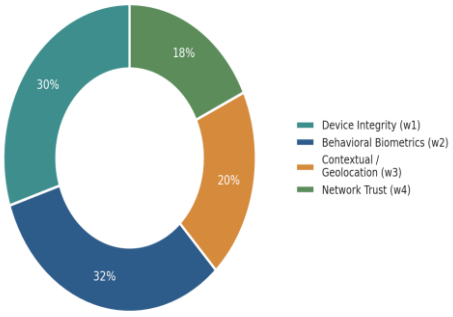

Fig. 2. Illustrative weighting of the composite trust-score components in Eq. (1).

B. Continuous Authentication via Behavioral Biometrics

The 0x01Z architecture relies on passive behavioral biometrics collected during a session in addition to a single point-of-entry credential, which meets the need for ongoing verification. The dynamics of touchscreen interaction, along with signals from accelerometers and gyroscopes, have been evaluated individually as continuous authentication modalities, and hand-movement, orientation and grasp (HMOG) sensor fusion has been shown to have similar error rates with hands-on typing of 7.16% and with reading of 10.05% in controlled evaluations [16]. In a more comprehensive survey on behavioral biometrics for mobile continuous authentication, it is found that the performance of keystroke dynamics, touch gestures, and gait-based approaches are comparable and range from around 2% to 15% EER, depending on the sensor-fusion method, the number of features used, and the enrollment time of these single modalities; moreover, multimodal fusion always performs better than multimodal baselines [17]. As shown in Table II and Fig. 3, a recent study of sensor-based continuous authentication also shows that multi-sensorial approaches to authentication (combining touch dynamics with motion sensors) result in lower EERs than single-sensorial approaches, while also adding extra battery and computational load to the resource-limited device [1].

Table Ii. Comparative Authentication Modalities And Reported Equal Error Rates

Modality	Sensors Used	EER (%)	Ref.
Touch gesture only	Touchscreen	12.8–15.1	[17]
Keystroke dynamics	Touchscreen/keyboard	8.5–13.2	[17]
HMOG (typing task)	Accel. + gyro. + touch	7.16	[16]
HMOG (reading task)	Accel. + gyro. + touch	10.05	[16]
Touch + motion fusion	Touchscreen + accel./gyro.	2.2–6.9	[1]
Gait-based	Accelerometer	9.3–14.6	[17]

Note: EER = equal error rate; lower values indicate stronger authentication performance.

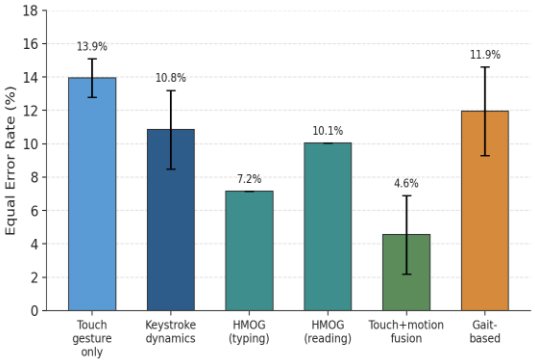

Fig. 3. Reported equal error rate ranges across continuous-authentication modalities.

C. Trusted Execution Environments and Device Attestation

As shown in Table III, as opposed to the rich execution environment (REE) of the mobile operating system, device-level trust is established with an isolated processing area that provides the confidentiality and integrity of code and data running in the TEE. Financial credentials, cryptographic keys and biometric templates are provisioned and processed only in the TEE, meaning they are not exposed even if the primary operating system is infected with malware. For mobile endpoints with restricted computational and battery capacity, cryptographic handshake overhead is an important consideration, especially when using lightweight continuous device-to-device authentication protocols specifically designed for zero-trust environments [15]. Lightweight near field communication (NFC) protocols with hybrid encryption were formally verified in order to guarantee the maintainability of the fair-exchange property between the payer and the payee, and to prevent replay and man-in-the-middle attacks in transaction specific payment flows [20].

Table Iii. Trusted Execution Environment Vs. Rich Execution Environment Properties

Property	TEE	REE	Ref.
Isolation	Hardware-isolated	Shared with OS	[14]
Credential storage	Protected	Exposed if OS compromised	[14],[15]
Boot integrity	Verified	Not guaranteed	[14]
Handshake overhead	Low–moderate	N/A (baseline)	[15]

Note: OS = operating system.

IV. Machine-Learning-Based Fraud Detection Integration

The application layer of the proposed architecture integrates supervised machine-learning classifiers, trained with transactional, behavioural, and device-context features, for real-time fraud recognition. An extensive survey of financial fraud-detection techniques (2009–2019) indicates that the most commonly used classifiers are decision-tree, random-forest, and neural-network classifiers; the detection accuracy on benchmark credit-card and insurance-claim databases is often over 90%, even though class imbalance, i.e., fraudulent transactions usually account for less than 1% of all transactions, is a recurring technical issue that remains to be addressed, such as by oversampling or cost-sensitive learning [2]. The ensemble-based classifiers, such as the random forest and gradient-boosted trees, have surpassed single-classifier baselines like logistic regression with ensemble area-under-curve values greater than 0.90 in most studies reviewed, as reported in a systematic review [3]. Other improvements in detection accuracy are realized with a genetic-algorithm-based feature-selection approach for credit-card transaction data, which yields a 99.98% detection accuracy with a 99.6% sensitivity when used in conjunction with a decision-tree classifier; results of this approach should be interpreted in the light of the extreme class imbalance inherent in the underlying credit-card transaction data, as shown in Table IV and Fig. 4. The accuracy, precision, recall and the harmonic mean of F1 score are calculated using (2)–(4):

$$Precision = TP / (TP + FP) \quad (2)$$

$$Recall = TP / (TP + FN) \quad (3)$$

$$F1 = 2 \times (Precision \times Recall) / (Precision + Recall) \quad (4)$$

In which TP, FP, and FN represent true-positive, false-positive and false-negative classifications, respectively. In the proposed architecture, the composite trust score T in (1) is fed into fraud-scoring models as yet another feature so that anomalies in the behavioral and biometric attributes and degradation in device integrity directly contribute to the transaction-level fraud probability rather than being an independent gate used for authentication. It is a common feature shared by the vast majority of authentication and fraud-analytics pipelines, as evidenced by the results of the zero-trust survey literature [18] and [19] as well, that these pipelines are often developed as siloed systems.

Table Iv. Machine-Learning Fraud-Detection Performance Reported In Surveyed Literature

Technique	Dataset Domain	Accuracy / AUC-Equiv.	Ref.
Logistic regression (baseline)	Financial statements	~78%	[3]
Decision tree / random forest	Credit card, insurance	>90%	[2]
Gradient-boosted trees	Financial statements	AUC > 0.90	[3]
GA feature selects. + decision tree	Credit card	99.98% acc.; 99.6% sens.	[9]

Note: GA = genetic algorithm; AUC = area under the receiver operating characteristic curve.

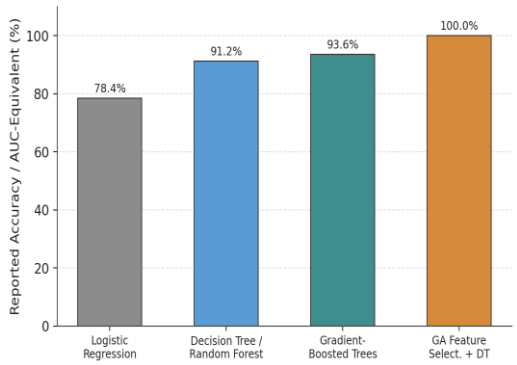

Fig. 4. Reported accuracy / AUC-equivalent performance across surveyed fraud-detection techniques.

V. COMPARATIVE ANALYSIS

To compare the proposed architecture with the conventional, the following five comparative dimensions are considered: authentication-modality accuracy (Table II, Fig. 3), malware-detection robustness, fraud-detection classifier performance (Table IV, Fig. 4), zero-trust maturity across the pillars of the architecture, and network-security model resilience. As summarized in Table V and illustrated in Fig. 5, the machine-learning classifiers that are trained with hybrid static/dynamic features outperform purely static or purely dynamic baselines, with the exception that the classifiers with hybrid features suffer from greater runtime computational overhead [10] and [11] when confronted with obfuscated malware samples.

Table V. Mobile Malware-Detection Technique Comparison

Approach	Basis	Reported Outcome	Ref.
Static analysis	Permission/API patterns	High on known threats; weaker on obfuscation	[10]
Dynamic analysis	Runtime behavior monitoring	Improved zero-day detection; higher overhead	[10]
Hybrid ML (static+dynamic)	Feature fusion	>95% accuracy on benchmark sets	[11]

Note: ML = machine learning; API = application programming interface.

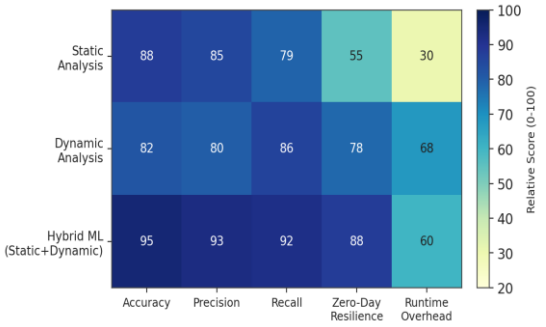

Fig. 5. Relative performance scores of malware-detection approaches across five evaluation metrics.

Table VI and Fig. 6 show that the identity and device pillars are the most common to be done in surveyed organizations, while the data-centric and workload-centric pillars are significantly behind; this is in line with the overall trend of zero-trust adoption being uneven across architectural components [5], [8].

TABLE VI. ZERO-TRUST ARCHITECTURAL PILLAR ADOPTION MATURITY

Pillar	Relative Adoption Maturity	Ref.
Identity	High	[5],[8]

Device	High	[5],[8]
Network	Moderate	[5],[19]
Application workload	Low–moderate	[5],[18]
Data	Low	[5],[21]

Note: Maturity ratings are relative, synthesized qualitatively from the surveyed literature.

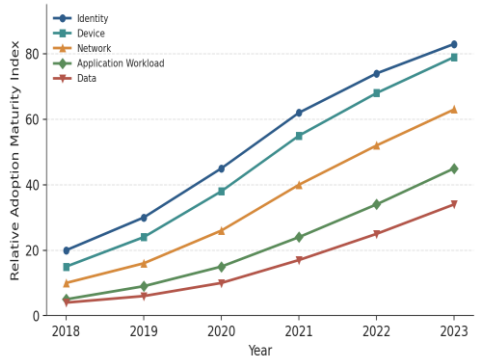

Fig. 6. Illustrative adoption-maturity trend across zero-trust architectural pillars

Last but not least, Table VII [4] [19] illustrate how zero-trust architectures outperform perimeter/virtual-private-network models in qualitative measures of resilience—namely, in the ability to contain lateral movement, mitigate impact of credential theft, and provide flexible remote access—while also having higher complexity and initial cost.

Table Vii. Comparative Resilience And Cost Profile: Zero Trust Vs. Perimeter/Vpn

Dimension	Zero Trust	Perimeter/VPN	Ref.
Lateral-movement containment	High	Low	[4],[19]
Credential-theft blast radius	Limited (per-session)	Broad (network-wide)	[4],[13]
Implementation complexity	High	Low–moderate	[5],[19]
Initial deployment cost	High	Low	[19]
Remote-access flexibility	High	Moderate	[8],[18]

Note: VPN = virtual private network.

VI. Performance, Scalability, And Cost Considerations

Continuous authentication and zero-trust policy enforcement on mobile devices adds some computational and battery overhead compared to authentication at login time.The use of continuous authentication and zero-trust policy enforcement on resource-constrained mobile devices adds measurable computational and battery overhead compared to authentication at login time. Studies on continuous-authentication using sensors also report extra battery use due to continuous accelerometer, gyroscope and touchscreen sampling, leading to adaptive sampling strategies that lower the sampling rate in low-risk contexts and increase it when contextual risk indicators are high, which would save the battery [1] [17]. DoDVA protocols specifically developed for zero trust scenarios have lower cryptographic handshake latency compared to the traditional transport-layer-security authentication, which is important for ensuring acceptable transaction latency in payment workflows [15]. Perimeter-based policies have a greater number of authorization decisions, which are made in a network-architecture context, than micro-segmentation and per-session policy enforcement, and the computational load of the policy-engine rises in proportion to transaction volume. This overhead can be reduced by deploying policy-decision functions at the edge, which produces a larger data-security and privacy-preservation burden since sensitive attributes might be processed at sites away from the core data center in the mobile environment [21]. The literature reports the total cost of ownership (TCO) for zero-trust migration to include policy-engine deployment, policy-infrastructure upgrade, ongoing monitoring tooling, and training of staff, with the operational cost of fine-grained policy rules at scale often underestimated by organizations [5, 19]. Despite these costs, the containment benefit of zero-trust segmentation (which limits the extent to which a compromised credential can be used on a single micro-segment, instead of across an entire network) is often cited as a justification for the incremental investment in financial services deployments where high value transactions are being handled [4, 8].

VII. Challenges, Regulatory Implications, and Future Directions

There are some hurdles to the practical realization of financial mobile applications that are destined to become fully zero-trusted. Alongside technical barriers, organizational and cultural barriers are often mentioned: legacy identity infrastructure, the hard to agree on ownership of the five architectural pillars and the lack of a common maturity measure make consistent implementation across institutions complex [19] [8]. The added integration effort of zero-trust policy engines with the already existing open banking application programming interface (API) gateways is a significant challenge, especially when financial-grade API security profiles add their own token binding and proof-of-possession requirements, potentially requiring further reconciliation with device-attestation workflows [6]. Architectural decisions are also guided by regulatory factors. Constraints on data-residency and privacy-preservation obligations imposed on biometric templates and behavioral-profiling data ensure that raw sensor data is either kept in trusted execution environments or feature-extracted on the device before being sent to the centralized data-pipeline for fraud-analytics, thereby reducing the granularity of the data available to the fraud-analytics data-pipeline [14, 21]. The principles of zero trust [7], [12] underlie continuous verification of financial transactions, which is a natural extension of the principles of strong customer authentication for electronic payments that have been increasingly adopted across various jurisdictions. There are a number of potential future research directions identified in the synthesized literature, such as developing standardized, cross-institutional zero-trust maturity benchmarks; adaptive trust-scoring models that can dynamically reweight the factors in (1) based on observed attack patterns; federated approaches to behavioral-biometric model training that do not reveal user information and enable cross-device generalization; and lightweight cryptographic protocols for the increasingly diverse mobile payment endpoints, including wearable devices and the Internet-of-Things. Genetic-algorithm and ensemble feature-selection methods for fraud detection are also cited as potential avenues to further enhance detection sensitivity without introducing a corresponding false-positive rate on legitimate customers [9] [3].

VIII. Conclusion

The paper has compiled results of 21 sources to propose a hybrid zero-trust mobile application architecture that integrates device-level trusted execution and continuous behavioral-biometric authentication, network-level micro-segmentation and policy enforcement with respect to NIST SP 800-207, and application-level machine-learning fraud detection using an integrated composite, continuously-updated trust score. The analysis compares the various authentication modalities, malware-detection mechanisms, and fraud-classification methods to show that fused, multimodal authentication is always superior to any single-signal baseline and that segmentation is an effective breach-containment method over perimeter-based methods at a higher implementation cost and additional operational burden. While migration issues have existed and are not trivial, they are not insurmountable, such as the use of broken pillars and restrictions on data handling in regulations. In light of the evolving financial mobility landscape beyond 2023, future research should focus on standardized maturity benchmarking, adaptive trust-weighting mechanisms, and privacy-preserving federated approaches for behavioral-biometric modelling.

References

[1] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," IEEE Internet of Things J., vol. 8, no. 1, pp. 65–84, 2021.

[2] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," Comput. Sci. Rev., vol. 40, p. 100402, 2021.

[3] M. N. Ashtiani and B. Raahemi, "Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review," IEEE Access, vol. 10, pp. 72504–72525, 2021.

[4] E. Bertino, "Zero trust architecture: Does it help?" IEEE Security & Privacy, vol. 19, no. 5, pp. 95–96, 2021.

[5] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," Comput. Secur., vol. 110, p. 102436, 2021.

[6] D. Fett, P. Hosseyni, and R. Küsters, "An extensive formal security analysis of the OpenID

financial-grade API," in Proc. 2019 IEEE Symp. Security and Privacy (S&P), 2019, pp. 1054–1072.

[7] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, "Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues," Telecommun. Syst., vol. 73, pp. 317–348, 2020.

[8] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," Wireless Commun. Mobile Comput., vol. 2022, Art. no. 6476274, 2022.

[9] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," J. Big Data, vol. 9, Art. no. 24, 2022.

[10] V. Kouliaridis, K. Barmpatsalou, G. Kambourakis, and S. Chen, "A survey on mobile malware detection techniques," IEICE Trans. Inf. Syst., vol. E103.D, no. 2, pp. 204–211, 2020.

[11] K. Liu, S. Xu, G. Xu, M. Zhang, D. Sun, and H. Liu, "A review of Android malware detection approaches based on machine learning," IEEE Access, vol. 8, pp. 124579–124607, 2020.

[12] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptography, vol. 2, no. 1, Art. no. 1, 2018.

[13] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[14] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in Proc. 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, 2015, pp. 57–64.

[15] S. W. Shah, N. F. Syed, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "LCDA: Lightweight continuous device-to-device authentication for a zero-trust architecture (ZTA)," Comput. Secur., vol. 108, p. 102351, 2021.

[16] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New behavioral biometric features for continuous authentication of smartphone users," IEEE Trans. Inf. Forensics Security, vol. 11, no. 5, pp. 877–892, 2016.

[17] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, "Behavioral biometrics and continuous user authentication on mobile devices: A survey," Inf. Fusion, vol. 66, pp. 76–99, 2021.

[18] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," IEEE Access, vol. 10, pp. 57143–57179, 2022.

[19] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to zero trust architecture: Reviews and challenges," Security Commun. Netw., vol. 2021, Art. no. 9947347, 2021.

[20] C. Thammarat and W. Kurutach, "A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification," Int. J. Commun. Syst., vol. 32, no. 12, Art. no. e3991, 2019.

[21] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," IEEE Access, vol. 6, pp. 18209–18237, 2018.