Vol. 7, No. 5, May 2026
E-ISSN:2723 – 6692 P-ISSN:2723– 6595
http://jiss.publikasiindonesia.id/

Zero Trust Architecture in Law Enforcement Mobile Governance: A Systematic Literature Review

Iwan Juniar Simanjutak*, Dana Indra Sensuse
Universitas Indonesia
Email: Iwan.juniar@ui.ac.id*, dana@cs.ui.ac.id

Keywords:
Zero Trust Architecture; law enforcement; mobile governance; cybersecurity; systematic literature review

Abstract

The expansion of mobile government has changed the operational environment of law enforcement agencies. Officers increasingly access case records, location-based applications, biometric systems, cloud repositories, and digital evidence workflows through mobile and distributed endpoints. These conditions challenge perimeter-based security and raise questions about how Zero Trust Architecture can support secure, accountable, and rights-sensitive mobile governance. This study reviews recent literature to synthesize how Zero Trust Architecture can be positioned within law enforcement mobile governance. A systematic literature review was conducted using a PRISMA-based protocol. The search used Scopus as the primary database and applied English-language, open-access, article, and 2020–2026 filters. From 96 initial records, duplicate removal, title and abstract screening, and full-text eligibility assessment produced 40 included articles. The synthesis shows that the literature is dominated by Zero Trust Architecture migration, dynamic access control, authentication, Internet of Things, edge, and 6G security, while studies directly linking Zero Trust Architecture to police mobile governance remain scarce. Four cross-cutting themes were identified: continuous identity and device verification, context- and risk-aware policy enforcement, evidence and data governance, and organizational readiness. The article proposes a governance-oriented Zero Trust Architecture framework for law enforcement mobile systems that connects technical controls with legal accountability, auditability, and public trust. The review concludes that Zero Trust Architecture should be treated not only as a cybersecurity architecture but also as a policy instrument for strengthening secure mobile public service delivery.

INTRODUCTION

Mobile governance has become an important expression of contemporary public administration because public agencies increasingly deliver services, manage field operations, and exchange data through mobile devices and platform-based applications (Castilla et al., 2023). In law enforcement, this transformation is more sensitive than ordinary public service digitalization because officers may use mobile systems for case reporting, identity verification, patrol coordination, forensic documentation, investigative interviews, and access to digital evidence. The development of mobile government services has therefore created a governance environment in which operational speed, inter-agency coordination, data accuracy, and security must be balanced with accountability, privacy, and procedural fairness (Alhanatleh et al., 2022; Gürler et al., 2024; Stoykova, 2024).

The security problem becomes more complex when law enforcement agencies operate beyond a traditional office network. Mobile devices are exposed to public networks, cloud resources, third-party applications, location-based services, and, in some cases, personally

owned or mixed-use devices. These conditions weaken the assumptions of perimeter-based protection. The National Institute of Standards and Technology defines Zero Trust as a cybersecurity paradigm that shifts defense from static network perimeters to users, assets, and resources, while requiring authentication and authorization before access to enterprise resources is granted (Rose et al., 2020). In this sense, Zero Trust Architecture is not simply a technical trend. It is a governance logic that assumes no implicit trust and requires continuous verification, least-privilege access, policy enforcement, and telemetry-driven decision-making.

The state of the art shows that Zero Trust Architecture has been widely examined in relation to enterprise migration, cloud computing, dynamic access control, the Internet of Things, edge computing, blockchain-enabled security, biometric authentication, 6G-enabled devices, and industrial infrastructures (Syed et al., 2022; Phiayura & Teerakanok, 2023; Xiao et al., 2022; Azad et al., 2024; Ameer et al., 2024). These studies provide important technical foundations, but they rarely place Zero Trust Architecture within the governance requirements of law enforcement mobile systems. A separate body of literature examines digital evidence, cross-border criminal investigations, data in policing, and crime governance, but these studies generally emphasize legal accuracy, institutional accountability, and data use rather than Zero Trust Architecture as an integrated access and governance model (Casino et al., 2022; Stoykova, 2024; Afzal & Panagiotopoulos, 2025).

This gap matters because law enforcement mobile governance requires more than secure login and device management. It requires access control that is traceable, explainable, proportional, and aligned with the sensitivity of police data, citizen data, and digital evidence. For example, an officer may need immediate access to case records in the field, while the institution must ensure that access is lawful, device posture is trusted, evidence records are protected, and every action is auditable. The problem is therefore not only how to deploy Zero Trust Architecture but also how to translate its principles into a governance framework suitable for law enforcement operations.

The specific issue addressed in this research is the limited integration of Zero Trust Architecture into law enforcement mobile governance. Traditional perimeter-based security assumes that users or devices inside an institutional network can be trusted, but this assumption is no longer suitable when officers access systems through mobile devices, public networks, cloud services, and field-based applications. Zero Trust Architecture responds to this problem by applying continuous verification, least-privilege access, identity assurance, device posture assessment, and policy-based authorization.

Previous research has discussed Zero Trust Architecture in various technical domains. Rose et al. (2020) introduced Zero Trust Architecture through NIST Special Publication 800-207 as a cybersecurity model that shifts protection from network perimeters toward users, assets, and resources. Syed et al. (2022), in a Scopus-indexed study, provided a comprehensive survey of Zero Trust Architecture and emphasized continuous authentication, segmentation, and policy enforcement. Meanwhile, Phiayura and Teerakanok (2023) proposed a migration framework showing that Zero Trust implementation requires staged planning, identity consolidation, asset mapping, and organizational readiness.

Other relevant studies also show the importance of Zero Trust in mobile, IoT, edge, and distributed environments. Xiao et al. (2022) highlighted context-aware and risk-aware access control as essential for Zero Trust systems, while Azad et al. (2024) reviewed Zero Trust

security in IoT environments where devices operate across unstable and heterogeneous networks. In the law enforcement context, Casino et al. (2022) examined cross-border criminal investigations and digital evidence, while Stoykova (2024) emphasized procedural accuracy in digital evidence governance. These studies show that security architecture must be connected with legal validity, chain of custody, and institutional accountability.

Despite these contributions, a clear research gap remains. Most Zero Trust studies focus on enterprise networks, cloud computing, IoT, edge systems, and technical access models, while studies on law enforcement generally focus on digital evidence, policing data, criminal investigation, or procedural governance. Very few studies directly connect Zero Trust Architecture with mobile governance in law enforcement. As a result, there is still limited conceptual guidance on how Zero Trust principles can be translated into a governance framework for police mobile systems.

The urgency of this research lies in the growing dependence of law enforcement institutions on mobile technologies. When officers access case files, citizen data, or digital evidence through mobile devices, the risk is not only technical but also legal and ethical. Unauthorized access, weak authentication, lost devices, excessive privileges, or incomplete audit trails can compromise evidence integrity and reduce public trust. Therefore, law enforcement agencies need a security governance model that ensures every access decision is lawful, proportional, traceable, and reviewable.

The novelty of this research is its effort to connect three bodies of knowledge that are often discussed separately: Zero Trust Architecture, law enforcement data and evidence governance, and mobile government. This study does not treat Zero Trust merely as a technical cybersecurity solution but as a governance-oriented framework that can support identity assurance, device verification, adaptive access policy, evidence protection, auditability, privacy safeguards, and organizational readiness in law enforcement mobile systems.

The purpose of this research is to synthesize recent literature and formulate a governance-oriented Zero Trust Architecture framework for law enforcement mobile governance. Specifically, this research seeks to identify dominant themes in Zero Trust and mobile security studies, explain their relevance to law enforcement operations, and develop a conceptual framework that can guide public institutions in managing secure mobile access to police data and digital evidence.

The contribution of this research is both theoretical and practical. Theoretically, it expands the interpretation of Zero Trust Architecture from a cybersecurity model into a public governance instrument. Practically, it provides guidance for law enforcement agencies in designing mobile systems that are secure, accountable, and aligned with legal authority. The main benefit of this research is that it can help public institutions strengthen digital policing, protect sensitive data, maintain evidence integrity, and increase public trust in technology-based law enforcement governance.

METHOD

This study used a systematic literature review design. The review was guided by the PRISMA 2020 reporting logic because PRISMA provides a transparent structure for identifying, screening, assessing, and reporting studies in a systematic review (Page et al., 2021). This method was selected to map the development of Zero Trust Architecture and

synthesize its relevance for law enforcement mobile governance. The review did not conduct a meta-analysis because the included studies were conceptually and methodologically diverse, consisting of surveys, conceptual frameworks, access control models, security architecture papers, e-government studies, and law enforcement-related governance studies.

The primary search source was Scopus, supported by DOI and publisher metadata verification. A Web of Science syntax was also prepared as a reproducibility comparator because the topic combines cybersecurity, mobile governance, and law enforcement, and exact phrase matching is likely to produce narrow results. The recommended Scopus search string was: TITLE-ABS-KEY (("zero trust" OR "zero trust architecture" OR ZTA OR ZTNA) AND ("law enforcement" OR policing OR police OR "digital evidence" OR "criminal investigation" OR "public safety" OR "mobile governance" OR "mobile government" OR "m-government" OR smartphone OR "mobile device" OR "mobile application" OR "identity governance" OR "access control")). The filters were publication year 2020 to 2026, document type article, English language, and open access availability.

The eligibility criteria were designed to retain studies with direct or conceptual relevance to secure mobile governance in law enforcement. Articles were included when they discussed Zero Trust Architecture, access control, identity and device authentication, mobile device security, IoT or edge security, e-government or mobile government security, police data governance, digital evidence, criminal investigation, or public safety technology. Articles were excluded when they were not journal articles, not written in English, not open access, outside the selected years, duplicated by DOI or title, or unrelated to access security, mobile systems, digital governance, or law enforcement contexts.

Data extraction focused on author, year, title, journal, DOI, thematic cluster, security concept, governance relevance, and implications for law enforcement mobile governance. The 40 included articles were then synthesized through thematic coding. The coding categories were developed from recurring concepts in the literature, namely Zero Trust principles, identity and access control, device and endpoint assurance, context- and risk-aware authorization, evidence and data governance, public sector digital transformation, and organizational readiness. The synthesis was conducted narratively because the purpose of the review was to build a conceptual framework rather than estimate statistical effects.

The review process followed the four major PRISMA stages. The identification stage produced 96 candidate records. Duplicate removal eliminated 22 records. Title and abstract screening was conducted on 74 records, and 26 records were excluded because they did not sufficiently address secure access, mobile security, digital governance, or law enforcement-related contexts. The eligibility stage assessed 48 full-text articles, and 8 articles were excluded because they were not verified as open access, did not meet the article type criteria, or were conceptually too distant. The final synthesis included 40 articles.

Table 1. Search strategy and eligibility criteria

Component	Description
Review design	Systematic Literature Review guided by PRISMA 2020
Primary database	Scopus
Complementary check	Web of Science search syntax and DOI or publisher metadata verification

Component	Description
Search concepts	Zero Trust Architecture, law enforcement, digital evidence, mobile governance, mobile government, mobile devices, identity governance, and access control
Time span	2020 to 2026
Document type and language	Open access journal articles written in English
Inclusion focus	ZTA, access control, mobile security, IoT or edge security, e government, police data, digital evidence, public safety, and law enforcement governance
Exclusion focus	Duplicates, non journal outputs, non English texts, inaccessible full texts, and articles unrelated to secure access or mobile governance

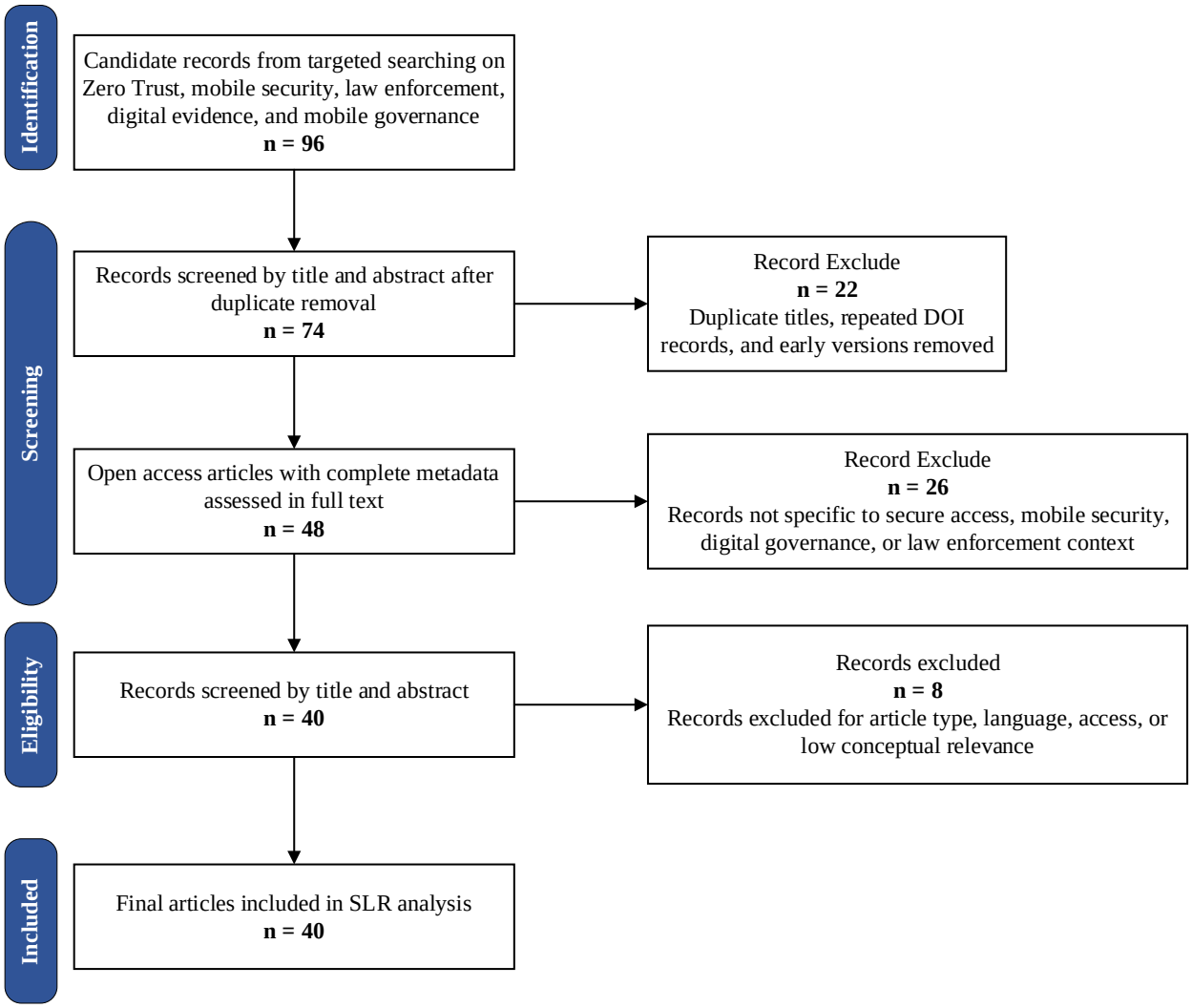

Figure 1. PRISMA 2020 flow diagram

RESULTS AND DISCUSSIONS

The final corpus consists of 40 articles grouped into four thematic clusters. The largest cluster concerns the architecture, migration, implementation, and evaluation of Zero Trust Architecture. This group includes comprehensive surveys, migration frameworks, dynamic access control models, trust score based models, and implementation studies. The second cluster concerns mobile, IoT, edge, 6G, and continuous authentication contexts. This cluster is important because law enforcement mobile governance relies on distributed endpoints, mobile

connectivity, and device level assurance. The third cluster focuses on law enforcement, digital evidence, police data, and crime governance. The fourth cluster concerns e government and mobile government, especially adoption, public value, trust, privacy, and security in digital public services.

The distribution of articles shows a clear imbalance. Zero Trust Architecture is technically mature in the cybersecurity literature, but its application to law enforcement mobile governance is still underdeveloped. The direct connection between ZTA, police operations, mobile public services, and evidence governance is limited. This confirms the novelty of this review, which synthesizes technical and governance literatures to formulate a policy relevant framework.

Table 2. Thematic distribution of included articles

Cluster	Number of articles	Main contribution	Implication for law enforcement mobile governance
ZTA architecture, migration, access control, and implementation	16	Defines principles, migration pathways, dynamic access control, trust scores, security design, and implementation priorities	Provides the technical foundation for continuous verification and least privilege access
Mobile, IoT, edge, 6G, device authentication, and distributed systems	13	Explains endpoint assurance, continuous authentication, biometric verification, edge access, and connected device security	Supports secure access from field devices, mobile applications, and distributed operational environments
Law enforcement, digital evidence, police data, and crime governance	5	Highlights procedural accuracy, cross border investigation, police data use, AI supported evidence processing, and platform based crime governance	Clarifies the legal and accountability requirements that security architecture must satisfy
E government, mobile government, public value, privacy, and trust	6	Explains citizen acceptance, public value, security perceptions, crisis management, and digital service delivery	Positions ZTA as part of secure, trustworthy, and accountable public sector transformation

Dominant Themes in Zero Trust Architecture Studies

The reviewed Zero Trust Architecture literature consistently emphasizes that access decisions should not be based on network location. Rose et al. (2020) explain that Zero Trust moves defense from static network perimeters to users, assets, and resources. This is consistent with later surveys that define Zero Trust Architecture through continuous verification, policy enforcement, segmentation, identity governance, device assessment, and telemetry (Syed et al., 2022; Kang et al., 2023). For mobile law enforcement, this means that a police officer, mobile device, application session, case database, and evidence repository must be treated as separate entities whose trust status can change over time.

Migration is a major topic in the literature. Teerakanok et al. (2021) and Phiayura and Teerakanok (2023) show that Zero Trust Architecture implementation requires staged planning rather than the immediate replacement of legacy systems. This is highly relevant to public institutions because law enforcement agencies often depend on legacy databases, fragmented systems, and inter-agency platforms. A practical transition requires asset inventory, data classification, identity consolidation, policy definition, telemetry collection, and gradual

enforcement. Without staged governance, Zero Trust implementation can become a technology procurement exercise rather than an institutional security reform.

Access control is another dominant theme. Xiao et al. (2022), Wang et al. (2025), Ma and Chiu (2025), and Jeong and Yang (2025) emphasize context, risk, dynamic authorization, and trust scores. These concepts are important for field policing because access risk varies by location, device condition, time, network, user role, task, data sensitivity, and case status. A detective accessing evidence from a secure office network should not be assessed in the same way as an officer accessing sensitive information through a mobile device on a public network. Dynamic access control therefore supports proportional security decisions rather than static allow-or-deny rules.

Studies on IoT, edge, 6G, continuous authentication, biometric verification, and distributed systems expand the relevance of Zero Trust Architecture to mobile environments (Alshomrani & Li, 2022; Ali et al., 2022; Son et al., 2024; Sasada et al., 2024; Azad et al., 2024). These studies suggest that law enforcement mobile governance should verify not only the human user but also device integrity, application behavior, cryptographic keys, network context, and session continuity. Continuous authentication is particularly important where devices are shared, stolen, lost, or used in fast-changing operational situations.

Several studies introduce blockchain, encryption, and delegation mechanisms for Zero Trust-enabled environments (Nie et al., 2025; Mukta et al., 2025; Sharma et al., 2025). These technologies may support audit trails, delegated access, and tamper-resistant evidence records, but they should be evaluated carefully in public sector contexts. Law enforcement agencies must ensure that technical immutability does not conflict with legal correction mechanisms, data retention rules, and privacy obligations. This reinforces the argument that Zero Trust implementation in law enforcement cannot be separated from public governance.

Law Enforcement Mobile Governance as a Zero Trust Use Case

The law enforcement literature included in this review identifies the sensitivity of data, evidence, and procedural accuracy. Casino et al. (2022) discuss the complexity of cross-border criminal investigations and digital evidence, where legal admissibility and data exchange depend on trust among agencies and jurisdictions. Stoykova (2024) emphasizes procedural accuracy in digital evidence governance, while Afzal and Panagiotopoulos (2025) show that data in policing involves organizational, ethical, and administrative challenges. These concerns indicate that law enforcement mobile governance requires security controls that preserve confidentiality, integrity, availability, authenticity, accountability, and fairness.

Mobile governance in policing differs from ordinary mobile government services because access may affect liberty, surveillance, investigation, and legal evidence. A mobile application used by law enforcement may process personal data, location data, biometric data, witness statements, case notes, videos, or digital evidence. These data categories require stronger access rules than general service information. Zero Trust Architecture can help by requiring identity proofing, device posture assessment, role-based and attribute-based policies, session monitoring, and complete audit logging.

However, Zero Trust Architecture alone does not automatically solve governance risks. A technically secure system can still produce unfair outcomes when policies are poorly defined, access roles are too broad, data classification is weak, audit logs are not reviewed, or oversight mechanisms are absent. The governance contribution of this review is therefore to place Zero

Trust Architecture within legal and organizational safeguards. A law enforcement ZTA model should specify who can access what data, under what legal basis, from what device, under what operational condition, for how long, and with what audit trail.

Mobile government studies also contribute to the framework because they show that digital public services depend on public value, trust, usability, crisis responsiveness, and institutional acceptance (Alhanatleh et al., 2022; Nookhao & Kiattisin, 2023; Gürler et al., 2024; Al Kautsar Maktub et al., 2025). For law enforcement, public trust is inseparable from security design. Citizens are more likely to accept digital policing systems when institutions can demonstrate that data access is controlled, misuse is traceable, and rights are protected. Zero Trust Architecture can therefore be framed as a trust-producing governance mechanism rather than merely a trust-denying security mechanism.

A Governance Oriented ZTA Framework

Based on the synthesis, this article proposes a governance oriented Zero Trust Architecture framework for law enforcement mobile governance. The framework connects technical controls with policy accountability. It consists of six interrelated dimensions: identity and role assurance, device and application posture, adaptive policy enforcement, evidence and data governance, audit and accountability, and organizational readiness.

Table 3. Governance oriented ZTA framework for law enforcement mobile governance

Dimension	Core question	Required capability	Governance outcome
Identity and role assurance	Who is requesting access and what authority do they have?	Strong identity proofing, multi factor authentication, role and attribute based access, separation of duties	Access is linked to lawful authority and specific duty
Device and application posture	Is the device and application environment trustworthy?	Device registration, endpoint health check, encryption, secure application management, lost device response	Mobile access is conditioned by verified device integrity
Adaptive policy enforcement	Should access be allowed under the current context?	Policy engine, risk scoring, least privilege, session time limits, network and location context, anomaly detection	Access decisions are proportional to risk and operational need
Evidence and data governance	What data is accessed and how sensitive is it?	Data classification, evidence chain of custody, metadata preservation, encryption, case based authorization	Digital evidence and police data remain accountable and admissible
Audit and accountability	Can every access decision be reconstructed and reviewed?	Immutable audit logs, supervisory review, misuse alerts, reporting dashboards, oversight procedures	Institutional accountability and public trust are strengthened
Organizational readiness	Can the institution operate and sustain ZTA?	Policy reform, training, legacy system mapping, procurement standards, inter agency agreements, change management	ZTA becomes an institutional governance capability

The first dimension is identity and role assurance. Law enforcement systems should not only identify a user but also verify whether the user has a legal and organizational basis to access a specific resource. This requires combining identity management with roles, case

assignment, rank, investigative authority, task status, and separation of duties. Strong authentication is necessary but insufficient without precise authorization rules.

The second dimension is device and application posture. Mobile access should depend on whether the device is registered, encrypted, updated, protected from compromise, and running authorized applications. This dimension is essential because mobile devices are operationally useful but physically vulnerable. Device loss, malware, unauthorized application installation, and insecure networks can create risks to sensitive police data.

The third dimension is adaptive policy enforcement. ZTA requires access decisions to be continuously evaluated. For example, a request to view a low sensitivity public safety bulletin may be allowed under broad conditions, while access to biometric records, witness identities, or evidence files may require higher assurance, a verified device, a secure network, case assignment, and supervisory approval. This adaptive logic enables policy granularity.

The fourth dimension is evidence and data governance. Digital evidence requires integrity, provenance, chain of custody, and procedural accuracy. Mobile systems should therefore log evidence access, protect metadata, prevent unauthorized copying, and maintain records that can be reviewed during investigation, prosecution, or oversight. The integration of ZTA with evidence governance ensures that security supports legal admissibility and procedural fairness.

The fifth dimension is audit and accountability. Zero Trust Architecture produces telemetry and logs, but these data are only meaningful when institutions review them and act on anomalies. Law enforcement agencies need procedures for supervisory review, misuse investigation, incident response, and public accountability. This converts technical monitoring into governance control.

The sixth dimension is organizational readiness. Public agencies often face budget constraints, legacy infrastructure, fragmented databases, limited cybersecurity staff, and complex procurement rules. The literature on ZTA migration suggests that successful adoption requires staged planning, maturity assessment, and change management. For law enforcement mobile governance, this includes training officers, revising data access policies, mapping legal authorities, and establishing inter agency agreements.

Policy and Implementation Agenda

The synthesis indicates that Zero Trust Architecture should be adopted through a policy led roadmap rather than through isolated technology deployment. Law enforcement agencies need to begin with data classification and authority mapping. Data assets should be classified according to sensitivity, legal basis, operational use, and evidence status. Access rules should then be aligned with case roles, operational needs, and legal mandates.

The next agenda is identity consolidation. Many public agencies operate multiple identity systems across units, applications, and partners. Zero Trust mobile governance requires unified identity governance so that user roles, case assignments, device ownership, and access history can be evaluated consistently. This agenda is particularly important for inter agency investigations and emergency operations.

Endpoint governance must also be prioritized. Mobile devices used for policing should be registered, encrypted, monitored, and subject to clear usage policies. Agencies should decide whether personally owned devices are allowed, what data can be accessed from them, and what

technical safeguards are mandatory. Without endpoint governance, ZTA policy enforcement will be incomplete.

Evidence systems require special treatment. When mobile devices are used to capture, upload, or retrieve evidence, the ZTA framework should preserve chain of custody and auditability. Every evidence access event should include user identity, device identity, time, location when legally appropriate, action taken, and case context. These controls help protect evidence integrity and support judicial review.

Finally, public oversight should be incorporated. Because law enforcement systems affect rights, security governance should include accountability mechanisms, audit review, privacy impact assessment, and complaint response. In this way, Zero Trust Architecture becomes part of democratic governance rather than only an internal cybersecurity mechanism.

Table 4. Recommended implementation roadmap

Phase	Priority action	Expected output
Phase 1	Map assets, data sensitivity, mobile applications, legal basis, and user roles	Data and authority inventory
Phase 2	Consolidate identity governance and strengthen authentication	Unified identity and role assurance
Phase 3	Register devices and enforce mobile endpoint posture	Trusted device and application environment
Phase 4	Deploy adaptive access policies for case data, operational data, and evidence repositories	Risk aware and least privilege access
Phase 5	Integrate audit logging, supervisory review, incident response, and evidence chain of custody	Accountable and reviewable law enforcement mobile governance
Phase 6	Evaluate maturity, train personnel, update policies, and coordinate inter agency agreements	Sustainable ZTA governance capability

Theoretical and Practical Implications

The theoretical implication of this review is that Zero Trust Architecture can be interpreted as a governance model, not only as a cybersecurity model. The zero trust principle of no implicit trust corresponds to public administration concerns about accountability, legality, transparency, and control of discretionary authority. In law enforcement mobile governance, every access decision becomes an administrative act that can be authorized, logged, justified, and reviewed.

The practical implication is that law enforcement agencies should not deploy mobile applications without a parallel access governance model. Mobile services can improve operational responsiveness, but they also expand the attack surface and increase the risk of misuse. A governance oriented ZTA framework can help agencies create secure access rules, protect evidence, manage distributed devices, and demonstrate accountability to oversight bodies and the public.

The review also indicates that future empirical research is needed. Most available studies are conceptual, technical, or domain specific. There is limited empirical evidence on how police agencies adopt Zero Trust Architecture, how officers experience adaptive access policies, how ZTA affects investigative efficiency, and how citizens perceive ZTA enabled digital policing.

Future studies should use case studies, design science, policy evaluation, and comparative institutional analysis to test the framework proposed in this article.

CONCLUSION

This article reviewed recent literature on Zero Trust Architecture and synthesized its relevance for law enforcement mobile governance. The systematic review identified 40 articles from an initial set of 96 records. The findings show that Zero Trust Architecture has developed strongly in cybersecurity, cloud, IoT, edge, 6G, authentication, and access control studies. However, direct discussion of Zero Trust Architecture in law enforcement mobile governance remains limited. This gap creates an opportunity to connect technical security architecture with public policy, digital evidence governance, and accountable policing.

The main finding is that Zero Trust Architecture should be understood as both a security architecture and a governance instrument. In law enforcement mobile systems, continuous verification, least-privilege access, device posture assessment, adaptive risk-based policy enforcement, and audit logging can support secure access to sensitive police data and digital evidence. However, these technical controls must be embedded within legal authority, organizational policy, the evidence chain of custody, privacy safeguards, and supervisory accountability.

The article contributes a governance-oriented ZTA framework with six dimensions: identity and role assurance, device and application posture, adaptive policy enforcement, evidence and data governance, audit and accountability, and organizational readiness. This framework can help law enforcement agencies plan secure mobile systems that are operationally useful, legally accountable, and aligned with public trust. The limitation of this review is that it relies on systematic literature synthesis rather than field implementation data. Future research should validate the framework through institutional case studies, implementation evaluations, and comparative analyses of law enforcement mobile governance practices.

REFERENCE

Afzal, M., & Panagiotopoulos, P. (2025). Data in policing: An integrative review. International Journal of Public Administration, 48(7), 411–430. https://doi.org/10.1080/01900692.2024.2360586

Al-Ansi, A. M., Garad, A., Jaboob, M., & Al-Ansi, A. (2024). Elevating e-government: Unleashing the power of AI and IoT for enhanced public services. Heliyon, 10(23), e40591. https://doi.org/10.1016/j.heliyon.2024.e40591

Al-Kautsar Maktub, M., Handayani, P. W., & Sunarso, F. P. (2025). Citizen acceptance and use of the Jakarta Kini (JAKI) e-government: Extended unified model for electronic government adoption. Heliyon, 11(2), e42078. https://doi.org/10.1016/j.heliyon.2025.e42078

Alhanatleh, H., Khaddam, A., & Abousweilem, F. (2022). Mobile government public value model for assessing the public institution's services: Evidence through the context of Jordan. International Journal of Data and Network Science, 6(4), 1295–1308. https://doi.org/10.5267/j.ijdns.2022.6.005

Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A maturity framework for Zero Trust security in multiaccess edge computing. Security and Communication Networks, 2022, Article 3178760. https://doi.org/10.1155/2022/3178760

Alshomrani, S., & Li, S. (2022). PUFDCA: A Zero-Trust-based IoT device continuous authentication protocol. Wireless Communications and Mobile Computing, 2022, Article 6367579. https://doi.org/10.1155/2022/6367579

Ameer, S., Praharaj, L., Sandhu, R., Bhatt, S., & Gupta, M. (2024). ZTA-IoT: A novel architecture for Zero-Trust in IoT systems and an ensuing usage control model. ACM Transactions on Privacy and Security, 27(3), Article 22. https://doi.org/10.1145/3671147

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of Zero Trust security in the age of IoT. Internet of Things, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227

Casino, F., Dasaklis, T. K., Spathoulas, G., Anagnostopoulos, M., Ghosal, A., Borocz, I., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity, 8(1), tyac014. https://doi.org/10.1093/cybsec/tyac014

Castilla, R., Pacheco, A., & Franco, J. (2023). Digital government: Mobile applications and their impact on access to public information. *SoftwareX*, *22*, 101382.

Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J. J. M., & Dwivedi, Y. K. (2025). Trust, risk, privacy and security in e-government use: Insights from a MASEM analysis. Information Systems Frontiers, 27, 1089–1105. https://doi.org/10.1007/s10796-024-10497-8

Gürler, S., Cavusoglu, B., Ozdamli, F., Mousa, K. M., & Baykan, H. (2024). Mobile government use and crisis management: The moderating role of techno-skepticism. Sustainability, 16(12), 4904. https://doi.org/10.3390/su16124904

Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust Architecture: Design, sensitivity analysis, and real-world performance evaluation. Applied Sciences, 15(17), 9551. https://doi.org/10.3390/app15179551

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of Zero Trust security: A brief survey. Entropy, 25(12), 1595. https://doi.org/10.3390/e25121595

Ma, Y. W., & Chiu, P. H. (2025). A novel risk-based access control engine in Zero Trust Architecture for IoT network. International Journal of Information Security, 24, Article 124. https://doi.org/10.1007/s10207-025-01030-2

Mukta, R., Pal, S., Chowdhury, K., Hitchens, M., Paik, H. Y., & Kanhere, S. S. (2025). Zero Trust-driven access control delegation using blockchain. Blockchain: Research and Applications, Article 100319. https://doi.org/10.1016/j.bcra.2025.100319

Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. Sensors, 25(2), 550. https://doi.org/10.3390/s25020550

Nookhao, S., & Kiattisin, S. (2023). Achieving a successful e-government: Determinants of behavioral intention from Thai citizens' perspective. Heliyon, 9(8), e18944. https://doi.org/10.1016/j.heliyon.2023.e18944

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, Article n71. https://doi.org/10.1136/bmj.n71

Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to Zero Trust Architecture. IEEE Access, 11, 19487–19511. https://doi.org/10.1109/ACCESS.2023.3248622

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sasada, T., Taenaka, Y., Kadobayashi, Y., & Fall, D. (2024). Web-biometrics for user authenticity verification in Zero Trust access control. IEEE Access, 12, 129611–129622. https://doi.org/10.1109/ACCESS.2024.3413696

Sharma, A., Rani, S., & Boulila, W. (2025). Blockchain-based Zero Trust networks with federated transfer learning for IoT security in Industry 5.0. PLOS ONE, 20(6), e0323241. https://doi.org/10.1371/journal.pone.0323241

Son, S., Kwon, D., Lee, S., Kwon, H., & Park, Y. (2024). A Zero-Trust authentication scheme with access control for 6G-enabled IoT environments. IEEE Access, 12, 154066–154079. https://doi.org/10.1109/ACCESS.2024.3484522

Stoykova, R. A. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. Computer Law & Security Review, 55, 106040. https://doi.org/10.1016/j.clsr.2024.106040

Stoykova, R., Porter, K., & Beka, T. (2024). The AI Act in a law enforcement context: The case of automatic speech recognition for transcribing investigative interviews. Forensic Science International: Synergy, 9, 100563. https://doi.org/10.1016/j.fsisyn.2024.100563

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access, 10, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and challenges. Security and Communication Networks, 2021, Article 9947347. https://doi.org/10.1155/2021/9947347

Wang, J., Wang, Z., Song, J., & Cheng, H. (2023). Attribute and user trust score-based Zero Trust access control model in IoV. Electronics, 12(23), 4825. https://doi.org/10.3390/electronics12234825

Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-Trust based dynamic access control for cloud computing. Cybersecurity, 8, Article 12. https://doi.org/10.1186/s42400-024-00320-x

Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and risk aware access control for Zero Trust systems. Security and Communication Networks, 2022, Article 7026779. https://doi.org/10.1155/2022/7026779

Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible Zero Trust Architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks, 156, 103414. https://doi.org/10.1016/j.adhoc.2024.103414