International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

A SECURE ARCHITECTURE FOR MANAGING CONFIDENTIAL DOCUMENTS IN MILITARY ELECTRONIC DATABASES

https://doi.org/10.5281/zenodo.23006110

Giyosjon Jumaev Abdivaxobovich[1],
Turapov Sherzod Nurmatovich[2]
[1]Artificial intellegance and digital technologies, Tashkent International University of Financial Management and Technologies,
[2]Head of Department of Act and Military Communication Institute
Tashkent, Uzbekistan
[1]giyosjonjumaev@gmail.com

Abstract

This article proposes a layered secure architecture for managing confidential documents stored in the electronic databases of military organizations. Modern military information systems demand a high level of confidentiality, integrity, and availability, yet traditional perimeter-based defenses are no longer sufficient against insider threats and sophisticated cyberattacks. The proposed architecture combines Zero Trust principles, the Bell-LaPadula multi-level security model, role- and attribute-based access control (RBAC/ABAC), and modern cryptographic safeguards (AES-256, TLS 1.3, PKI/HSM) into a single, coherent design. Real statistical data collected from the U.S. Department of Defense's Zero Trust strategy, NIST SP 800-53, and IBM's 2025 Cost of a Data Breach Report were analyzed to ground the design in current threat and cost evidence. The results show that a layered approach substantially strengthens protection not only against external attacks but also against insider threats. The article concludes with practical recommendations for implementing the proposed architecture and outlines directions for future research.

Keywords

military information security, Zero Trust architecture, Bell-LaPadula model, multi-level security, access control, database encryption, confidential documents.

1. INTRODUCTION

Digital transformation has not bypassed the military domain — from command-and-control systems to personnel and service records, large volumes of confidential documents are now stored and processed in electronic databases.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

While such centralized digital storage improves convenience and operational efficiency, it simultaneously expands the attack surface and increases the risk that confidential information will be leaked or altered without authorization.

International experience confirms that this risk is real. According to IBM's 2025 annual Cost of a Data Breach Report, the average global cost of a single incident is USD 4.44 million, rising to USD 10.22 million in the United States. Data breach costs in the public sector rose by 10.8 percent (roughly USD 310,000) in 2025, reaching an average of about USD 2.86 million (Figure 1) — evidence that government and military structures are becoming increasingly vulnerable to cyber threats. Another important indicator is that breaches caused by malicious insiders are the most expensive threat category, averaging USD 4.92 million — demonstrating that securing the external perimeter alone is not enough.

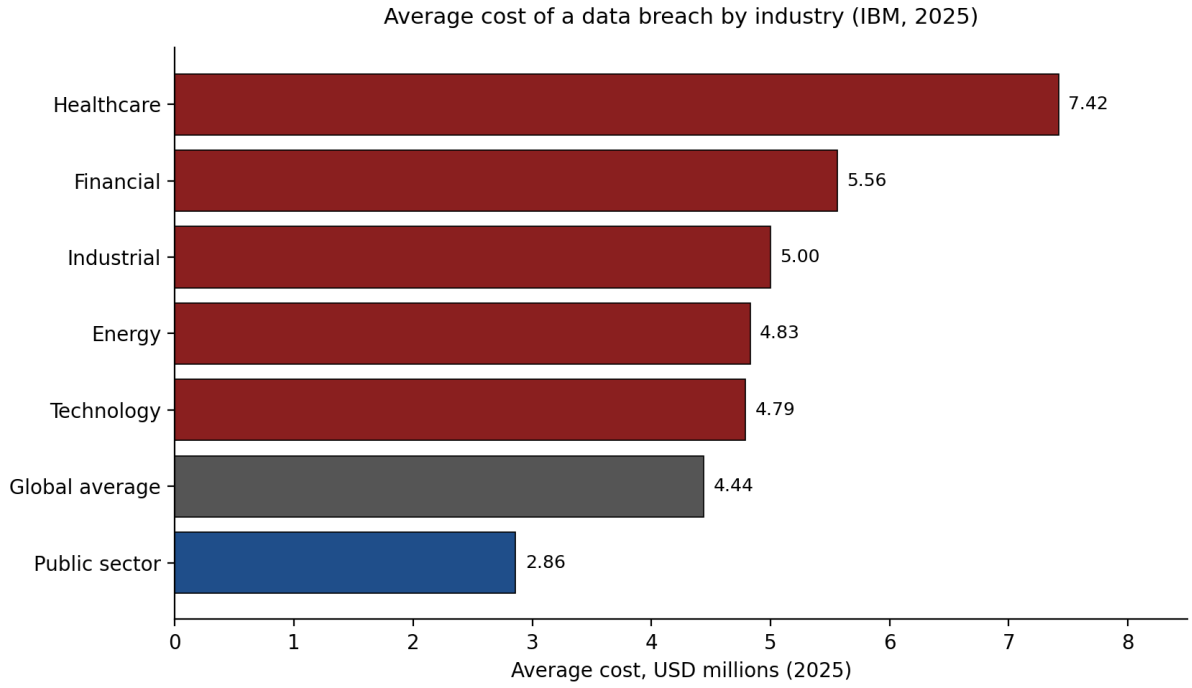

Figure 1. Average cost of a data breach by industry, in USD millions (compiled by the author from IBM Cost of a Data Breach Report, 2025).

In response to these threats, the U.S. Department of Defense (DoD) is implementing a Zero Trust strategy, adopted in 2022 and subsequently refined. The strategy rests on five core tenets: assume a hostile environment, presume breach, never trust and always verify, scrutinize explicitly, and apply unified analytics. In practice, the strategy is organized around seven pillars: user, device, application and workload, data, network and environment, automation and orchestration, and visibility and analytics. This approach is being rolled out across the entire U.S. federal government in accordance with Executive Order 14028.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

At the same time, a distinctive feature of military databases — the division of documents into different classification levels (unclassified, for official use only, secret, top secret) — requires a mechanism that complements the standard Zero Trust approach, namely a multi-level security (MLS) model. Developed in 1973 for the U.S. Air Force, the Bell-LaPadula model continues to serve as the theoretical foundation for restricting access by classification level in government and military systems today.

The purpose of this article is to combine the three directions noted above — Zero Trust architecture, the multi-level security model, and modern cryptographic tools — into a single, practically implementable architecture, and to justify it in the context of military electronic databases. The article is structured as follows: Section 2 describes the research methodology and the architecture design approach; Section 3 presents the proposed architecture, its layers, and comparison tables; Section 4 discusses the results; and Section 5 presents conclusions and directions for future research.

2. METHODS

The research follows a design-science methodology: security requirements for the military document lifecycle were first identified, relevant normative and scholarly sources were then analyzed, an architecture satisfying these requirements was designed, and finally the proposed solution was evaluated through comparison with existing standards.

2.1. Identifying security requirements

The following core requirements were established for a military document management system: (1) confidentiality — only individuals with appropriate authorization and a genuine need-to-know may access information; (2) integrity — preventing unauthorized modification of documents; (3) availability — ensuring uninterrupted system operation during operational situations; (4) accountability — ensuring every access and action is logged and non-repudiable.

2.2. Reference frameworks and theoretical foundations

Three reference sources anchored the architecture design: first, the Access Control (AC) family of recommendations in NIST Special Publication 800-53; second, the five tenets and seven pillars set out in the DoD Zero Trust Reference Architecture (version 2.0) and the DoD Zero Trust Overlays (2024); and third, the mandatory access control (MAC) model proposed by Bell and LaPadula, in particular its two core rules — the simple security property (a subject may read only an object at or below its own level — no read up) and the star property (a subject may write only to an object at or above its own level — no write down).

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

2.3. Design approach: defense-in-depth

The architecture was designed as six independent yet interconnected layers: an authentication layer, a Zero Trust policy engine, an access control layer (RBAC/ABAC combined with Bell-LaPadula MLS), a cryptographic protection layer, a database segmented by classification level, and an audit/monitoring layer. Each layer has its own independent control mechanism, so that a failure in one layer does not by itself compromise the system as a whole.

2.4. Evaluation method

The proposed solution was evaluated through comparative analysis: access control models (RBAC, ABAC, MAC/MLS) were compared on granularity, flexibility, administrative overhead, and compliance with the need-to-know principle; encryption algorithms were compared on security level, performance, and practical applicability. In addition, the layers of the proposed architecture were mapped onto the DoD Zero Trust seven pillars, allowing the architecture's alignment with the official strategy to be demonstrated.

3. RESULTS

The research produced the six-layer secure architecture shown in Figure 2.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

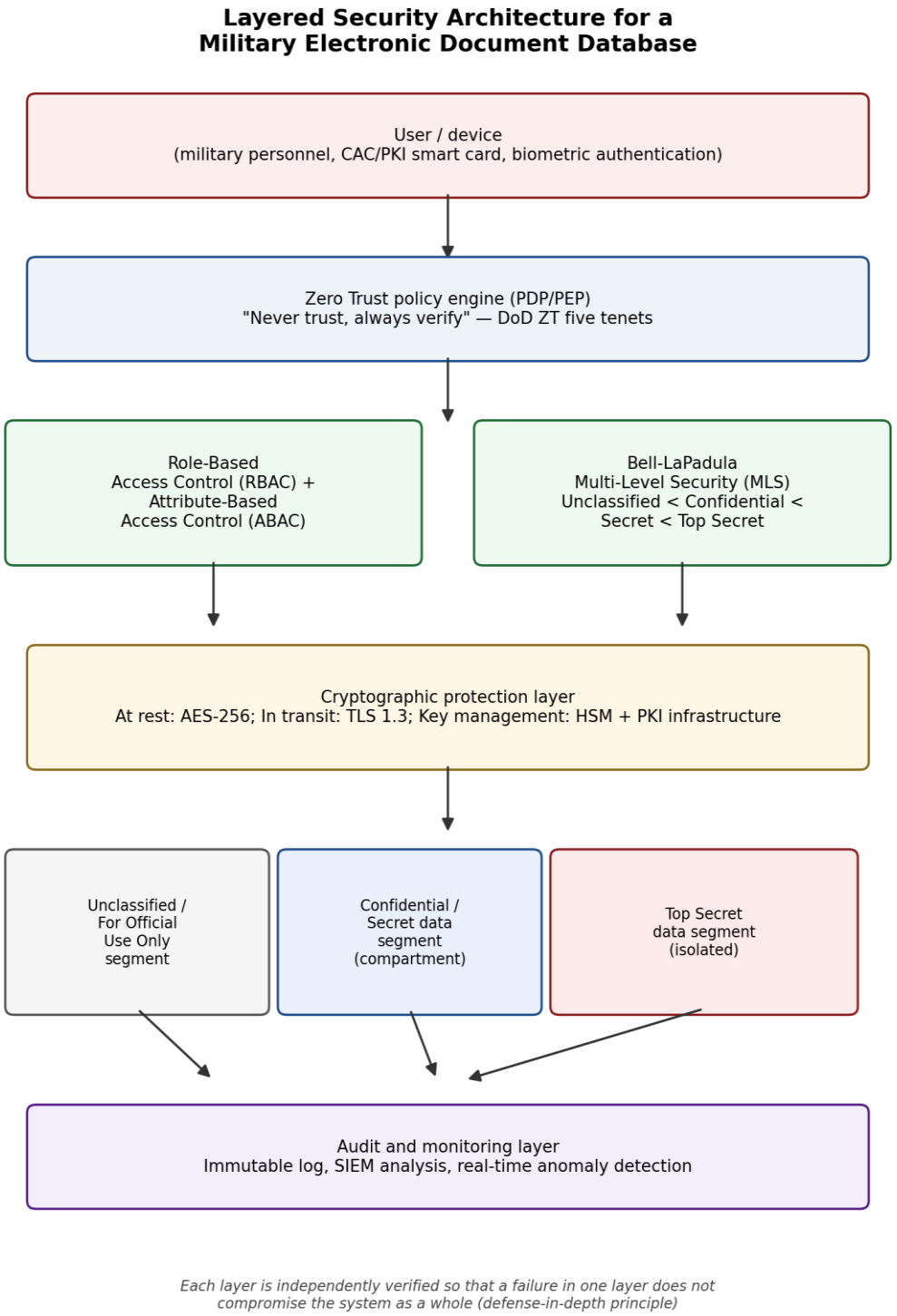

Figure 2. Proposed multi-layer security architecture for a military electronic document database (developed by the author).

The architecture operates as follows: a user first verifies their identity via a PKI-based smart card (such as a CAC-type card) and biometric authentication; every subsequent request is then routed through the Zero Trust policy engine

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

(Policy Decision Point / Policy Enforcement Point), which dynamically evaluates the user, device, and context (location, time, risk level); at the access control layer, role-based (RBAC) and attribute-based (ABAC) rules are applied together with the Bell-LaPadula MLS model — RBAC/ABAC answers the question of "what can this user do," while MLS answers "what classification level of data can this user see"; approved requests then pass through the cryptographic layer (AES-256 at rest, TLS 1.3 in transit, hardware security module (HSM) for key management); the database itself is segmented into compartments by classification level; and finally, every action is written to an immutable audit log and analyzed in real time by a SIEM system.

3.1. Comparative analysis of access control models

Criterion	RBAC	ABAC	MAC / Bell-LaPadula (MLS)
Core principle	Based on user role	Based on user, resource, and environment attributes	Based on classification level and compartment
Granularity	Medium	High	High (by classification)
Compliance with need-to-know	Partial	Good	Full (via compartments)
Administrative overhead	Low-medium (grows more complex as roles increase)	High (policies must be written and tested)	Medium (classification scheme is stable)
Dynamic adaptability	Low	High (adapts to context in real time)	Low (static levels)
Typical use in military systems	General permissions at position/unit level	Integration with the Zero Trust policy engine	High-level classification of confidential documents

Table 1. Comparative analysis of access control models.

3.2. Comparative analysis of cryptographic tools

Tool / algorithm	Application area	Security level	Note
AES-256	Encryption of data at rest	High (symmetric, 256-bit key)	Approved by NIST; recommended for government confidential documents

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

TLS 1.3	Protection of data in transit	High	Faster than earlier versions with a handshake protocol free of known vulnerabilities
RSA-4096 / ECC (P-384)	Key exchange and digital signatures	High	Used for certificate validation within the PKI infrastructure
HSM (hardware security module)	Storage and management of cryptographic keys	Very high	Ensures keys remain isolated from the software environment

Table 2. Cryptographic tools used in the proposed architecture.

3.3. Mapping the architecture to the DoD Zero Trust seven pillars

DoD ZT pillar	Architecture layer	Function provided
User	Authentication layer	PKI smart card and biometric verification
Device	Zero Trust policy engine	Continuous verification of device posture
Application and workload	Access control layer	Application-level permissions via RBAC/ABAC
Data	MLS + cryptographic layer	Protection through classification and encryption
Network and environment	Segmented database	Microsegmentation, isolated compartments
Automation and orchestration	Policy engine + audit layer	Automated enforcement of policies
Visibility and analytics	Audit and monitoring layer	SIEM, immutable log, anomaly detection

Table 3. Mapping of the proposed architecture's layers to the DoD Zero Trust seven pillars.

4. DISCUSSION

The results indicate that relying on a single model — for example, RBAC alone or perimeter security alone — is not sufficient for military databases. As Table 1 shows, while the Bell-LaPadula model fully satisfies the need-to-know principle, it is static in nature and does not account for dynamic context (for instance, the need

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

to grant temporary access during an emergency). For this reason, combining it with ABAC and a Zero Trust policy engine is recommended — this combination reconciles the rigidity of static classification with dynamic flexibility.

From an economic standpoint, the data in Figure 1 justifies investment in such an architecture: the average loss in the public sector (USD 2.86 million) and, in particular, the high cost of insider threats (USD 4.92 million) justify the expense of multiple, redundant control mechanisms. IBM's report also notes that organizations making extensive use of AI and automation save an average of USD 1.9 million per incident — further reinforcing the importance of the SIEM-based automated anomaly detection layer in the proposed architecture.

The proposed solution also has limitations. First, the architecture was developed at a conceptual level; testing it on a real military network fell outside the scope of this study due to confidentiality constraints. Second, the complexity of ABAC policies can increase the risk of administrative errors, so additional tools for automated policy verification and testing are required. Third, multiple layers of encryption and verification can affect system latency, which calls for additional engineering solutions for operational systems running in real time.

Two directions merit particular attention for future research: first, planning a transition to post-quantum cryptographic algorithms (such as the key encapsulation mechanisms currently being standardized by NIST) in light of advances in quantum computing; second, given the growing threat of "shadow AI" (the use of unmonitored AI tools) noted in IBM's 2025 report, integrating AI-tool access to the database into Zero Trust policies as well.

5. CONCLUSION

This article proposed a six-layer secure architecture for managing confidential documents in military electronic databases. The architecture unifies Zero Trust principles, the Bell-LaPadula multi-level security model, RBAC/ABAC access control, and modern cryptographic tools into a single system. The comparative analysis shows that no single model (RBAC, ABAC, or MLS) alone can satisfy every requirement, but their combined application simultaneously ensures compliance with the need-to-know principle, dynamic adaptability, and a high level of accountability. Real statistical data (IBM, 2025) confirm that the cost of data breaches in government and military structures is rising, which makes the proposed layered approach practically relevant. Military and government organizations are advised to implement this architecture in stages, beginning with the highest-classification data segment.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-14| Issue-9| 2026 Published: |22-09-2026|

REFERENCES:

1. U.S. Department of Defense, Office of the CIO. DoD Zero Trust Strategy. Version 1.1, April 2024.

2. U.S. Department of Defense, Office of the CIO. Department of Defense Zero Trust Overlays. Version 1.1, June 2024.

3. U.S. General Services Administration. Zero Trust Strategy Buyer's Guide: Department of Defense (DoD) Zero Trust Strategy. Version 1.4, May 2025.

4. IBM Security. Cost of a Data Breach Report 2025. IBM Corporation, 2025.

5. Bell, D. E., LaPadula, L. J. Secure Computer Systems: Mathematical Foundations. MITRE Corporation Technical Report, 1973.

6. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5.

7. The White House. Executive Order 14028 — Improving the Nation's Cybersecurity. May 2021.