Jurnal Kecerdasan Buatan dan Teknologi Informasi
Vol. 5, No. 2, May 2026, pp. 226-234
e-ISSN: 2964-2922, p-ISSN: 2963-6191
DOI : https://doi.org/10.69916/jkbti.v5i2.455

LITERATURE ANALYSIS ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN STRENGTHENING CYBERSECURITY IN E-GOVERNMENT SERVICES

Erfan Wahyudi[*1], Wiredarme[2]

[1,2]Institut Pemerintahan Dalam Negeri, Indonesia
Email: [1]erfan.wahyudie@gmail.com, [2]wiredarme@ipdn.ac.id

(Received: April 27, 2026; Revised: May 10, 2026; Published: May 10, 2026)

Abstract

The rapid expansion of e-government services has increased the importance of cybersecurity in protecting public digital infrastructure, citizen data, and the continuity of government operations. In this context, Artificial Intelligence (AI) has emerged as a promising approach to strengthening cyber defense through real-time monitoring, anomaly detection, intelligent classification, and adaptive threat response. This study examines the role of AI in strengthening cybersecurity in e-government services through a Systematic Literature Review (SLR) of 27 selected articles published between 2019 and 2025. The review synthesizes the literature at the intersection of AI, cybersecurity, and digital government to identify major research trends, dominant methodological approaches, thematic classifications, and key implementation challenges. The findings show that AI is increasingly positioned not only as a tool for improving administrative efficiency, but also as a strategic enabler of cyber resilience in public-sector digital ecosystems. The literature highlights that machine learning, deep learning, explainable AI, anomaly detection, and privacy-preserving learning models have substantial potential for improving the security of citizen portals, digital identity systems, inter-agency platforms, and smart-government infrastructures. However, implementation remains constrained by fragmented data environments, interoperability problems, institutional readiness gaps, limited explainability, privacy concerns, and the dual-use nature of AI in cyber defense and cyber offense. This study concludes that AI is most effective when integrated into a broader socio-technical framework encompassing governance, accountability, transparency, and organizational capacity.

Keywords: artificial intelligence; cybersecurity; digital government; e-government services; explainable ai.

1. INTRODUCTION

The digital transformation of government has progressed far beyond the digitization of isolated administrative routines toward integrated, data-intensive, and citizen-facing service ecosystems. In the literature on digital government, this evolution is described as a movement from simple transformation toward broader contextualization, where digital infrastructures reshape how governments organize processes, interact with citizens, and deliver public value [1]. In the same vein, digital transformation in the public sector is increasingly understood not merely as technology adoption, but as a structural reconfiguration of organizational processes, institutional logics, and service delivery models [2]. Within this context, e-government services now occupy a strategic position in contemporary governance, making cybersecurity a foundational requirement for continuity, legitimacy, and administrative resilience rather than a purely technical back-office concern.

The importance of cybersecurity in e-government is closely tied to citizen trust. The long-standing e-government literature has consistently shown that trust, perceived risk, and confidence in digital infrastructures strongly influence citizens' willingness to use government online services [3], [4]. More recent meta-analytic evidence reinforces this position by demonstrating that trust in government, trust in the internet, perceived risk, and privacy-security perceptions significantly shape trust in e-government and, ultimately, citizens' intention to use digital public services [5]. This means that cybersecurity in e-government is not only a matter of system protection; it is also a determinant of service adoption, institutional credibility, and public confidence in digital governance.

At the same time, artificial intelligence (AI) has emerged as one of the most consequential technological developments in public administration. Prior studies argue that AI can improve governmental decision support, automate complex administrative tasks, enhance service responsiveness, and enable predictive capabilities across public management functions [6], [7]. Systematic reviews of AI in public governance further show that the field has expanded rapidly, but also remains marked by concerns related to transparency, accountability, privacy, fairness, and human oversight [8], [9]. In public service settings specifically, AI does not simply introduce new tools; it also reshapes bureaucratic discretion and the relationship between administrative rules, professional judgment, and automated recommendations [10]. These developments are highly relevant for cybersecurity because digital public

services increasingly require adaptive, data-driven defenses capable of functioning at scale across diverse service environments.

The cybersecurity challenge becomes even more complex as government services become interconnected across agencies, platforms, databases, and smart-government infrastructures. Research on smart government emphasizes that interconnection and interoperability are now central to modern public service architecture [11]. Yet this interdependence also expands the attack surface, making critical information infrastructures, identity systems, inter-agency data exchange, and citizen-facing portals more vulnerable to phishing, ransomware, intrusion, data leakage, and service disruption [12], [13]. Recent work on e-government cybersecurity further stresses that many governmental cybersecurity arrangements remain fragmented, reactive, and insufficiently integrated across governance, risk management, and secure data exchange dimensions [13]. Thus, the intensification of digital government has simultaneously increased the strategic importance and operational difficulty of cybersecurity governance.

In this setting, AI is increasingly positioned as a promising means of strengthening cybersecurity in e-government environments. The broader cybersecurity literature shows that AI and machine learning can improve anomaly detection, automate threat intelligence, enhance intrusion detection, support phishing and malware classification, and accelerate cyber incident response [14], [15]. More recent reviews also indicate that AI-based cybersecurity systems can outperform static or purely rule-based approaches in handling dynamic, high-volume, and previously unseen attack patterns, especially when supported by predictive analytics and continuous learning [16], [18]. Furthermore, explainable AI has become increasingly important in cybersecurity because high-performing models alone are insufficient in contexts where organizations must justify, audit, and govern security decisions [17]. For the public sector, these capabilities are especially attractive because governmental systems must protect large volumes of sensitive personal and institutional data while maintaining continuity, legality, and accountability.

However, the adoption of AI for cybersecurity in e-government is not unproblematic. The same technologies that strengthen cyber defense can also intensify cyber offense. Studies on generative AI and AI weaponization show that AI can be used to automate phishing, assist malware development, enhance reconnaissance, and increase the speed and scale of cyberattacks [19], [20]. In addition, AI-based security systems face well-known challenges related to data quality, adversarial manipulation, false positives, explainability, privacy protection, governance, and institutional readiness [15]–[18]. These issues are particularly consequential in e-government, where cybersecurity decisions intersect with legal accountability, public trust, civil rights, administrative due process, and the obligation to protect citizens' data under heightened standards of transparency and fairness.

Despite the growing relevance of this issue, the current scholarship remains fragmented. Reviews on AI in public administration mainly emphasize adoption, governance, ethics, and decision-making in government [7]–[10], while reviews on AI in cybersecurity largely focus on generic technical domains, enterprise systems, or the broader cyber-defense ecosystem [14]–[20]. Meanwhile, recent studies on e-government cybersecurity tend to discuss holistic governance frameworks, interoperability, or critical infrastructure protection without centering a focused synthesis of how AI specifically contributes to cybersecurity strengthening across e-government services [12], [13]. This fragmentation indicates a clear research gap: there is still limited integrative understanding of how AI functions as a cybersecurity enabler within the institutional, technical, and governance realities of e-government.

Accordingly, this study aims to conduct a systematic literature-based analysis of the role of artificial intelligence in strengthening cybersecurity in e-government services. The study focuses on three main questions: **(1)** What are the dominant trends and research directions concerning AI for cybersecurity in e-government services? **(2)** What AI models, methods, and application domains are most frequently reported in the literature? **(3)** What technical, organizational, ethical, and governance challenges shape the implementation of AI-driven cybersecurity in e-government environments? The novelty of this article lies in its specific integrative focus on the intersection of AI, cybersecurity, and e-government services**,** bringing together public administration scholarship, digital government literature, and cybersecurity research into a single analytical framework. By doing so, the article is expected to contribute both conceptually and practically to the design of more adaptive, accountable, and resilient digital public service ecosystems.

2. RESEARCH METHODS

2.1. Research Design

This study employs a Systematic Literature Review (SLR) design to identify, evaluate, and synthesize scholarly evidence on the role of Artificial Intelligence (AI) in strengthening cybersecurity in e-government services. The SLR approach was selected because it provides a transparent, replicable, and methodologically rigorous procedure for consolidating fragmented knowledge, identifying research trends, and revealing conceptual as well as empirical gaps across an emerging interdisciplinary field [21]–[25]. In this study, the review is positioned at the intersection of three streams of scholarship, namely AI, cybersecurity, and digital government, with the aim of producing an integrated analytical understanding of how AI-based techniques are being used to protect public digital infrastructures, platforms, and services.

The review protocol was organized according to the staged logic commonly recommended for standalone literature reviews: planning the review, identifying relevant records, screening and assessing eligibility, extracting and categorizing evidence, and synthesizing the findings into higher-order analytical themes [21]–[25]. To improve reporting clarity and reproducibility, the review also follows the reporting principles of **PRISMA 2020**, particularly in documenting the search process, screening decisions, inclusion procedures, and final study selection [25].

2.2. Literature Search Strategy

The literature search was conducted using major scholarly databases that are highly relevant to information systems, computer science, cybersecurity, and public administration research. The core databases selected for this review were Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and Google Scholar. These sources were chosen to ensure broad coverage of peer-reviewed journal articles and conference proceedings discussing AI models, cyber defense mechanisms, and digital government applications. The publication window was limited to 2019–2025 in order to capture the most recent phase of AI adoption in cybersecurity and public digital services, including the acceleration of machine learning, deep learning, explainable AI, and generative AI in cyber defense contexts [22]–[25]. The search strings were developed through an iterative process and adapted to the syntax of each database. The main Boolean formulation used in this review was as follows:

("artificial intelligence" OR "machine learning" OR "deep learning" OR "neural network" OR "natural language processing" OR "explainable AI" OR XAI) AND ("cybersecurity" OR "cyber security" OR "information security" OR "network security" OR "intrusion detection" OR "malware detection" OR phishing OR ransomware OR "threat detection") AND ("e-government" OR egovernment OR "digital government" OR "electronic government" OR "smart government" OR "public sector" OR "government services")

To increase retrieval sensitivity, supplementary searches were also conducted using narrower combinations such as AI + e-government + cybersecurity, machine learning + public sector cyber defense, and AI-driven threat detection in government services. In addition, backward and forward snowballing were applied to the reference lists of highly relevant papers in order to identify additional studies that might not have been captured in the primary database search [22], [23], [25].

2.3. Inclusion and Exclusion Criteria

The inclusion criteria were defined to ensure conceptual relevance and methodological consistency. Studies were included if they met the following conditions: (1) published in English; (2) appeared in peer-reviewed journals or indexed conference proceedings; (3) explicitly discussed AI-related techniques such as machine learning, deep learning, NLP, explainable AI, or intelligent automation; (4) addressed cybersecurity issues such as intrusion detection, malware analysis, phishing detection, ransomware mitigation, threat intelligence, anomaly detection, or security monitoring; and (5) situated the analysis within e-government, digital government, smart government, public sector platforms, or government digital services. These criteria are consistent with established SLR guidance, which emphasizes the need to align eligibility rules directly with the review question and the intended analytical scope [22]–[25]. Studies were excluded if they were editorials, book reviews, news items, theses, white papers, or other non-peer-reviewed outputs; if they focused exclusively on private-sector cybersecurity without meaningful relevance to public digital services; if they addressed AI in government administration without a cybersecurity dimension; or if full-text access was unavailable. Papers that mentioned AI, cybersecurity, or e-government only tangentially, without substantive analytical discussion, were also excluded. The purpose of these exclusion rules was to maintain topical precision and reduce conceptual dilution during synthesis [22], [23], [25].

2.4. Study Selection Procedure

The study selection process was carried out systematically to ensure that only relevant and methodologically appropriate studies were included in the final review corpus. The initial search across the selected databases yielded 198 records. After the removal of 41 duplicate records, a total of 157 articles remained for title and abstract screening. At this stage, 92 records were excluded because they were not sufficiently relevant to the focus of the study, including articles that discussed cybersecurity without reference to government services, studies on AI in public administration without a cybersecurity dimension, and publications that addressed digital government only marginally. The remaining 65 articles were then subjected to full-text eligibility assessment. During this stage, 38 articles were excluded for one or more reasons, namely: lack of explicit focus on e-government or public-sector digital services, insufficient discussion of Artificial Intelligence as a substantive analytical or technical component, limited relevance to cybersecurity strengthening, and incomplete or inaccessible full-text content. As a result, 27 articles met all inclusion criteria and were retained as the final corpus for the systematic literature review.

To enhance the transparency and reproducibility of the review, the selection procedure followed a PRISMA-oriented logic consisting of four sequential stages: identification, deduplication, screening, and eligibility assessment. This stepwise procedure ensured that the final set of included studies was conceptually aligned with the objective of the research, namely to analyze the role of Artificial Intelligence in strengthening cybersecurity in e-government services. The final 27 selected studies therefore constituted the analytical basis for the thematic synthesis presented in the Results and Discussion section [22], [23], [25].

2.5. Data Extraction and Quality Appraisal

After the final set of eligible studies was established, the data were extracted into a structured data extraction matrix. The matrix included the following variables: author(s), year of publication, country or region of study, publication type, research objective, e-government domain, type of cybersecurity problem addressed, AI technique applied, dataset or data environment, evaluation metrics, principal findings, reported implementation challenges, and governance or ethical considerations. This structured extraction process was designed to support systematic comparison across studies and to facilitate thematic coding during the synthesis stage [22], [23]. Because the selected literature was expected to include diverse methodological designs, the methodological quality of the included studies was appraised using the Mixed Methods Appraisal Tool (MMAT) version 2018. The MMAT is suitable for reviews that combine qualitative, quantitative, and mixed-methods evidence, and it provides a flexible framework for assessing methodological coherence across heterogeneous studies [28]. In the present review, quality appraisal was used not to mechanically eliminate studies, but to support a more cautious interpretation of evidence, especially where claims were based on limited data, weak validation procedures, or unclear methodological reporting.

2.6. Data Analysis

The extracted studies were analyzed using thematic content analysis, informed by the principles of thematic analysis proposed by Braun and Clarke and the logic of thematic synthesis developed for systematic reviews [26], [27]. The analysis proceeded in three stages. First, the relevant findings of each study were coded line by line or idea by idea, with attention to recurring concepts such as intrusion detection, anomaly detection, phishing prevention, threat intelligence, governance, explainability, privacy, interoperability, and institutional readiness. Second, similar codes were grouped into descriptive categories. Third, those descriptive categories were synthesized into broader analytical themes aligned with the research questions of this article [26], [27]. Based on the orientation of this study, the final synthesis was organized around three major analytical dimensions: (1) trends and research directions in AI-enabled cybersecurity for e-government services; (2) models, methods, and application domains of AI-based cyber defense in public digital environments; and (3) implementation challenges, including technical, organizational, ethical, governance, and regulatory issues. This thematic structure was selected to ensure direct consistency between the introduction, the review questions, and the interpretation of findings [22]–[27].

2.7. Validity and Reliability

Several measures were taken to enhance the validity and reliability of the review. First, the review protocol specified the databases, search strings, eligibility criteria, and analytical categories in advance in order to reduce ad hoc decision-making. Second, the use of multiple databases and supplementary snowballing improved retrieval breadth and reduced the likelihood of missing highly relevant studies. Third, the explicit use of a data extraction matrix and a formal appraisal instrument strengthened procedural consistency. Finally, the PRISMA-oriented reporting structure increased transparency by making the study identification and selection process traceable and replicable [22]–[25], [28]. Overall, this methodological design was intended to produce a rigorous and analytically coherent synthesis of current scholarship on AI and cybersecurity in e-government services, while also generating a strong basis for identifying research gaps, dominant technological approaches, and strategic implications for digital public governance [21]–[25].

3. RESULTS AND DISCUSSION

3.1. Characteristics of the Reviewed Literature

The reviewed literature indicates that the intersection of artificial intelligence, cybersecurity, and e-government services remains an emerging but rapidly expanding area of inquiry. Most studies are still distributed across adjacent domains rather than concentrated in one established research stream. In particular, the literature is commonly situated within three broader clusters: AI in public governance, AI and machine learning in cybersecurity, and cybersecurity governance in digital government or smart government environments. This pattern suggests that the field is conceptually rich but still fragmented, with relatively limited studies explicitly integrating all three dimensions into a single analytical framework [8], [9], [13], [29]. Another notable characteristic of the reviewed literature is the predominance of conceptual, review-based, and framework-oriented studies over field-based empirical investigations in operational government settings. The literature on AI in public governance repeatedly emphasizes the need for more public-sector-specific, explanatory, and implementation-oriented studies, while cybersecurity studies in e-

government similarly point to the need for more integrated and practice-grounded models. As a result, the current body of knowledge is sufficiently developed to identify major themes, opportunities, and risks, but still limited in terms of real-world evidence from specific service environments such as citizen portals, digital identity systems, inter-agency platforms, and smart-government infrastructures [8], [9], [13]. In substantive terms, the reviewed studies consistently portray AI not merely as an automation tool for improving administrative efficiency, but increasingly as a strategic enabler of cyber resilience, threat detection, secure interoperability, and digital trust in public service delivery. This is a significant shift, because it expands the role of AI from service enhancement to the broader protection of digital public infrastructures and data-intensive government ecosystems [13], [29].

3.2. Results Analysis

The analysis of the reviewed studies is organized according to the three research questions formulated in this article, namely: (1) the main trends and research directions in AI-driven cybersecurity for e-government services, (2) the dominant models and methods used, and (3) the implementation challenges and strategic implications of adopting AI in public-sector cyber defense.

a. Trends and Research Directions on AI in Cybersecurity for E-Government Services

The first major trend identified in the literature is the movement from viewing AI primarily as a tool for service automation and administrative efficiency toward understanding it as an enabling layer for secure and resilient digital government. Recent studies increasingly connect AI adoption in government with the protection of digital infrastructure, the mitigation of cyber risks, and the strengthening of institutional resilience in interconnected public-service ecosystems [8], [13], [29].

A second trend is the emergence of holistic cybersecurity thinking in e-government. Rather than relying on stand-alone technical controls, recent scholarship emphasizes the need to integrate AI-based monitoring and detection with broader cybersecurity governance, risk management, secure data exchange, and interoperability frameworks. This trend is particularly relevant in e-government because public digital services typically span multiple agencies, legal mandates, and legacy systems, making fragmented approaches increasingly ineffective [13].

A third trend concerns the growing importance of trustworthy, explainable, and accountable AI in public-sector cybersecurity. The literature suggests that predictive performance alone is insufficient in government settings, where automated decisions must also be interpretable, auditable, and compatible with public values such as legality, fairness, and procedural accountability [8], [9], [32].

b. Models and Methods Used in AI-Based Cybersecurity

The reviewed literature shows that the dominant AI approaches in cybersecurity remain machine learning, deep learning, anomaly detection, behavioral analytics, and intelligent classification models. These methods are frequently used for intrusion detection, phishing identification, malware classification, suspicious traffic analysis, and predictive threat intelligence. In many cases, deep learning models are preferred for high-dimensional and dynamic data environments, whereas anomaly-based methods are considered particularly useful when labeled attack data are limited or when new forms of cyber threats emerge rapidly [30], [31]. For e-government services, these models are especially relevant in the protection of citizen service portals, digital identity systems, cloud-based government platforms, and inter-agency communication infrastructures. Studies on AI-enhanced e-government suggest that AI can improve not only service responsiveness but also the mitigation of cyber-attacks by enabling faster and more adaptive risk detection capabilities [13], [29]. The literature also reveals a growing interest in Explainable AI (XAI) and privacy-preserving AI architectures. XAI is increasingly treated as a critical component for making security-related predictions interpretable and governable, while federated learning is regarded as a promising approach for distributed environments in which security-relevant data are fragmented across multiple institutional actors and cannot easily be centralized because of legal or privacy constraints [32], [33].

c. Challenges and Strategic Implications of AI Adoption

Despite its strong potential, the implementation of AI in cybersecurity for e-government services is constrained by a series of technical and institutional challenges. Common issues include fragmented data environments, limited interoperability, insufficient organizational readiness, the black-box nature of advanced models, and the growing sophistication of AI-enabled cyber threats. These constraints indicate that AI cannot be treated as an isolated technological solution; rather, it must be embedded within broader governance, oversight, and capability-building frameworks [8], [9], [13], [31]. The strategic implication of this finding is that strengthening cybersecurity in e-government requires more than technical deployment. It requires an integrated model in which AI supports detection and response, governance frameworks define accountability and risk controls, and public institutions invest in data management, interoperability, transparency, and professional capacity. In this sense, the literature points toward a socio-technical view of AI-driven cyber defense rather than a purely technological one [13], [32], [33].

3.3. Topic Classification

Based on the synthesis of the reviewed studies, the literature can be grouped into five major thematic clusters, as presented in Table 1.

Table 1. Main topic clusters

Topic Cluster	Scope and Main Focus
1. AI-Based Threat Detection and Intrusion Monitoring	This cluster focuses on the use of machine learning, deep learning, and anomaly detection models to identify malicious traffic, network intrusions, phishing attempts, ransomware behavior, and abnormal system activities in real time.
2. AI-Enhanced E-Government Service Security	This cluster examines how AI is applied to strengthen the cybersecurity of citizen-facing portals, digital identity systems, smart-government infrastructures, and cloud-based public service platforms.
3. Explainable and Trustworthy AI for Public Cybersecurity	This cluster emphasizes model transparency, interpretability, accountability, auditability, and human oversight in AI-driven cybersecurity systems, especially in public-sector settings where decisions must be justifiable.
4. Privacy-Preserving and Distributed Cybersecurity Intelligence	This cluster highlights federated learning, decentralized analytics, secure multi-institution collaboration, and privacy-preserving architectures for government environments in which data are distributed across agencies.
5. Governance, Ethics, and Institutional Readiness	This cluster focuses on regulatory compliance, data governance, organizational capacity, inter-agency coordination, public trust, and the ethical implications of deploying AI in cybersecurity governance.

This classification shows that the field is not limited to technical detection alone. Rather, it has developed into a broader research agenda that combines technical intelligence, institutional governance, public accountability, and digital trust. Such a pattern is consistent with recent literature that links AI in government to broader questions of implementation, governance, and public-sector legitimacy [8], [9], [13], [32], [33].

3.4. Gap and Challenge Analysis

Although the literature demonstrates the growing relevance of AI for strengthening cybersecurity in e-government services, several important research gaps and implementation challenges remain.

a. Limited Empirical Evidence in Specific E-Government Contexts

One of the clearest gaps is the limited number of empirical studies conducted in specific and operational public-service environments. Much of the literature remains conceptual or review-based, while real-world evaluations in digital identity systems, local government platforms, tax systems, health-government interfaces, and cross-agency infrastructures are still relatively scarce. This limits the ability of the literature to assess how AI performs under the institutional, legal, and technical conditions of actual government systems [8], [9], [13].

b. Black-Box Models and Accountability Risks

Another persistent challenge is the black-box nature of many advanced AI models. In public-sector cybersecurity, opaque predictions are problematic because security alerts and automated responses may have administrative, legal, and service-level consequences. Therefore, the lack of explainability undermines not only trust in AI outputs but also the ability of institutions to justify and audit cybersecurity decisions [32].

c. Data Silos, Privacy, and Interoperability Constraints

E-government systems are often distributed across multiple agencies and platforms, creating fragmented data environments that hinder integrated cyber defense. At the same time, cross-agency data sharing is constrained by privacy rules, legal mandates, and institutional boundaries. This creates a tension between the need for broad cyber intelligence and the obligation to protect sensitive public data. Federated and privacy-preserving approaches offer potential solutions, but their application in public-sector cybersecurity remains underdeveloped [13], [33].

d. Dual-Use Nature of AI and Adversarial Threats

AI is not only a defensive asset but also a potential enabler of offensive cyber activity. Recent literature on cybersecurity warns that AI, including generative AI, can be exploited to automate phishing, enhance reconnaissance, support malware development, and increase the speed and sophistication of attacks. This dual-use nature of AI creates a strategic challenge for e-government, because the same technological advances that improve defense may simultaneously elevate the threat landscape faced by public institutions [31], [34], [35].

e. Institutional Readiness and Governance Deficits

A further challenge lies in the limited readiness of public institutions to deploy AI-driven cybersecurity systems effectively. Successful implementation requires technical infrastructure, skilled personnel, governance mechanisms, procurement capacity, and clear oversight arrangements. The literature suggests that weak institutional readiness may reduce the practical value of AI systems even when the models themselves are technically advanced [9], [13].

3.5. Discussion

a. The Role of AI in Strengthening Cybersecurity in E-Government Services

The reviewed literature shows that AI plays a significant role in strengthening cybersecurity in e-government services by enabling more adaptive, predictive, and scalable forms of cyber defense. Through anomaly detection, intelligent classification, behavioral analysis, and predictive monitoring, AI can improve the ability of public institutions to identify threats earlier and respond more effectively than static or rule-based mechanisms alone [30], [31]. In e-government environments, this capability is particularly important because public digital services are increasingly interconnected and data-intensive. Citizen-facing systems, inter-agency data exchange platforms, and smart-government infrastructures require cyber defense mechanisms that can operate continuously and across diverse service contexts. In this regard, AI functions not only as a technical tool but as a strategic layer for supporting digital state resilience [13], [29].

b. Implementation of AI in Public Digital Service Environments

The literature further indicates that the value of AI depends on how well it is integrated into broader public-sector digital ecosystems. Effective implementation requires alignment between AI models, cybersecurity governance, service architecture, institutional workflows, and legal obligations. This means that successful AI adoption in e-government cannot be reduced to algorithm selection alone; it must also involve secure interoperability, human oversight, clear accountability, and data governance arrangements [8], [9], [13]. Moreover, the rise of explainable and privacy-preserving AI suggests that the future of AI-driven cybersecurity in e-government lies in systems that are not only accurate but also auditable, trustworthy, and institutionally governable. This is especially relevant in public settings where automated cybersecurity decisions may affect access, services, and institutional legitimacy [32], [33].

c. Strategic Implications for Future Research and Practice

Taken together, the literature supports an integrative interpretation: AI strengthens cybersecurity in e-government most effectively when it is embedded in a broader socio-technical system composed of detection capability, governance control, explainability, privacy protection, and organizational readiness. This implies that future research should move beyond general claims about AI effectiveness and instead examine which combinations of models, service domains, governance arrangements, and institutional capacities produce the most robust outcomes in real government environments [8], [13], [33]. From a practical perspective, public institutions should approach AI not as a stand-alone cybersecurity solution, but as one component of a broader digital governance strategy. Investments in AI-driven cybersecurity need to be accompanied by regulatory frameworks, inter-agency coordination, capacity building, explainability mechanisms, and safeguards against the misuse of AI by malicious actors. Only through such an integrated approach can AI contribute meaningfully to secure, resilient, and trusted e-government services [13], [31], [32].

4. CONCLUSION

This study has examined the role of Artificial Intelligence (AI) in strengthening cybersecurity in e-government services through a systematic literature review approach. The findings indicate that AI has become increasingly important in the protection of digital public services, not only as a tool for automation and efficiency, but also as a strategic mechanism for enhancing cyber resilience, detecting threats in real time, and supporting more adaptive security responses in interconnected government environments. The reviewed literature demonstrates that AI-based approaches, particularly machine learning, deep learning, anomaly detection, explainable AI, and privacy-preserving learning architectures, offer significant potential for improving the security of citizen-facing portals, digital identity systems, cloud-based platforms, and inter-agency information infrastructures. At the same time, the review shows that the contribution of AI to cybersecurity in e-government cannot be understood solely in technical terms. Its effectiveness is strongly influenced by broader institutional and governance conditions, including data availability and quality, interoperability across public agencies, organizational readiness, regulatory compliance, transparency requirements, and accountability mechanisms. The literature also reveals that public-sector cybersecurity differs from general organizational cybersecurity because security decisions in government are closely tied to public trust, legality, service continuity, and the protection of citizens' rights. For this reason, the integration of AI into e-government cybersecurity must be approached as a socio-technical and governance issue rather than as a stand-alone technological intervention.

Another important conclusion is that the field remains fragmented and still lacks sufficient empirical evidence from specific operational e-government contexts. Much of the existing scholarship is conceptual, review-based, or broadly focused on either AI in public administration or AI in cybersecurity, without fully integrating both within actual digital government service environments. This confirms the existence of a research gap and highlights the need for more context-sensitive studies that examine how AI-based cybersecurity models function in real government systems such as digital identity services, taxation platforms, public health infrastructures, municipal smart-government networks, and cross-agency service ecosystems. Overall, this study concludes that AI can make a substantial contribution to strengthening cybersecurity in e-government services when it is embedded within a comprehensive framework that combines intelligent threat detection, cybersecurity governance, explainability, privacy protection, and institutional capacity building. Accordingly, future research should move beyond general claims of AI effectiveness and focus on empirical validation, comparative implementation models, and governance-oriented design in diverse public-sector contexts. From a practical perspective, governments should not treat AI as a universal solution, but as one strategic component within a broader effort to build secure, trustworthy, accountable, and resilient digital public service systems.

REFERENCES

[1] T. Janowski, "Digital government evolution: From transformation to contextualization," *Government Information Quarterly*, vol. 32, no. 3, pp. 221–236, 2015, doi: https://doi.org/10.1016/j.giq.2015.07.001

[2] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," *Government Information Quarterly*, vol. 36, no. 4, art. no. 101385, 2019, doi: https://doi.org/10.1016/j.giq.2019.06.002

[3] L. Carter and F. Bélanger, "The utilization of e-government services: Citizen trust, innovation and acceptance factors," *Information Systems Journal*, vol. 15, no. 1, pp. 5–25, 2005, doi: https://doi.org/10.1111/j.1365-2575.2005.00183.x

[4] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems*, vol. 17, no. 2, pp. 165–176, 2008, doi: https://doi.org/10.1016/j.jsis.2007.12.002.

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

[6] B. W. Wirtz and W. M. Müller, "An integrated artificial intelligence framework for public management," *Public Management Review*, vol. 21, no. 7, pp. 1076–1100, 2019, doi: https://doi.org/10.1080/14719037.2018.1549268.

[7] B. W. Wirtz, P. F. Langer, and C. Fenner, "Artificial intelligence in the public sector – a research agenda," *International Journal of Public Administration*, vol. 44, no. 13, pp. 1103–1128, 2021, doi: https://doi.org/10.1080/01900692.2021.1947319.

[8] A. Zuiderwijk, Y.-C. Chen, and F. Salem, "Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda," *Government Information Quarterly*, vol. 38, no. 3, art. no. 101577, 2021, doi: https://doi.org/10.1016/j.giq.2021.101577.

[9] R. Madan and M. Ashok, "AI adoption and diffusion in public administration: A systematic literature review and future research agenda," *Government Information Quarterly*, vol. 40, no. 1, art. no. 101774, 2023, doi: https://doi.org/10.1016/j.giq.2022.101774.

[10] J. Bullock, M. M. Young, and Y.-F. Wang, "Artificial intelligence, bureaucratic form, and discretion in public service," *Information Polity*, vol. 25, no. 4, pp. 491–506, 2020, doi: https://doi.org/10.3233/IP-200223.

[11] Ž. Bojović, Đ. Klipa, P. D. Bojović, I. M. Jovanović, J. Šuh, and V. Šenk, "Interconnected Government Services: An Approach toward Smart Government," *Applied Sciences*, vol. 13, no. 2, art. no. 1062, 2023, doi: https://doi.org/10.3390/app13021062.

[12] P. A. W. Putro, D. I. Sensuse, and W. S. S. Wibowo, "Framework for critical information infrastructure protection in smart government: A case study in Indonesia," *Information and Computer Security*, vol. 32, no. 1, pp. 112–129, 2024, doi: https://doi.org/10.1108/ICS-03-2023-0031.

[13] V. Figueroa, L. E. Sánchez Crespo, A. Santos-Olmo, D. G. Rosado, and E. Fernández-Medina, "Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals," *International Journal of Information Security*, vol. 24, art. no. 121, 2025, doi: https://doi.org/10.1007/s10207-025-01024-0.

[14] F. Kamoun, F. Iqbal, M. A. Esseghir, and T. Baker, "AI and machine learning: A mixed blessing for cybersecurity," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, art. no. 9297323, doi: https://doi.org/10.1109/ISNCC49221.2020.9297323.

[15] N. Mohamed, "Current trends in AI and ML for cybersecurity: A state-of-the-art survey," *Cogent Engineering*, vol. 10, no. 2, art. no. 2272358, 2023, doi: https://doi.org/10.1080/23311916.2023.2272358.

[16] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction," *Applied Artificial Intelligence*, vol. 38, no. 1, art. no. 2439609, 2024, doi: https://doi.org/10.1080/08839514.2024.2439609.
[17] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey," *IEEE Access*, vol. 10, pp. 93575–93600, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3204171.
[18] I. H. Sarker, "Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," *Security and Privacy*, vol. 6, no. 5, art. no. e295, 2023, doi: https://doi.org/10.1002/spy2.295.
[19] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3300381.
[20] C. Nobles, "The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review," *Procedia Computer Science*, vol. 239, pp. 547–555, 2024, doi: https://doi.org/10.1016/j.procs.2024.06.206.
[21] D. Tranfield, D. Denyer, and P. Smart, "Towards a methodology for developing evidence-informed management knowledge by means of systematic review," *British Journal of Management*, vol. 14, no. 3, pp. 207–222, 2003, doi: https://doi.org/10.1111/1467-8551.00375.
[22] C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems*, vol. 37, art. 43, 2015, doi: https://doi.org/10.17705/1CAIS.03743.
[23] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," *Journal of Planning Education and Research*, vol. 39, no. 1, pp. 93–112, 2019, doi: https://doi.org/10.1177/0739456X17723971.
[24] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333–339, 2019, doi: https://doi.org/10.1016/j.jbusres.2019.07.039.
[25] M. J. Page *et al*., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021, doi: https://doi.org/10.1136/bmj.n71.
[26] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006, doi: https://doi.org/10.1191/1478088706qp063oa.
[27] J. Thomas and A. Harden, "Methods for the thematic synthesis of qualitative research in systematic reviews," *BMC Medical Research Methodology*, vol. 8, art. 45, 2008, doi: https://doi.org/10.1186/1471-2288-8-45.
[28] Q. N. Hong *et al*., "The Mixed Methods Appraisal Tool (MMAT) version 2018 for information professionals and researchers," *Education for Information*, vol. 34, no. 4, pp. 285–291, 2018, doi: https://doi.org/10.3233/EFI-180221.
[29] A. Al-Besher and K. Kumar, "Use of artificial intelligence to enhance e-government services," *Measurement: Sensors*, vol. 24, Art. no. 100484, 2022, doi: https://doi.org/10.1016/j.measen.2022.100484.
[30] R. Sen, G. Heim, and Q. Zhu, "Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics," *Communications of the Association for Information Systems*, vol. 51, pp. 179–209, 2022, doi: https://doi.org/10.17705/1CAIS.05109.
[31] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," *Knowledge and Information Systems*, vol. 67, pp. 6969–7055, 2025, doi: https://doi.org/10.1007/s10115-025-02429-y.
[32] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey," *IEEE Access*, vol. 10, pp. 93575–93600, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3204171.
[33] H. Li, L. Ge, and L. Tian, "Survey: federated learning data security and privacy-preserving in edge-Internet of Things," *Artificial Intelligence Review*, vol. 57, Art. no. 130, 2024, doi: https://doi.org/10.1007/s10462-024-10774-7.
[34] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3300381.
[35] C. Nobles, "The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review," *Procedia Computer Science*, vol. 239, pp. 547–555, 2024, doi: https://doi.org/10.1016/j.procs.2024.06.206.