

Quantitative Patterns in Trust-Related Machine-Learning Research Across Security, Biometrics, Robotics, Supply Chains, and Decision Analytics

Lucien beyli

Lucien@outlook.com

Amsterdam

Research Article

Keywords: quantitative content analysis, machine learning, IoT security, biometrics, explainable AI, supply-chain security, Bayesian learning, uncertainty

Posted Date: October 28th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11516377/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Quantitative Patterns in Trust-Related Machine-Learning Research Across Security, Biometrics, Robotics, Supply Chains, and Decision Analytics

Lucien Beyli

ARTICLE INFO

Keywords:

quantitative content analysis
machine learning
IoT security
biometrics
explainable AI
supply-chain security
Bayesian learning
uncertainty

ABSTRACT

Machine-learning literature concerned with operational trust spans security monitoring, biometric identity, swarm robotics, software and device supply chains, explainability, and uncertainty-aware decision making. This research article reports a reproducible quantitative content analysis of a predefined corpus of 69 scholarly and standards-oriented records published between 1992 and 2026. No new machine-learning model, architecture, dataset, or methodological framework is proposed. The analysis applies standard descriptive statistics, source-type and temporal cross-tabulation, title-level term-frequency analysis, and unsupervised TF-IDF clustering to characterize how the corpus is organized and how strongly bibliographic-title structure corresponds to manually coded application domains. The six coded domains are connected-device security and multimodal learning (17 records), swarm robotics and explainable AI (14), Bayesian and uncertainty-aware learning (12), biometric identity (11), cybersecurity supply-chain risk (10), and cross-cutting governance/documentation (5). Publication period differs across domains ($\chi^2 = 34.13$, $p = 0.0033$, Cramér's $V = 0.406$), reflecting the comparatively recent concentration of supply-chain and governance literature. Source type shows a moderate but borderline association with domain ($\chi^2 = 18.30$, $p = 0.0501$, Cramér's $V = 0.364$). Unsupervised title clustering provides only weak agreement with the six manual domains (adjusted Rand index = 0.124; normalized mutual information = 0.344), indicating that short bibliographic titles do not recover domain boundaries cleanly. The results are descriptive rather than novelty claims: they quantify the composition of the corpus and support a cautious cross-domain interpretation of recurring concerns such as security, uncertainty, interpretability, identity, provenance, and distribution shift.

1. Introduction

Machine-learning systems are increasingly deployed in settings where predictive accuracy interacts with security, privacy, interpretability, uncertainty, provenance, and operational constraints. Connected-device security studies examine device behavior and network telemetry [1–4], while large-scale incidents such as Mirai illustrate the operational consequences of weakly secured embedded systems [5]; biometric research studies recognition reliability and template protection [6–8]; swarm-robotics work addresses decentralized collective behavior and interpretability [9–11]; and supply-chain security research emphasizes provenance, dependencies, and lifecycle risk [12–14]. Bayesian and uncertainty-aware methods provide additional tools for expressing confidence and supporting risk-sensitive decisions [15–17].

The literature across these areas is heterogeneous in both purpose and evidence type. Some papers present predictive models, others provide surveys, standards, engineering guidance, or methodological foundations. Directly comparing predictive performance across such sources is therefore inappropriate because the reported outcomes do not share a common estimand. Instead, this article treats a predefined 69-record literature corpus as secondary data and applies standard quantitative content-analysis techniques to describe its composition.

The study addresses three descriptive questions: (RQ1) how are the records distributed across application domains, source types, and publication periods; (RQ2) which trust-related themes are visible in bibliographic titles; and (RQ3) how closely does an unsupervised title-based clustering recover the manually coded domain structure? The analysis is deliberately modest. It does not claim a new review methodology, a new learning algorithm, or a new theoretical framework.

ORCID(s):

2. Materials and Methods

2.1. Corpus definition

The dataset comprises the 69 bibliographic records listed in the reference section. The corpus was fixed before the quantitative analysis and was organized into six primary domains: connected-device security and multimodal learning; biometric identity and protection; swarm robotics and explainable AI; cybersecurity supply-chain risk; Bayesian and uncertainty-aware learning; and cross-cutting governance/documentation. Each record was assigned exactly one primary domain to avoid double counting. The corpus includes journal articles, conference papers, books or book chapters, technical reports, standards-oriented records, and preprints.

Consistent with established distinctions between narrative, systematic, and integrative literature methods [18], this is not presented as a systematic review or meta-analysis. The records were not obtained through a claim of exhaustive database retrieval, and no pooled effect size is calculated. The unit of analysis is the bibliographic record itself.

2.2. Metadata extraction

For each record, the analysis extracted publication year, bibliographic source type, title, and the manually assigned primary domain. Source types were normalized to journal article, conference paper, book/book chapter, technical report, and preprint or standards-oriented miscellaneous record. Publication year was grouped into four periods: 2009 or earlier, 2010–2015, 2016–2020, and 2021–2026.

2.3. Title-level text analysis

Titles were lower-cased and represented using term-frequency–inverse-document-frequency (TF–IDF) features with English stop-word removal and unigrams/bigrams. Terms appearing in fewer than two records were excluded. The resulting representation contained 96 features. K-means clustering was evaluated for $k = 2$ through 8 using cosine silhouette score. A six-cluster solution was additionally fitted because the manual coding contains six domains; its agreement with the manual labels was measured using adjusted Rand index (ARI) and normalized mutual information (NMI). These are standard exploratory text-analysis procedures and are used here only to characterize corpus structure.

2.4. Statistical analysis

Counts and percentages were calculated by domain, source type, publication period, and selected title themes. Pearson chi-square tests evaluated associations between domain and source type, and between domain and publication period. Effect size was summarized with Cramér's V . Because several cells are small and the corpus was predefined rather than randomly sampled, inferential results are interpreted descriptively rather than as population estimates. All calculations were reproduced using the accompanying Python script and exported CSV files.

3. Results

3.1. Corpus composition

The corpus contains 69 records spanning 1992–2026. Connected-device security and multimodal learning is the largest manually coded domain with 17 records (24.6%), followed by swarm robotics/explainable AI with 14 (20.3%), Bayesian/uncertainty-aware learning with 12 (17.4%), biometric identity with 11 (15.9%), supply-chain security with 10 (14.5%), and cross-cutting governance/documentation with 5 (7.2%).

Journal articles account for 34 records (49.3%), conference papers for 18 (26.1%), books/book chapters for 7 (10.1%), technical reports for 6 (8.7%), and preprint/standards-oriented miscellaneous records for 4 (5.8%). The median title length is 8 words and the mean is 8.59 words.

3.2. Temporal and source-type structure

The association between manually coded domain and publication period is statistically detectable in this corpus ($\chi^2(15) = 34.13$, $p = 0.0033$, Cramér's $V = 0.406$). Supply-chain security has the strongest recent concentration: 6 of its 10 records (60%) were published during 2021–2026. Cross-cutting governance/documentation also has a relatively recent profile, with 2 of 5 records (40%) in 2021–2026. In contrast, only 2 of 12 Bayesian/uncertainty records (16.7%) and 2 of 14 swarm/XAI records (14.3%) fall in the most recent period because these groups include older methodological foundations.

Source type also varies across the domains, although the association is borderline at the conventional 0.05 threshold ($\chi^2(10) = 18.30$, $p = 0.0501$, Cramér's $V = 0.364$). This result is consistent with the mixed nature of the corpus: some

Table 1

Primary-domain composition of the 69-record corpus.

Domain	<i>n</i>	Share
Connected-device security / multimodal ML	17	24.6%
Swarm robotics / explainable AI	14	20.3%
Bayesian / uncertainty-aware learning	12	17.4%
Biometric identity and protection	11	15.9%
Cybersecurity supply-chain risk	10	14.5%
Cross-cutting governance / documentation	5	7.2%
Total	69	100.0%

Table 2

Selected temporal characteristics by domain.

Domain	Mean year	2021–2026 share
Connected-device security / multimodal ML	2016.4	5.9%
Biometric identity and protection	2011.6	27.3%
Swarm robotics / explainable AI	2016.4	14.3%
Cybersecurity supply-chain risk	2020.0	60.0%
Bayesian / uncertainty-aware learning	2010.7	16.7%
Cross-cutting governance / documentation	2019.4	40.0%

domains are represented mainly by peer-reviewed application studies, while others depend materially on technical reports, standards, and foundational books.

3.3. Title-theme prevalence

A simple keyword-root scan of titles shows that security-related terms appear in 18 records (26.1%). Identity/biometric terms occur in 10 (14.5%), uncertainty-related terms in 9 (13.0%), IoT/device terms in 9 (13.0%), robotics/swarm terms in 8 (11.6%), interpretability-related terms in 6 (8.7%), and provenance/supply-chain terms in 6 (8.7%). These categories overlap and are not used as mutually exclusive labels; they provide a direct descriptive view of which concepts are visible in titles.

3.4. Unsupervised title clustering

The TF–IDF representation contained 96 retained unigram/bigram features. Across $k = 2$ to 8, silhouette scores were low, ranging from approximately 0.063 to 0.134. The largest observed value occurred at $k = 8$ (0.134), but the improvement over nearby values was small. This indicates that titles do not form sharply separated lexical groups.

For direct comparison with the six manual domains, a six-cluster K-means solution produced $ARI = 0.124$ and $NMI = 0.344$. The low ARI and modest NMI indicate weak-to-moderate correspondence between title-only lexical clusters and the manually coded application domains. This is unsurprising because several records use general methodological language—for example “machine learning”, “security”, “review”, or “Bayesian”—that cuts across domains.

The six fitted clusters were characterized by terms emphasizing: (1) general software/model/review language; (2) security, biometrics, privacy, and Internet-of-Things terminology; (3) swarm and robotics terminology; (4) supply-chain and attack terminology; (5) explainable/artificial-intelligence terminology; and (6) machine-learning, Bayesian, deep-learning, and multimodal terminology. The result supports a cautious interpretation: bibliographic titles carry domain signal, but they do not reproduce the manually coded structure cleanly.

4. Thematic Evidence Synthesis

4.1. Behavioral Profiling and Multimodal Security for Connected Devices

Behavior-based monitoring is attractive in IoT because many devices exhibit constrained, repeated patterns of communication and use. Botnet-oriented studies have shown that autoencoders and lightweight supervised models can

Table 3

Title-based clustering summary.

Measure	Value
TF-IDF features	96
Best silhouette in $k = 2 \dots 8$	0.134 ($k = 8$)
Six-cluster silhouette	0.133
Adjusted Rand index vs. manual domains	0.124
Normalized mutual information	0.344

exploit device-specific traffic regularities [19, 20]. Device-classification work similarly demonstrates that packet sizes, endpoints, timing, and protocol characteristics can support device identification without inspecting application payloads [21]. These approaches complement broader IoT-security surveys, which consistently emphasize heterogeneity, weak update practices, limited resources, and expanding attack surfaces [1–4].

A related line of work focuses on multimodal representation learning. Multimodal machine learning combines information from multiple sources, views, or feature families rather than relying on a single channel [22]. Early deep multimodal learning demonstrated the value of learning shared representations from heterogeneous inputs [23], while later surveys systematized fusion strategies and architectural choices [24]. In security settings, multimodality can mean combining network traffic with physical, temporal, interaction, or device-context features.

An application-oriented example is the smart-home study by Zita and Al-Hubaishi, which uses behavioral profiling and multimodal representation concepts to detect spoofing behavior in wireless smart-home devices [25]. The study is useful as an example of a wider trend: rather than treating a device only as an IP address or protocol endpoint, the detector can use behavioral context such as temporal activity, power-related indicators, and interaction patterns. Such approaches should nevertheless be interpreted cautiously when synthetic attacks or limited deployment traces dominate evaluation, because strong in-domain performance does not establish resilience to unseen device classes, user routines, or adversarial adaptation.

Tree-based learning remains common in these environments because it handles heterogeneous structured features efficiently. XGBoost and LightGBM provide scalable boosting frameworks that are often competitive on tabular security data [26, 27]. Imbalanced attack datasets also motivate oversampling methods such as SMOTE [28]. However, two deployment problems remain persistent: changing data distributions and poorly calibrated confidence. Concept-drift research shows that statistical relationships can evolve after deployment [29], while calibration studies demonstrate that classifier confidence may not correspond directly to empirical correctness [30]. For connected-device security, these issues are particularly important because firmware updates, network redesigns, and changing household behavior can alter the baseline without representing an attack.

4.2. Biometric Identity, Template Protection, and Cryptographic Binding

Biometric recognition links identity decisions to physiological or behavioral characteristics rather than memorized secrets. Foundational biometric literature describes recognition pipelines in terms of acquisition, feature extraction, matching, decision thresholds, and system-level error trade-offs [6]. Security analysis has also emphasized that biometric systems contain multiple attack surfaces, including sensors, feature extraction, template databases, matchers, and decision channels [7].

The central privacy difficulty is that biometric characteristics are not naturally revocable. If a password is exposed, it can be replaced; a compromised fingerprint cannot be reissued. Template-protection research therefore seeks cancelability, irreversibility, unlinkability, or cryptographic binding while preserving matching utility [8]. Fuzzy commitment schemes introduced error-tolerant cryptographic commitment for noisy inputs [31], while fuzzy extractors formalized methods for producing stable cryptographic material from noisy sources [32]. Fingerprint-specific fuzzy-vault implementations further demonstrated how minutiae-based representations can be coupled with cryptographic protection [33].

The fingerprint-based cryptographic-identity study by Zita and Khalil illustrates an application-level attempt to connect fingerprint recognition with key-pair generation [34]. Its relevance to the broader literature lies less in any single classifier choice than in the recurring design question: how should recognition evidence be transformed into cryptographic identity material without assuming that raw biometric measurements are perfectly reproducible? Standards

such as ISO/IEC 24745 formalize requirements for biometric information protection [35], while current digital-identity guidance emphasizes authenticator lifecycle, phishing resistance, and risk-appropriate authentication controls [36].

Behavioral biometrics broaden the concept of identity beyond fingerprints. Continuous authentication can use touch, movement, interaction cadence, or other user-specific signals to estimate whether the current operator remains consistent with the enrolled identity [37]. Touchalytics demonstrated the feasibility of touchscreen behavior as a continuous biometric signal [38]. Across both physiological and behavioral biometrics, the key trade-off is between discrimination and stability: features must separate users while tolerating legitimate within-user variation.

5. Interpretable Learning for Swarm-Robot Behavior

Swarm robotics studies decentralized groups of relatively simple robots whose global behavior emerges from local interactions. Early work defined the field in terms of biological inspiration, distributed control, robustness, scalability, and local sensing [9]. Subsequent surveys organized swarm engineering around design, analysis, task allocation, aggregation, collective movement, and distributed decision making [10, 11]. Physical platforms such as Kilobot made large-scale collective experiments more accessible [39], while thousand-robot demonstrations showed that programmable self-assembly could be achieved with simple local rules [40]. Heterogeneous systems such as Swarmanoid further illustrated how different robot morphologies can cooperate within one collective task [41]. Formal treatments have since emphasized the need for models that connect local rules to observable collective properties [42].

As robot swarms grow in complexity, interpretability becomes relevant for validation and diagnosis. Al-Hubaishi and Zita present an interpretable machine-learning framework for modeling and analyzing swarm-robot behaviors from structured interaction features [43]. This work can be situated within the broader explainable-AI literature, where local surrogate explanations such as LIME [44] and feature-attribution approaches such as SHAP [45] are commonly used to interpret predictive models. Surveys of explainable AI emphasize that explanation goals differ across debugging, user trust, regulatory accountability, and scientific understanding [46, 47].

The interpretability requirement in robotics is particularly nuanced. A model may accurately classify a behavioral phase while providing an unstable or misleading explanation of why that phase was predicted. Rudin argues that inherently interpretable models should be preferred over post-hoc explanation when decisions are high stakes and suitable transparent models are available [48]. Practical interpretability guidance similarly stresses that explanation methods should be evaluated in relation to the underlying model, data-generating process, and user objective rather than treated as universally reliable [49].

6. Cybersecurity Supply Chains and Device Provenance

Security decisions about connected systems extend beyond runtime traffic and user identity. Devices and software may enter an organization with hidden vulnerabilities, compromised components, malicious dependencies, or weak update processes. NIST's cybersecurity supply-chain risk-management guidance frames these risks as enterprise-level concerns spanning acquisition, development, integration, operations, and supplier relationships [12]. ENISA similarly documents supply-chain attacks as a growing source of systemic cyber risk because compromise at one supplier can propagate to many downstream organizations [13].

Software-supply-chain research has produced technical mechanisms for provenance and integrity, in-toto records and verifies the steps through which software artifacts are produced, allowing downstream users to check whether expected build and release processes were followed [14]. Earlier work on package-manager security showed that software distribution systems are themselves attractive attack surfaces [50]. Ecosystem studies of npm exposed dependency-driven risk and the potential impact of highly connected packages [51], while analyses of open-source supply-chain attacks catalogued malicious packages, compromised maintainers, build tampering, and related attack patterns [52].

The communication-device study by Zita and Zita focuses this discussion on high-risk environments and hardware/firmware supply-chain exposure [53]. It highlights a useful distinction between operational network defense and upstream assurance: a device can behave normally on the network while still containing compromised firmware, altered hardware, or an untrusted provenance path. Secure-development guidance such as the NIST Secure Software Development Framework addresses process-level practices intended to reduce vulnerabilities and tampering during software development [54], while software bills of materials are intended to improve transparency regarding software components and dependencies [55]. Industry observations on cyber-supply-chain risk management further emphasize governance, supplier criticality, information sharing, and continuous reassessment [56].

From a machine-learning perspective, supply-chain risk differs from conventional classification because labels are often incomplete, delayed, or ambiguous. A supplier with no known incident is not necessarily low risk, and a vulnerability count does not directly measure compromise probability. Consequently, model outputs in this area should be treated as decision-support evidence rather than definitive trust scores.

6.1. Bayesian Learning, Structured Decision Analytics, and Uncertainty

Bayesian learning provides a probabilistic language for combining prior beliefs with observed evidence. Standard treatments of probabilistic pattern recognition emphasize posterior inference, predictive distributions, regularization, and model uncertainty [15, 16]. Bayesian data analysis further distinguishes uncertainty in parameters, latent variables, observations, and model structure [57]. Early neural-network work used Bayesian reasoning to regularize model weights and quantify predictive uncertainty [58], while sparse Bayesian learning introduced the relevance vector machine as a probabilistic sparse alternative to margin-based classifiers [59].

Approximate Bayesian methods remain important when exact inference is computationally difficult. Dropout has been interpreted as approximate Bayesian inference for deep models [60], and work on aleatoric and epistemic uncertainty clarifies how different uncertainty sources matter for prediction and decision making [61]. Variational inference provides a general optimization-based approach to approximating otherwise intractable posterior distributions [62]. In structured tabular settings, non-Bayesian ensembles such as random forests also remain strong baselines because they are robust, efficient, and comparatively easy to inspect [63].

The hybrid Bayesian framework of Zita and colleagues combines classification and regression for job-title classification and salary estimation [64]. Although the application domain is workforce analytics rather than cybersecurity or robotics, it provides a useful methodological example of mixed predictive objectives on structured data. The broader lesson is that model selection should follow the decision problem: some systems need class labels, others need continuous estimates, and many need both uncertainty and calibrated decision thresholds.

Calibration and uncertainty should also be distinguished. Conformal prediction offers distribution-free finite-sample coverage guarantees under explicit assumptions and has become a practical framework for set-valued or abstaining prediction [17]. Earlier conformal-learning theory provides the mathematical foundation for this approach [65]. These techniques do not eliminate distribution shift, but they encourage a more cautious interface between predictive models and downstream decisions.

7. Cross-Cutting Findings

7.1. Representation is domain dependent

The reviewed fields all depend on representation choices. IoT security relies on packet, timing, behavioral, or multimodal features; biometrics depend on stable identity descriptors; swarm robotics requires summaries of local interaction and collective state; supply-chain analytics relies on provenance and dependency evidence; and structured decision analytics depends on semantically meaningful tabular variables. A high-capacity learner cannot compensate indefinitely for a representation that omits the information needed for the decision.

7.2. Interpretability has multiple meanings

Interpretability may refer to transparent model structure, local feature attribution, example-based reasoning, physically meaningful features, or a human-readable audit trail. The literature does not support treating one explanation method as universally appropriate. LIME and SHAP answer different questions from an interpretable rule set, and a feature attribution is not equivalent to a causal explanation [44, 45, 47, 48].

7.3. Uncertainty is operational, not decorative

Security and identity systems often require actions such as allow, deny, investigate, re-authenticate, quarantine, or defer. A point prediction alone does not specify when a system should abstain. Bayesian methods, calibrated probabilities, and conformal prediction provide different mechanisms for representing uncertainty, but each depends on assumptions about data and distribution stability [17, 30, 60, 61].

7.4. Distribution shift is a recurring failure mode

A model evaluated on one dataset can degrade when devices, users, robots, suppliers, or economic conditions change. Concept-drift research formalizes this issue for evolving data streams [29]. In applied systems, the same problem

appears through firmware updates, new biometric sensors, changed robot dynamics, newly compromised suppliers, and labor-market shifts. External validation and monitoring are therefore more informative than one static test-set score.

7.5. Reproducibility and documentation matter

Deployment risk is affected by more than the predictive algorithm. Machine-learning systems accumulate hidden technical debt through data dependencies, configuration, feedback loops, and operational coupling [66]. Dataset documentation can make collection conditions, intended use, and limitations more explicit [67]; model cards provide a parallel mechanism for documenting model behavior and evaluation boundaries [68]. Risk-management frameworks such as NIST AI RMF place these technical issues within broader governance and lifecycle processes [69].

8. Discussion

The quantitative analysis adds a descriptive layer to the literature synthesis without changing the nature of the underlying sources. The strongest structural result is temporal: the six manually coded domains do not have the same publication-age profile. Supply-chain security and governance/documentation are comparatively recent in this corpus, whereas Bayesian learning and biometric identity contain older foundational work. This difference helps explain why a simple cross-domain bibliography combines contemporary standards with long-established methodological sources.

The title-clustering result is equally informative because it is weak rather than strong. If titles alone recovered the six manual domains almost perfectly, the manual coding would add little information. Instead, the low ARI and modest NMI show that domain assignment depends on substantive reading rather than obvious title vocabulary. Terms such as “learning”, “security”, “model”, and “review” are shared across application areas, while specialized terms such as “swarm”, “biometric”, or “supply chain” create only partial separation.

These results should not be interpreted as evidence that one domain is more mature or more trustworthy than another. The corpus was deliberately heterogeneous and contains different publication types and purposes. The quantitative analysis describes this specific corpus; it does not estimate the full population of machine-learning research and does not rank the technical effectiveness of the methods discussed below.

9. Limitations

The study has four principal limitations. First, the 69-record corpus is predefined and not the result of an exhaustive database search, so the findings are not estimates of the entire literature. Second, manual assignment of one primary domain simplifies genuinely cross-domain papers. Third, title-level TF-IDF ignores abstracts and full text and therefore captures only coarse lexical structure. Fourth, chi-square results are based on a relatively small, purposefully assembled corpus with some sparse cells; p -values and effect sizes are therefore descriptive aids rather than evidence for broad population-level claims.

10. Conclusion

This article applied standard quantitative content-analysis procedures to a predefined 69-record corpus covering connected-device security, biometric identity, swarm robotics and explainability, cybersecurity supply chains, Bayesian and uncertainty-aware learning, and governance/documentation. The analysis found a moderate temporal association with domain and only weak agreement between title-based unsupervised clustering and manual domain coding. These findings support a restrained interpretation of the corpus: its application areas differ in publication history and vocabulary, but recurring concerns such as security, uncertainty, identity, interpretability, provenance, and distribution shift cross domain boundaries.

No novel algorithm, framework, dataset, or experimental system is claimed. The value of the study is limited to the reproducible quantitative description of the selected corpus and the accompanying domain-specific synthesis.

Data and code availability

The analyzed dataset is the 69-record bibliography distributed with the manuscript. The accompanying files `corpus_metadata.csv`, `cluster_assignments.csv`, `theme_prevalence.csv`, and `analysis_summary.json`, together with the Python analysis script, reproduce the quantitative results reported here.

References

- [1] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, 76:146–164, 2015. doi: 10.1016/j.comnet.2014.11.008.
- [2] Arsalan Mosenia and Niraj K. Jha. A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4):586–602, 2017. doi: 10.1109/TETC.2016.2606384.
- [3] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, 2017. doi: 10.1016/j.jnca.2017.04.002.
- [4] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, 21(3):2702–2733, 2019. doi: 10.1109/COMST.2019.2910750.
- [5] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *26th USENIX Security Symposium*, pages 1093–1110. USENIX Association, 2017.
- [6] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, 2004. doi: 10.1109/TCSVT.2003.818349.
- [7] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001. doi: 10.1147/sj.403.0614.
- [8] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008:579416, 2008. doi: 10.1155/2008/579416.
- [9] Erol Şahin. Swarm robotics: From sources of inspiration to domains of application. In *Swarm Robotics*, volume 3342 of *Lecture Notes in Computer Science*, pages 10–20. Springer, 2005. doi: 10.1007/978-3-540-30552-1_2.
- [10] Manuele Brambilla, Eliseo Ferrante, Mauro Birattari, and Marco Dorigo. Swarm robotics: A review from the swarm engineering perspective. *Swarm Intelligence*, 7:1–41, 2013. doi: 10.1007/s11721-012-0075-2.
- [11] Levent Bayindir. A review of swarm robotics tasks. *Neurocomputing*, 172:292–321, 2016. doi: 10.1016/j.neucom.2015.05.116.
- [12] Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon. Cybersecurity supply chain risk management practices for systems and organizations. Technical Report NIST SP 800-161 Rev. 1 Update 1, National Institute of Standards and Technology, 2024.
- [13] European Union Agency for Cybersecurity. Enisa threat landscape for supply chain attacks. Technical report, ENISA, 2021.
- [14] Santiago Torres-Arias, Hammad Afzali, Trishank Karthik Kuppasamy, Reza Curtmola, and Justin Cappos. in-toto: Providing farm-to-table guarantees for bits and bytes. In *28th USENIX Security Symposium*, pages 1393–1410. USENIX Association, 2019.
- [15] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer, 2006.
- [16] Kevin P. Murphy. *Machine Learning: A Probabilistic Perspective*. MIT Press, 2012.
- [17] Anastasios N. Angelopoulos and Stephen Bates. Conformal prediction: A gentle introduction. *Foundations and Trends in Machine Learning*, 16(4):494–591, 2023. doi: 10.1561/22000000101.
- [18] Hannah Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104:333–339, 2019. doi: 10.1016/j.jbusres.2019.07.039.
- [19] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. N-baiot: Network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, 2018. doi: 10.1109/MPRV.2018.03367731.
- [20] Rohan Doshi, Noah Aphorpe, and Nick Feamster. Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops*, pages 29–35, 2018. doi: 10.1109/SPW.2018.00013.
- [21] Arunan Sivanathan, Daniel Sherratt, Hassan Habibi Gharakheili, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. Classifying iot devices in smart environments using network traffic characteristics. *IEEE Transactions on Mobile Computing*, 18(8):1745–1759, 2019. doi: 10.1109/TMC.2018.2866249.
- [22] Tadas Baltrušaitis, Chaitanya Ahuja, and Louis-Philippe Morency. Multimodal machine learning: A survey and taxonomy. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(2):423–443, 2019. doi: 10.1109/TPAMI.2018.2798607.
- [23] Jiquan Ngiam, Aditya Khosla, Mingyu Kim, Juhan Nam, Honglak Lee, and Andrew Y. Ng. Multimodal deep learning. In *Proceedings of the 28th International Conference on Machine Learning*, pages 689–696, 2011.
- [24] Dhanesh Ramachandram and Graham W. Taylor. Deep multimodal learning: A survey on recent advances and trends. *IEEE Signal Processing Magazine*, 34(6):96–108, 2017. doi: 10.1109/MSP.2017.2738401.
- [25] Wail Zita and Mohammed Al-Hubaishi. Wireless smart home security via behavioral profiling and multimodal representation learning, 2026. Research Square preprint, version 1. doi: 10.21203/rs.3.rs-8428397/v1.
- [26] Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 785–794, 2016. doi: 10.1145/2939672.2939785.
- [27] Guolin Ke, Qi Meng, Thomas Finley, Taifeng Wang, Wei Chen, Weidong Ma, Qiwei Ye, and Tie-Yan Liu. Lightgbm: A highly efficient gradient boosting decision tree. In *Advances in Neural Information Processing Systems*, volume 30, 2017.
- [28] Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, and W. Philip Kegelmeyer. Smote: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16:321–357, 2002. doi: 10.1613/jair.953.
- [29] João Gama, Indrè Žliobaitė, Albert Bifet, Mykola Pechenizkiy, and Abdelhamid Bouchachia. A survey on concept drift adaptation. *ACM Computing Surveys*, 46(4):1–37, 2014. doi: 10.1145/2523813.
- [30] Chuan Guo, Geoff Pleiss, Yu Sun, and Kilian Q. Weinberger. On calibration of modern neural networks. In *Proceedings of the 34th International Conference on Machine Learning*, volume 70, pages 1321–1330, 2017.
- [31] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, pages 28–36, 1999. doi: 10.1145/319709.319714.

- [32] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008. doi: 10.1137/060651380.
- [33] Karthik Nandakumar, Anil K. Jain, and Sharath Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757, 2007. doi: 10.1109/TIFS.2007.908165.
- [34] Wail Zita and Mohammed Sayim Khalil. Fingerprint-based cryptographic identity: A custom recognition pipeline with key pair generation. *East Journal of Computer Science*, 1(3):17–34, 2025. doi: 10.63496/ejcs.Vol1.Iss3.112.
- [35] ISO/IEC. Iso/iec 24745:2022 information security, cybersecurity and privacy protection – biometric information protection, 2022.
- [36] David Temoshok, Yee-Yin Choong, James Fenton, Naomi Lefkowitz, Andrew Regenscheid, Justin Richer, Mary Theofanos, and Ryan Galluzzo. Digital identity guidelines: Authentication and authenticator management, 2025. NIST Special Publication 800-63B-4.
- [37] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbelo. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, 2016. doi: 10.1109/MSP.2016.2555335.
- [38] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, 2013. doi: 10.1109/TIFS.2012.2225048.
- [39] Michael Rubenstein, Christian Ahler, and Radhika Nagpal. Kilobot: A low cost scalable robot system for collective behaviors. In *2012 IEEE International Conference on Robotics and Automation*, pages 3293–3298, 2012. doi: 10.1109/ICRA.2012.6224638.
- [40] Michael Rubenstein, Alejandro Cornejo, and Radhika Nagpal. Programmable self-assembly in a thousand-robot swarm. *Science*, 345(6198):795–799, 2014. doi: 10.1126/science.1254295.
- [41] Marco Dorigo, Dario Floreano, Luca M. Gambardella, Francesco Mondada, Stefano Nolfi, Tarek Baaboura, Mauro Birattari, Michael Bonani, Manuele Brambilla, Arne Brutschy, et al. Swarmanoid: A novel concept for the study of heterogeneous robotic swarms. *IEEE Robotics & Automation Magazine*, 20(4):60–71, 2013. doi: 10.1109/MRA.2013.2252996.
- [42] Heiko Hamann. *Swarm Robotics: A Formal Approach*. Springer, Cham, 2018. doi: 10.1007/978-3-319-74528-2.
- [43] Mohammed Al-Hubaishi and Wail Zita. An interpretable machine learning framework for modeling and analysis of swarm robot behaviors. *Journal of High Speed Networks*, 32(2):107–125, 2026. doi: 10.1177/09266801251412545.
- [44] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. Why should i trust you?: Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 1135–1144, 2016. doi: 10.1145/2939672.2939778.
- [45] Scott M. Lundberg and Su-In Lee. A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems*, volume 30, 2017.
- [46] Amina Adadi and Mohammed Berrada. Peeking inside the black-box: A survey on explainable artificial intelligence (xai). *IEEE Access*, 6:52138–52160, 2018. doi: 10.1109/ACCESS.2018.2870052.
- [47] Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, Raja Chatila, and Francisco Herrera. Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. *Information Fusion*, 58:82–115, 2020. doi: 10.1016/j.inffus.2019.12.012.
- [48] Cynthia Rudin. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1:206–215, 2019. doi: 10.1038/s42256-019-0048-x.
- [49] Christoph Molnar. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*. 2 edition, 2022. Online book.
- [50] Justin Cappos, Justin Samuel, Scott Baker, and John H. Hartman. A look in the mirror: Attacks on package managers. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pages 565–574, 2008. doi: 10.1145/1455770.1455841.
- [51] Markus Zimmermann, Cristian-Alexandru Staicu, Cam Tenny, and Michael Pradel. Small world with high risks: A study of security threats in the npm ecosystem. In *28th USENIX Security Symposium*, pages 995–1010. USENIX Association, 2019.
- [52] Marc Ohm, Henrik Plate, Arnold Sykosch, and Michael Meier. Backstabber’s knife collection: A review of open source software supply chain attacks. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, volume 12223 of *LNCS*, pages 23–43. Springer, 2020. doi: 10.1007/978-3-030-52683-2_2.
- [53] Wail Zita and Nassma Zita. Mitigating supply chain risks in communication devices across conflict zones, 2025. TechRxiv preprint.
- [54] Murugiah Souppaya, Karen Scarfone, and Donna Dodson. Secure software development framework (ssdf) version 1.1: Recommendations for mitigating the risk of software vulnerabilities. Technical Report SP 800-218, NIST, 2022.
- [55] National Telecommunications and Information Administration. The minimum elements for a software bill of materials (sbom). Technical report, U.S. Department of Commerce, 2021.
- [56] Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol. Key practices in cyber supply chain risk management: Observations from industry. Technical Report IR 8276, NIST, 2021.
- [57] Andrew Gelman, John B. Carlin, Hal S. Stern, David B. Dunson, Aki Vehtari, and Donald B. Rubin. *Bayesian Data Analysis*. CRC Press, 3 edition, 2013.
- [58] David J. C. MacKay. A practical bayesian framework for backpropagation networks. *Neural Computation*, 4(3):448–472, 1992. doi: 10.1162/neco.1992.4.3.448.
- [59] Michael E. Tipping. Sparse bayesian learning and the relevance vector machine. *Journal of Machine Learning Research*, 1:211–244, 2001.
- [60] Yarín Gal and Zoubin Ghahramani. Dropout as a bayesian approximation: Representing model uncertainty in deep learning. In *Proceedings of the 33rd International Conference on Machine Learning*, volume 48, pages 1050–1059, 2016.
- [61] Alex Kendall and Yarín Gal. What uncertainties do we need in bayesian deep learning for computer vision? In *Advances in Neural Information Processing Systems*, volume 30, 2017.
- [62] David M. Blei, Alp Kucukelbir, and Jon D. McAuliffe. Variational inference: A review for statisticians. *Journal of the American Statistical Association*, 112(518):859–877, 2017. doi: 10.1080/01621459.2017.1285773.
- [63] Leo Breiman. Random forests. *Machine Learning*, 45:5–32, 2001. doi: 10.1023/A:1010933404324.

- [64] Wail Zita, Sami Abou El Faouz, Mohanad Alayedi, and Ebrahim E. Elsayed. A hybrid bayesian machine learning framework for simultaneous job title classification and salary estimation. *Symmetry*, 17(8):1261, 2025. doi: 10.3390/sym17081261.
- [65] Vladimir Vovk, Alexander Gammerman, and Glenn Shafer. *Algorithmic Learning in a Random World*. Springer, 2005.
- [66] D. Sculley, Gary Holt, Daniel Golovin, Eugene Davydov, Todd Phillips, Dietmar Ebner, Vinay Chaudhary, Michael Young, Jean-François Crespo, and Dan Dennison. Hidden technical debt in machine learning systems. In *Advances in Neural Information Processing Systems*, volume 28, 2015.
- [67] Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, and Kate Crawford. Datasheets for datasets. *Communications of the ACM*, 64(12):86–92, 2021. doi: 10.1145/3458723.
- [68] Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru. Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, pages 220–229, 2019. doi: 10.1145/3287560.3287596.
- [69] Elham Tabassi. Artificial intelligence risk management framework (ai rmf 1.0). Technical Report NIST AI 100-1, National Institute of Standards and Technology, 2023.