American Journal of Applied Science and Technology

VOLUME Vol.06 Issue04 2026
PAGE NO. 1-15

Sustainable Self-Compacting Cementitious Composites and Intelligent Intrusion Detection for IOT Systems: A Dual-Lens Analysis of Resilience in Built and Digital Infrastructure

Dr. Emilia Varga

Department of Civil and Digital Systems Engineering, Central European Institute of Technology, Hungary

Received: 05 February 2026; **Accepted:** 03 March 2026; **Published:** 01 April 2026

Abstract: Background: Contemporary infrastructure resilience is increasingly defined by two parallel demands: the need for durable, sustainable, and high-performance construction materials, and the need for intelligent, adaptive, and trustworthy cybersecurity mechanisms for highly connected Internet of Things environments. The references supplied for this study cover self-compacting concrete, reactive powder concrete, foam concrete, fiber modification, supplementary cementitious materials, sulfate and thermal resistance, and sustainable mix design. They also cover intrusion detection for IoT, wireless sensor networks, in-vehicle networks, graph neural networks, transformers, explainable artificial intelligence, network forensics, transfer learning, and benchmark datasets. Although these literatures are usually studied independently, both address the same deeper problem: how complex systems can remain reliable under uncertain, evolving, and often hostile operating conditions.

Objective: This article develops an original, publication-ready research synthesis based strictly on the provided references. Its purpose is to construct an integrated analytical framework that explains how resilience is designed, assessed, and improved in both material infrastructure and cyber-physical infrastructure.

Methodology: A text-based integrative research design was employed. The civil engineering literature was interpreted through the lenses of mix optimization, durability, thermal response, sustainable materials, and fiber-enhanced performance. The cybersecurity literature was interpreted through the lenses of data representation, lightweight detection, graph-based learning, explainability, transfer robustness, and IoT-specific attack detection. These domains were then compared at the conceptual level of system resilience, adaptive performance, and design under constraints.

Results: The analysis indicates that sustainable self-compacting and advanced cementitious composites achieve resilience through material tailoring, reduced defect sensitivity, and environmentally conscious substitution strategies. In parallel, IoT intrusion detection systems achieve resilience through feature engineering, lightweight models, graph-based learning, self-supervision, explainability, and robustness-preserving transfer methods. Across both domains, resilience emerges not from single-variable optimization but from structured balance among performance, adaptability, efficiency, and reliability.

Conclusion: The article argues that civil material innovation and cybersecurity intelligence should be understood as parallel sciences of resilience. Though their objects differ, both require multi-factor design, tolerance to uncertainty, and disciplined evaluation under real constraints. This integrated perspective offers a broader theoretical basis for future research on sustainable and secure infrastructure.

Keywords: Self-compacting concrete, sustainable materials, intrusion detection, Internet of Things, graph neural networks, infrastructure resilience, advanced composites.

Introduction: Infrastructure in the twenty-first century is no longer reducible to roads, buildings, servers, or networks considered separately. It is increasingly hybrid, layered, and interdependent. Built systems depend on digital monitoring and automation. Digital systems depend on physical deployment, environmental stability, and reliable hosting environments. As a result, the question of resilience can no longer be confined to one discipline. Civil engineers ask how concrete structures can sustain load, heat, internal chemical attack, and environmental degradation while remaining cost-effective and sustainable. Cybersecurity researchers ask how networked systems, especially Internet of Things environments, can detect, interpret, and resist malicious behavior under conditions of scale, heterogeneity, and data imbalance. Although these fields use different terminologies, they are animated by a common problem: how can complex, performance-critical systems be designed to remain functional when exposed to stress, uncertainty, and evolving forms of failure?

The references supplied for this article reveal this duality with striking clarity. One cluster focuses on self-compacting concrete, reactive powder concrete, foam concrete, fiber-modified systems, waste incorporation, slag substitution, metakaolin enhancement, magnetized water, sulfate resistance, and thermal behavior (Abbas et al., 2022; Al-Obaidy, 2017; Altwair et al., 2025; Awang & Aljoumaily, 2017; Benjeddou et al., 2022; Gheidan et al., 2025; Majeed et al., 2023; Memon et al., 2018; Ozodabas, 2018; Saand et al., 2019; Salman & Al-Mulali, 2025). Another cluster focuses on intrusion detection systems for IoT and related cyber-physical environments, drawing on machine learning classifiers, support vector machines, deep autoencoders, graph neural networks, self-supervised learning, transformers, explainable models, distributed attack detection, and specialized IoT datasets (Akuthota & Bhargava, 2025; Alrayes et al., 2024; Binbusayyis, 2025; Deng et al., 2023; Duan et al., 2023; Gaur & Kumar, 2022; Ghorbani & Fakhrahmad, 2022; Gu & Lu, 2021; Hu et al., 2023; Huang et al., 2025; Jan et al., 2019; Koroniotis et al., 2018, 2020; Lo et al., 2022; Mahbooba et al., 2021; Neto et al., 2023; Nguyen & Kashef, 2023; Sadia et al., 2024; Sadhwani et al., 2023).

At first glance, these literatures appear unrelated. One concerns mineral binders, rheology, aggregate systems, thermal degradation, and mechanical behavior. The other concerns packet flows, malicious traffic, feature embeddings, deep models, and attack classification. Yet at a deeper level, both literatures are engaged in a parallel scientific enterprise. Both are concerned with heterogeneous systems whose performance depends on the interaction of many variables. Both involve trade-offs between efficiency and robustness. Both are increasingly shaped by sustainability and scalability concerns. Both have moved beyond simplistic single-parameter design toward high-dimensional optimization. And both are confronted by the reality that real systems fail not only under idealized laboratory conditions, but under noisy, dynamic, and often adversarial environments.

Self-compacting concrete is one of the clearest examples of modern performance-oriented material design. Unlike conventional concrete, self-compacting concrete must achieve high flowability, filling ability, and passing ability without segregation, while also delivering structural and durability performance acceptable for practical use (Memon et al., 2018). That requirement makes it a design problem of balance rather than brute strength. The material must move easily yet remain stable; it must be workable yet sufficiently cohesive; it must often perform under sustainability constraints involving partial replacement materials or industrial by-products (Abbas et al., 2022; Altwair et al., 2025; Saand et al., 2019). This makes self-compacting concrete an ideal case study for resilience in materials science, because its performance depends on carefully tuned interactions among constituents rather than on maximizing a single property.

Reactive powder concrete and foam concrete extend this logic into more specialized territory. Reactive powder concrete pursues exceptional density, strength, and advanced performance through finely controlled composition, often incorporating fibers and nontraditional additives (Al-Mulla & Al-Rihimy, 2025; Majeed et al., 2023). Foam concrete, by contrast, introduces deliberate cellular structure and weight reduction while trying to preserve enough mechanical adequacy for intended applications (Awang & Aljoumaily, 2017; Salman & Al-Mulali, 2025). These material systems remind us that performance in infrastructure materials is not uniform. Different structural and operational contexts require different balances of density, strength, thermal behavior, sustainability, and specialized functionality. Thus, resilience in concrete science is not the pursuit of one universally superior material. It is the pursuit of materials tailored to perform reliably within a defined envelope of constraints.

The cybersecurity references show a closely analogous evolution. Early intrusion detection research often focused on relatively traditional machine learning pipelines and manually engineered features, with

special attention to support vector machines, fuzzy models, and conventional classifiers (Sheng & Zhigang, 2018; Gu & Lu, 2021; Gaur & Kumar, 2022). Over time, the field expanded toward sparse autoencoders, hybrid architectures, feature engineering frameworks, and lightweight models suited to IoT constraints (Ghorbani & Fakhrahmad, 2022; Kamaldeep et al., 2023; Sadhwani et al., 2023). More recently, graph neural networks, self-supervised methods, transformers, and contrastive distillation approaches have emerged as responses to the relational, dynamic, and sometimes label-limited nature of modern network traffic (Deng et al., 2023; Duan et al., 2023; Hu et al., 2023; Akuthota & Bhargava, 2025; Huang et al., 2025). Here too, resilience is no longer achieved by a single classifier metric in a static benchmark environment. It increasingly depends on architecture choice, representation strategy, trustworthiness, generalization capacity, and operational efficiency.

A central problem in both domains is that failure mechanisms are evolving. In concrete systems, durability threats include internal sulfate attack, high temperature exposure, variable environmental loads, and the uncertain long-term implications of introducing waste or alternative materials into mixes (Al-Obaidy, 2017; Benjeddou et al., 2022; Gheidan et al., 2025). In intrusion detection systems, threats include DDoS attacks, botnets, multiclass cyberattacks, label scarcity, adversarial generalization challenges, and the growing heterogeneity of IoT and in-vehicle network environments (Gaur & Kumar, 2022; Ismail et al., 2022; Koroniotis et al., 2018; Huan et al., 2024; Alrayes et al., 2024). In both cases, the system must be designed not only for known conditions, but for a spectrum of possible disruptions. This places a premium on flexible design principles rather than brittle optimizations.

The sustainability dimension is also crucial. In concrete research, sustainability appears through low-cost self-consolidation concrete using sustainable materials, the use of Libyan iron slag, blast furnace slag, metakaolin, glass waste, and nanotechnology-enhanced foam concrete with sustainability claims (Abbas et al., 2022; Altwair et al., 2025; Awang & Aljoumaily, 2017; Majeed et al., 2023; Saand et al., 2019; Salman & Al-Mulali, 2025). These studies reflect the wider transformation of civil engineering away from purely Portland-cement-dominant thinking toward material circularity and resource efficiency. In cybersecurity, sustainability appears differently but no less importantly. It emerges as computational efficiency, lightweight deployment, transfer learning, distributed detection, and model architectures that can operate in resource-constrained devices or real-time systems (Jan et al., 2019; Nguyen & Kashef, 2023; Akuthota & Bhargava, 2025; Alrayes et al., 2024). Here, sustainability is not environmental material substitution but operational viability under finite computation, energy, and labeling resources. This difference is instructive. It shows that sustainability is domain-specific in form but not in importance.

Another common theme is the move from generic solutions to context-aware systems. Concrete design is increasingly tailored to particular risks and application contexts: thermal resistance, sulfate durability, attenuation properties, fiber behavior, or workability under self-compaction requirements (Al-Obaidy, 2017; Benjeddou et al., 2022; Gheidan et al., 2025; Majeed et al., 2023). Similarly, intrusion detection research increasingly targets specific operational environments such as IoT networks, wireless sensor networks, smart airports, and in-vehicle networks, rather than assuming one universal network threat model (Jan et al., 2019; Koroniotis et al., 2020; Sadia et al., 2024; Huan et al., 2024). This contextualization reflects scientific maturity. As fields advance, they tend to abandon overly generic claims and instead pursue performance under specific, realistic conditions.

The references also indicate an important methodological shift in both domains. Concrete research increasingly studies interactions among multiple modifiers rather than isolated components. For example, fiber-reinforced systems are analyzed not only in terms of strength, but thermal and mechanical behavior, moisture-related interactions, and compatibility with supplementary cementitious materials (Al-Mulla & Al-Rihimy, 2025; Gheidan et al., 2025). Likewise, intrusion detection research increasingly combines representation learning, feature selection, graph structure, self-supervision, and explainability rather than treating classification as a standalone step (Borisov et al., 2019; Mahbooba et al., 2021; Lo et al., 2022; Deng et al., 2023; Huang et al., 2025). This reflects a shared scientific realization: real-world resilience is emergent. It arises from the coordinated behavior of interacting system elements, not from a single local improvement.

Despite these parallels, the two literatures are rarely placed into dialogue. Civil engineering papers on self-compacting or foam concrete do not usually speak to intrusion detection frameworks. Cybersecurity papers on graph neural networks do not usually concern themselves with material durability or sustainability. This disciplinary separation is understandable, but it also limits theoretical imagination. A comparative reading can reveal common design philosophies that are otherwise obscured. For example, both domains confront the problem of signal and noise. In concrete, rheological balance and mix stability determine whether performance-enhancing components yield

coherent material behavior or undesirable segregation and brittleness. In intrusion detection, feature engineering and representation learning determine whether useful attack patterns emerge from noisy traffic or are lost in irrelevant variation. Both domains also confront the problem of robustness versus specialization. A system optimized too narrowly may perform impressively under one test condition yet fail under variation.

The literature gap addressed by this article therefore lies not in the absence of studies within either field, but in the absence of a structured cross-domain interpretation of resilience. Existing references richly document innovations within sustainable self-compacting and advanced cementitious materials, and within IoT intrusion detection. What is missing is a scholarly synthesis that interprets these innovations as parallel efforts to engineer reliability in complex systems. Such a synthesis does not collapse the differences between concrete and cybersecurity. Instead, it uses those differences to illuminate common principles: adaptive design, constrained optimization, robustness to evolving stressors, and the need for meaningful evaluation frameworks.

Accordingly, the objective of this article is to generate a complete, publication-ready original research narrative based strictly on the provided references, examining sustainable advanced cementitious composites and intelligent intrusion detection systems as dual manifestations of resilience science. The article argues that both literatures can be understood through a common conceptual framework centered on reliability under uncertainty, performance tuning under constraints, and the transition from static designs to adaptive systems. More specifically, the article aims to explain how sustainable self-compacting and related concrete systems achieve resilience through material selection and structural behavior, how modern intrusion detection systems achieve resilience through algorithmic intelligence and representation learning, and how the comparison of these domains can enrich our understanding of infrastructure as a whole.

The central proposition advanced here is that resilient infrastructure is both physical and computational, and that the scientific principles underpinning reliable material systems and reliable intrusion detection systems are more analogous than they first appear. In both domains, performance depends on complex internal architecture, sensitivity to context, and the careful balancing of competing objectives. Recognizing this parallel does not merely produce an interesting interdisciplinary insight. It offers a stronger intellectual basis for thinking about future infrastructure as an integrated socio-technical environment requiring both sustainable physical materials and trustworthy digital defenses.

METHODOLOGY

This article employs an integrative, text-based research methodology grounded strictly in the references supplied by the user. The methodological approach was designed to satisfy two simultaneous requirements: first, to remain fully anchored in the provided literature without introducing external sources; second, to produce a publication-ready research narrative rather than a simple annotated summary. Because the supplied references span two distinct technical domains—advanced cementitious materials and intrusion detection for IoT and related networks—the method had to be both domain-sensitive and conceptually integrative.

The first step in the methodological design was corpus segmentation. The references were divided into two primary knowledge clusters. The first cluster contained literature related to self-compacting concrete, reactive powder concrete, foam concrete, material sustainability, thermal and chemical durability, and modifier effects. This cluster included work on sustainable self-consolidation concrete, magnetized water, sulfate attack, Libyan iron slag, granulated blast furnace slag, nanotechnology in foam concrete, polymeric fibers, glass waste in reactive powder concrete, high-temperature effects, basalt fiber, metakaolin, and broad review literature on self-compacting concrete with cementitious materials and fibers (Abbas et al., 2022; Abbas et al., 2022; Al-Mulla & Al-Rihimy, 2025; Al-Obaidy, 2017; Altwair et al., 2025; Awang & Aljoumaily, 2017; Benjeddou et al., 2022; Gheidan et al., 2025; Majeed et al., 2023; Memon et al., 2018; Ozodabas, 2018; Saand et al., 2019; Salman & Al-Mulali, 2025). The second cluster contained the intrusion detection literature, including traditional machine learning, hybrid models, explainable AI, graph neural networks, self-supervised methods, transformers, distributed deep learning, and benchmark datasets relevant to IoT, wireless sensor networks, botnets, smart airports, and in-vehicle networks (Akuthota & Bhargava, 2025; Alrayes et al., 2024; Binbusayyis, 2025; Borisov et al., 2019; Chang & Branco, 2021; Deng et al., 2023; Duan et al., 2023; Gaur & Kumar, 2022; Ghorbani & Fakhrahmad, 2022; Gu & Lu, 2021; Hu et al., 2023; Huan et al., 2024; Huang et al., 2025; Ismail et al., 2022; Jan et al., 2019; Kamaldeep et al., 2023; Koroniotis & Moustafa, 2020; Koroniotis et al., 2018, 2020; Lo et al., 2022; Mahbooba et al., 2021; Neto et al., 2023; Nguyen & Kashef, 2023; Sadia et al., 2024; Sadhwani et al., 2023; Sheng & Zhigang, 2018).

The second methodological step was internal thematic coding within each cluster. In the concrete cluster, sources were coded across six themes: sustainability and material substitution; rheological and fresh-state control; mechanical and structural performance; durability under chemical and thermal attack; fiber and microstructural modification; and specialized or emerging enhancements. For example, sustainable substitution was coded from Abbas et al. (2022), Altwair et al. (2025), Awang and Aljoumaily (2017), Majeed et al. (2023), and Saand et al. (2019). Durability under chemical or thermal exposure was coded from Al-Obaidy (2017), Benjeddou et al. (2022), and Gheidan et al. (2025). Fiber and interfacial behavior was informed by Al-Mulla and Al-Rihimy (2025), Ozodabas (2018), and Gheidan et al. (2025). Emerging enhancements were interpreted through Abbas et al. (2022) on magnetized water and Salman and Al-Mulali (2025) on nanotechnology in foam concrete.

In the intrusion detection cluster, sources were coded across seven themes: lightweight and resource-aware detection; classical machine learning and hybrid approaches; feature engineering and feature selection; explainability and trust; graph-based learning; self-supervised, transfer, and robustness-oriented learning; and application-specific environments and datasets. Lightweight design was coded from Jan et al. (2019), Sadhwani et al. (2023), and Akuthota and Bhargava (2025). Classical and hybrid approaches were informed by Sheng and Zhigang (2018), Gu and Lu (2021), Gaur and Kumar (2022), Ghorbani and Fakhrahmad (2022), and Ismail et al. (2022). Feature engineering and feature selection were informed by Kamaldeep et al. (2023) and Borisov et al. (2019). Explainability and trust came from Mahbooba et al. (2021). Graph-based learning was strongly represented by Chang and Branco (2021), Lo et al. (2022), Deng et al. (2023), Duan et al. (2023), and Hu et al. (2023). Robustness-preserving and self-supervised learning were drawn from Nguyen and Kashef (2023) and Huang et al. (2025). Application-specific adaptation was drawn from Huan et al. (2024), Koroniotis et al. (2018, 2020), Sadia et al. (2024), and Neto et al. (2023).

The third methodological step was comparative abstraction. This was the key step that transformed the article from two adjacent mini-reviews into an integrated research paper. After identifying thematic structures within each domain, the study abstracted a higher-order set of conceptual dimensions shared by both literatures. These dimensions were: resilience under stress, performance optimization under constraints, adaptive architecture, role of auxiliary modifiers, domain-specific evaluation, robustness under uncertainty, and sustainability or efficiency. These shared dimensions were not imposed arbitrarily; they emerged through repeated cross-reading of the literature. For example, resilience under stress is explicit in studies of sulfate attack, high temperature, and thermal behavior in concrete, and equally explicit in studies of cyberattacks, DDoS detection, and IoT intrusion resilience (Al-Obaidy, 2017; Benjeddou et al., 2022; Gaur & Kumar, 2022; Alrayes et al., 2024). Adaptive architecture appears in the tailoring of concrete mixes through slag, fibers, metakaolin, or glass waste, and in the tailoring of detection systems through graph neural networks, transformers, or self-supervised learning (Altwair et al., 2025; Ozodabas, 2018; Deng et al., 2023; Akuthota & Bhargava, 2025).

The fourth methodological step was interpretive triangulation. A major claim in the article was accepted only when supported by convergence from multiple references and, where possible, from both domains. For example, the claim that resilience is not a single-variable property but a balanced systems outcome was supported in the concrete domain by the interaction of workability, strength, durability, and sustainable substitution across Abbas et al. (2022), Memon et al. (2018), and Gheidan et al. (2025), and in the intrusion detection domain by the interaction of accuracy, lightweight deployment, explainability, and robustness across Jan et al. (2019), Mahbooba et al. (2021), and Huang et al. (2025). This triangulation approach reduced the risk of overstating isolated findings and strengthened the internal coherence of the analysis.

The fifth methodological step was handling of heterogeneous evidence types. The reference list includes experimental studies, reviews, conference papers, benchmark datasets, and arXiv preprints. Rather than forcing all sources into a single evidentiary category, the methodology treated them according to functional role. Experimental concrete studies were read primarily for evidence of modifier effects, durability responses, and performance implications. Review articles were used for field-level synthesis and trend identification. In the cybersecurity cluster, benchmark dataset papers and conference papers were read not only as empirical contributions but as indicators of methodological direction, community priorities, and operational concerns. Preprints such as Chang and Branco (2021) and Koroniotis and Moustafa (2020) were used cautiously as conceptually relevant but not given disproportionate authority over peer-reviewed contributions.

The sixth methodological step was constraint-sensitive interpretation. Because the user explicitly requested strict reliance on the provided references, the article avoided introducing external definitions, performance statistics, standards, or theoretical frameworks not

recoverable from the cited works. This required a descriptive-analytical style rather than a quantitatively comparative one. The article therefore focuses on mechanisms, implications, trade-offs, and conceptual relationships rather than unsupported numerical benchmarking. This approach is especially important because the two domains use different metrics and evaluation standards. Attempting to artificially quantify them against one another would have produced a false equivalence unsupported by the literature.

The seventh methodological step was synthesis through the concept of infrastructure resilience. Rather than comparing concrete and intrusion detection directly at the level of objects, the study compared them at the level of function. Concrete is a material substrate of physical infrastructure. Intrusion detection is a defensive substrate of digital or cyber-physical infrastructure. Both are therefore infrastructural sciences in the broad sense. This framing allowed the article to treat them as different expressions of the same systems problem: ensuring dependable operation under stress. The synthesis was structured to preserve technical specificity while extracting broader theoretical significance.

The eighth methodological step involved exclusion logic. Several plausible but unsupported directions were intentionally excluded. For instance, the article does not speculate on smart concrete embedded with IoT sensors, because no such references were provided. It does not claim unified evaluation metrics for concrete durability and cyberattack resistance, because the literature does not support such a direct formal mapping. It also avoids making policy or economic claims beyond what can be reasonably inferred from sustainable material and lightweight model discussions. This exclusion discipline was necessary to maintain fidelity to the source base.

The ninth methodological step was argument sequencing. The article first establishes each domain on its own technical terms before drawing conceptual comparisons. This was methodologically important because premature analogy can flatten domain-specific meaning. By first allowing self-compacting and related cementitious composites to speak through workability, fibers, thermal resistance, slag substitution, and chemical durability, and allowing intrusion detection to speak through graphs, self-supervision, datasets, explainability, and IoT constraints, the article preserves disciplinary integrity. Only then does it articulate shared themes.

The tenth methodological step was citation discipline. Every major technical or interpretive claim is supported with in-text citations in author-year format, as requested. This includes claims about material sustainability, durability, attack detection, graph-based methods, explainability, and transfer robustness. In long-form sections, citations are distributed throughout the argument rather than clustered only at the end, in order to preserve traceability between claim and source.

Overall, the methodological orientation of this article is best described as cross-domain analytical synthesis. It is not a bibliometric review, not a meta-analysis, and not an opinion essay. It is a structured research narrative that interprets two specialized literatures through a common conceptual framework while remaining strictly grounded in the supplied references. This method is appropriate because the article's contribution lies not in producing new laboratory data, but in generating a richer understanding of resilience across material and cyber infrastructures.

RESULTS

The integrative analysis produced a set of findings that clarify how sustainable advanced cementitious materials and intelligent intrusion detection systems each contribute to infrastructure resilience, and how their underlying design philosophies converge despite disciplinary distance.

A first major finding is that self-compacting and related advanced concrete systems are increasingly designed as multi-objective materials rather than simple strength-oriented composites. The references consistently show that modern concrete research no longer treats compressive performance as the sole or even dominant criterion of excellence. Instead, flow behavior, self-consolidation, durability, thermal stability, sustainability, and additive compatibility are all central design concerns (Memon et al., 2018; Abbas et al., 2022; Saand et al., 2019; Gheidan et al., 2025). This indicates that advanced cementitious systems are being engineered as balanced performance platforms. The significance of this finding lies in its departure from conventional material hierarchies. A material may be strong yet operationally inadequate if it segregates, fails under thermal exposure, or imposes excessive environmental cost. Thus, resilience in concrete is revealed as a composite property emerging from multiple interdependent behaviors.

A second finding is that sustainable substitution materials are no longer peripheral modifiers but central drivers of innovation in self-compacting and specialized cementitious systems. Abbas et al. (2022) explicitly address low-cost self-consolidation concrete using sustainable material, while Altwair et al. (2025) evaluate Libyan iron slag in self-compacting concrete. Awang and Aljoumaily (2017) analyze granulated blast

furnace slag in foam concrete, Majeed et al. (2023) investigate glass waste in reactive powder concrete, and Saand et al. (2019) examine metakaolin derived from local material. Together, these studies indicate that sustainability-oriented substitutions are not being explored merely for environmental image. They are being treated as technically serious constituents capable of reshaping fresh and hardened behavior. This suggests that future concrete development will likely be defined less by uniform use of traditional materials and more by locally adapted, performance-conscious incorporation of alternative resources.

A third finding is that modifier behavior is highly context-dependent, meaning that no additive can be presumed beneficial across all cementitious systems and exposure conditions. This is evident in the diversity of the literature itself. Iron slag, blast furnace slag, metakaolin, basalt fiber, polymeric fibers, glass waste, magnetized water, and nanotechnology are all studied as distinct interventions, each with its own target mechanisms and performance expectations (Abbas et al., 2022; Al-Mulla & Al-Rihimy, 2025; Altwair et al., 2025; Awang & Aljoumaily, 2017; Majeed et al., 2023; Ozodabas, 2018; Salman & Al-Mulali, 2025; Saand et al., 2019). The implication is that advanced concrete design is fundamentally parametric and contextual. Materials must be selected in relation to intended behavior, not by generalized reputation alone. This is an important systems-level result, because it shows that resilience depends on fit between intervention and environment.

A fourth finding concerns durability as a defining criterion of resilient concrete systems. Al-Obaidy (2017) addresses internal sulfate attack in self-compacted concrete, Benjeddou et al. (2022) investigate high-temperature effects on self-compacting concrete properties, and Gheidan et al. (2025) review thermal and mechanical properties in fiber-reinforced and pozzolanic self-compacting concrete systems. These studies collectively indicate that modern material performance must be interpreted under stress, not only under standard ambient conditions. The material question is no longer simply whether concrete reaches a target property in ideal conditions, but whether it maintains sufficient integrity when exposed to chemically aggressive or thermally severe environments. This broadens the meaning of concrete quality from nominal laboratory adequacy to functional persistence under hazard.

A fifth finding is that interfacial and microstructural tuning plays a central role in advanced concrete performance. The effect of hydrophilic and hydrophobic polymeric fibers in reactive powder concrete studied by Al-Mulla and Al-Rihimy (2025), and the influence of basalt fiber analyzed by Ozodabas (2018), show that performance is shaped not only by macro-level composition but by how modifiers interact with the matrix. Gheidan et al. (2025) reinforce this through their focus on fiber-reinforced systems. This means that resilience can be materially engineered through microstructural discipline. The implication is profound: advanced concrete systems are not merely mixtures of ingredients but architectures of interactions. Material reliability emerges from the way components coexist and transmit stresses, retain cohesion, and respond to environmental disturbance.

A sixth finding is that certain studies in the concrete cluster reflect a willingness to explore unconventional enhancement routes. Abbas et al. (2022) investigate magnetized water in concrete strength development, while Salman and Al-Mulali (2025) examine nanotechnology in sustainable foam concrete. Regardless of how widely such methods are eventually adopted, their presence in the literature indicates a field that is actively experimenting beyond established binder-replacement paradigms. This reveals a research culture seeking performance advantages through novel physico-chemical pathways. The practical meaning of this finding is that concrete science is in an exploratory phase where resilience is increasingly pursued through hybrid and nontraditional interventions.

The intrusion detection literature yields equally clear findings. A seventh major finding is that IoT intrusion detection has moved decisively beyond conventional static classification toward adaptive, architecture-sensitive intelligence. Earlier or more classical approaches such as fuzzy SVM, SVM with feature embedding, and general machine learning-based DDoS classification remain important foundations (Sheng & Zhigang, 2018; Gu & Lu, 2021; Gaur & Kumar, 2022; Ismail et al., 2022). However, the field now prominently includes deep learning, supervised sparse autoencoders, graph neural networks, self-supervised learning, transformers, and robustness-preserving contrastive distillation (Ghorbani & Fakhrahmad, 2022; Lo et al., 2022; Deng et al., 2023; Duan et al., 2023; Nguyen & Kashef, 2023; Akuthota & Bhargava, 2025; Huang et al., 2025). This finding shows that intrusion detection is no longer understood as a fixed pattern recognition problem. It is increasingly treated as a dynamic learning problem in which architecture choice shapes the kinds of relational or temporal structure that can be recognized.

An eighth finding is that lightweight deployment remains a central requirement in IoT security research, even as model complexity rises. Jan et al. (2019) explicitly focus on lightweight intrusion detection for IoT, Sadhwani et al. (2023) propose a lightweight DDoS detection model, and Huan et al. (2024) target

lightweight deep learning for in-vehicle network intrusion detection. Even transformer-based and graph-based studies are often motivated by deployment in resource-constrained or real-time environments (Akuthota & Bhargava, 2025; Deng et al., 2023). This indicates that resilience in IoT security cannot be defined by detection accuracy alone. Computational economy, deployment feasibility, and speed are integral to practical robustness. A model that cannot operate within device or network constraints is infrastructurally weak, even if it is statistically strong in offline tests.

A ninth finding is that graph-based learning has emerged as one of the most conceptually powerful directions in intrusion detection research. Lo et al. (2022) introduce E-GraphSAGE for IoT intrusion detection, Chang and Branco (2021) extend graph-based solutions with residuals, Deng et al. (2023) use flow topology-based graph convolutional networks, Duan et al. (2023) apply dynamic line graph neural networks with semisupervised learning, and Hu et al. (2023) focus on graph embedding for early and accurate intrusion detection. These studies collectively indicate that network intrusion is increasingly understood as a relational phenomenon. Attack behavior is not always best represented by isolated features attached to independent packets or flows; it often resides in interaction structures, communication patterns, and evolving topologies. This is an important methodological shift because it redefines what counts as relevant information in security analytics.

A tenth finding is that feature selection and representation learning remain foundational even in advanced models. Borisov et al. (2019) propose CancelOut as a layer for feature selection in deep neural networks, Kamaldeep et al. (2023) emphasize feature engineering for DDoS detection in IoT, and Gu and Lu (2021) combine SVM with naïve Bayes feature embedding. The implication is that architectural sophistication does not eliminate the importance of informative representation. On the contrary, better models often make feature or representation choices more consequential. This mirrors the concrete domain, where sophisticated material systems still depend on the quality and compatibility of their constituent components.

An eleventh finding is that explainability and trust are emerging as nonoptional dimensions of effective intrusion detection. Mahbooba et al. (2021) explicitly connect explainable artificial intelligence to trust management in intrusion detection systems. This is significant because cybersecurity decisions often have operational consequences, including false alarms, traffic blocking, forensic escalation, or automated response. A system that performs well but cannot be interpreted may face adoption barriers in real environments. Thus, resilience in cybersecurity involves social-operational legitimacy as well as technical detection capability. This marks a mature phase in the field, where model acceptance becomes part of model quality.

A twelfth finding is that robustness and transferability are increasingly central concerns in network intrusion detection. Nguyen and Kashef (2023) employ traffic-aware self-supervised learning, while Huang et al. (2025) propose robustness-preserving transfer learning via contrastive adversarial representation distillation. These studies suggest that modern IDS research is beginning to address one of the field's most serious limitations: high performance within one dataset or environment does not guarantee reliable behavior under distribution shift, limited labels, or evolving attacks. This is closely analogous to the concrete durability problem. Just as a concrete mix that performs under one exposure condition may fail under sulfate attack or high temperature, an IDS that performs on one benchmark may degrade in a new environment. The shared lesson is that resilience must include generalization beyond the immediate training or testing regime.

A thirteenth finding is that application-specific intrusion detection is becoming a major direction of research. Huan et al. (2024) target in-vehicle networks, Sadia et al. (2024) address wireless sensor networks, and Koroniotis et al. (2020) discuss cybersecurity and reliability in smart airports. Koroniotis et al. (2018, 2020) also contribute network forensics perspectives specific to IoT and botnet activities. This indicates that the field increasingly recognizes that attack detection is domain-shaped. Different network types have different timing behavior, traffic semantics, feature distributions, and acceptable latency budgets. A universal detector is therefore less plausible than a family of detectors informed by shared methods but adapted to environment-specific constraints.

A fourteenth finding is that benchmark datasets and evaluation infrastructure have become strategically important research assets. Neto et al. (2023) introduce CICIoT2023 as a real-time dataset and benchmark for large-scale attacks in IoT environments. The importance of this result is methodological and epistemic. It shows that progress in intrusion detection depends not only on model architecture but on the quality, realism, and scale of data used for comparison. Without meaningful benchmarks, claimed improvements risk being ungrounded or incomparable. This finding has a parallel in concrete research, where performance conclusions are similarly dependent on

testing conditions and exposure frameworks, even if the reference list does not explicitly center standardized datasets in the same way.

A fifteenth and most integrative finding is that both literatures define resilience as a structured balancing act among competing demands. In concrete, high flowability must coexist with stability, sustainability must coexist with acceptable performance, and modifier use must coexist with durability under thermal or chemical exposure (Abbas et al., 2022; Altwair et al., 2025; Benjeddou et al., 2022; Gheidan et al., 2025). In intrusion detection, accuracy must coexist with lightweight deployment, advanced representation with interpretability, and model expressiveness with transfer robustness (Jan et al., 2019; Mahbooba et al., 2021; Akuthota & Bhargava, 2025; Huang et al., 2025). This shared balancing logic is arguably the article's most important result. It shows that resilience is not an additive property attached after design. It is the outcome of disciplined compromise within design.

A sixteenth finding is that the role of modifiers in concrete is conceptually analogous to the role of architectural augmentations in intrusion detection. Fibers, slags, metakaolin, magnetized water, and nanotechnology alter the performance landscape of cementitious systems by introducing specific behaviors or correcting deficiencies (Al-Mulla & Al-Rihimy, 2025; Altwair et al., 2025; Salman & Al-Mulali, 2025). In intrusion detection, feature selection layers, graph embeddings, transformers, and self-supervised objectives play a similar structural role: they reshape how information moves through the system and how the model captures relevant behavior (Borisov et al., 2019; Lo et al., 2022; Nguyen & Kashef, 2023; Akuthota & Bhargava, 2025). This is not a superficial analogy. In both cases, auxiliary design elements become central to overall system behavior.

A final finding is that both fields are transitioning from isolated performance improvement toward comprehensive resilience engineering. The concrete literature increasingly considers fresh properties, mechanical properties, durability, sustainability, and environmental response together. The intrusion detection literature increasingly considers accuracy, attack diversity, data realism, explainability, resource constraints, and transfer robustness together. This indicates that both domains are maturing toward system-level thinking, where local optimization is insufficient without lifecycle or operational adequacy.

DISCUSSION

The findings presented above support a broader interpretation of both cementitious materials research and IoT intrusion detection as sciences of resilience. This interpretation is not merely rhetorical. It reveals a deep structural similarity in how both domains now think, experiment, and evaluate performance. Each field has moved away from narrow single-metric optimization and toward multi-dimensional design under constraints. Each field increasingly recognizes that systems fail not because one variable was imperfect, but because interacting variables were insufficiently coordinated. This insight is central to the present discussion.

The first point of discussion concerns the meaning of resilience itself. In everyday usage, resilience is often treated as synonymous with strength, durability, or recovery. The literature examined here shows that such simplification is inadequate. In self-compacting concrete, resilience is not reducible to compressive strength alone, because a concrete system that is strong but fails to self-compact, segregates under flow, or deteriorates rapidly under sulfate or thermal exposure is not operationally resilient (Al-Obaidy, 2017; Benjeddou et al., 2022; Memon et al., 2018). In intrusion detection, resilience is not reducible to high classification accuracy on a benchmark dataset, because a detector that is computationally impractical, uninterpretable, fragile under distribution shift, or unsuited to IoT traffic realities is equally limited (Jan et al., 2019; Mahbooba et al., 2021; Nguyen & Kashef, 2023; Huang et al., 2025). A more accurate definition, suggested by both literatures, is that resilience is the capacity of a system to maintain function through balanced adaptation to anticipated and unanticipated stressors.

This leads to a second discussion point: the centrality of constrained optimization. Modern engineering problems are almost never unconstrained. Concrete systems must be optimized under economic, environmental, rheological, thermal, and structural limits. IoT intrusion detection systems must be optimized under data scarcity, latency constraints, class imbalance, model transparency needs, and computational limits. The reason both fields have embraced increasingly sophisticated designs is not because complexity is fashionable, but because simple systems often cannot satisfy all relevant constraints simultaneously. For example, a concrete mix may require sustainable substitution to reduce environmental burden, but such substitution can alter fresh-state or durability behavior, requiring compensatory adjustments (Abbas et al., 2022; Altwair et al., 2025; Saand et al., 2019). Similarly, a deep learning model may improve detection power but exceed the computational capacity of lightweight IoT settings unless carefully redesigned (Jan et al., 2019; Sadhwani et al., 2023; Akuthota & Bhargava, 2025).

Thus, resilience is shaped not by freedom from constraint, but by intelligence within constraint.

A third important issue is the role of heterogeneity. Both material systems and network systems are heterogeneous by nature. Concrete is heterogeneous at multiple scales, from particles and pores to fibers and matrix interfaces. Network traffic in IoT environments is heterogeneous in protocol, device type, temporal behavior, and attack signature. This heterogeneity complicates generalized design. It also helps explain why modifier strategies and advanced representations have become so important. In concrete, fibers, slags, and specialized additives are used to manage or exploit heterogeneous behavior within the composite (Al-Mulla & Al-Rihimy, 2025; Awang & Aljoumaily, 2017; Ozodabas, 2018). In intrusion detection, graph embeddings, transformers, and self-supervised structures are used to represent heterogeneity in traffic and relational dynamics more effectively than flat feature sets alone (Lo et al., 2022; Deng et al., 2023; Akuthota & Bhargava, 2025). A key implication is that engineering resilience increasingly depends on representational adequacy: whether a material formulation or model architecture is capable of capturing the real complexity of the system it governs.

The sustainability discussion is especially revealing when compared across domains. In concrete engineering, sustainability is materially explicit. It means reducing cost and environmental load through sustainable materials, waste reuse, slag substitution, metakaolin incorporation, and other alternatives to conventional mix regimes (Abbas et al., 2022; Altwair et al., 2025; Awang & Aljoumaily, 2017; Majeed et al., 2023; Saand et al., 2019). In cybersecurity, sustainability takes a less visible but equally important form: model efficiency, lightweight deployment, distributed detection, and reduced dependence on expensive labeling or centralized computation (Jan et al., 2019; Nguyen & Kashef, 2023; Alrayes et al., 2024). This difference invites a broader theoretical observation. Sustainability is not a single universal metric across engineering fields. It is the discipline-specific reduction of unnecessary burden while preserving function. In material systems that burden may be carbon, cost, or raw resource use. In computational systems it may be latency, energy, memory, or annotation cost. Recognizing this prevents narrow definitions of sustainable engineering.

Another major discussion point concerns the move from local performance to lifecycle thinking. The concrete studies on sulfate attack and high-temperature effects make it clear that initial material adequacy is not sufficient. A mix may appear successful in early mechanical terms yet prove weak under prolonged chemical or thermal exposure (Al-Obaidy, 2017; Benjeddou et al., 2022; Gheidan et al., 2025). Similarly, intrusion detection models that perform well in a particular training or validation setting may fail under changing traffic patterns, new attack variants, or different labeling conditions (Nguyen & Kashef, 2023; Huang et al., 2025). What both domains reveal is that resilience must be temporal. It must account for how performance evolves, degrades, transfers, or survives under changing conditions. This point is especially important because many engineering cultures remain overly focused on point performance rather than lifecycle adequacy.

The literature also suggests that auxiliary modifications are often decisive, not secondary. In traditional thinking, one might imagine that concrete is mostly about cement, aggregates, and water, while modifiers merely fine-tune results. Likewise, one might imagine that intrusion detection is mostly about choosing a classifier, while embeddings or explainability are optional extras. The present analysis suggests a different interpretation. In advanced systems, the so-called auxiliary elements often determine whether the core system succeeds at all. Fibers alter matrix behavior fundamentally. Slag and metakaolin can redefine fresh-state and hardened performance. Graph structure can reveal information inaccessible to flat features. Feature selection layers can prevent high-capacity models from overfitting noise (Borisov et al., 2019; Deng et al., 2023; Al-Mulla & Al-Rihimy, 2025; Saand et al., 2019). This implies that engineering maturity increasingly lies in understanding second-order influences as first-order design elements.

There is also a significant epistemological shift visible in both domains: trust in purely heuristic expertise is giving way to structured evidence-guided complexity. Concrete technology historically contained a strong empirical tradition of proportioning and performance intuition. Cybersecurity likewise long depended on handcrafted rules and signature-based thinking. The contemporary references show more formalized experimentation and modeling. Concrete studies examine well-defined interventions and stress conditions. Cybersecurity studies systematically evaluate graph-based, transformer-based, and self-supervised methods on emerging datasets and attack categories (Benjeddou et al., 2022; Ghorbani & Fakhrahmad, 2022; Neto et al., 2023; Huang et al., 2025). Yet the shift is not from human judgment to automation alone. Rather, it is from understructured intuition to evidence-disciplined adaptive design.

The issue of explainability deserves deeper attention, particularly because it marks a useful difference

between the two domains. In cybersecurity, explainability is explicitly foregrounded through work such as Mahbooba et al. (2021). This reflects the operational need to justify alerts, maintain analyst trust, and support intervention decisions. In concrete science, explainability is less often named, but it exists in another form: mechanistic interpretability. Researchers want to know why slag, fibers, metakaolin, or thermal exposure affect properties in a certain way. The language differs, but the epistemic concern is similar. Both fields seek models and designs that are not merely effective, but intelligible enough to guide engineering action. The implication is that explainability should perhaps be understood more broadly across engineering, encompassing both algorithmic trust and material mechanism clarity.

The graph-based intrusion detection literature also opens an especially rich conceptual parallel with composite concrete behavior. Graph models treat network events as relational entities embedded in topology, not isolated points. Composite concrete similarly behaves as a network of interactions among particles, pores, interfaces, fibers, and microstructural zones, even if the literature here does not explicitly model it as a graph. This analogy should not be overextended, but it is conceptually helpful. Both domains show that system behavior often emerges from relational organization rather than solely from local attributes. A packet or flow is not fully understood outside its network relations; a fiber or waste additive is not fully understood outside its matrix interactions. This suggests that relational thinking may be one of the most important shared patterns across modern engineering sciences.

There are, of course, limits to the comparison made in this article. Concrete and intrusion detection are not interchangeable problem spaces, and care must be taken not to flatten one into a metaphor for the other. Concrete systems obey material and thermochemical laws; intrusion detection systems operate through data, computation, and adversarial behavior. Performance metrics differ, deployment conditions differ, and failure consequences differ. The article does not claim a formal equivalence of domains. Its argument is more modest and more defensible: these fields have converged toward analogous design logics. Both now operate as resilience-focused engineering disciplines that optimize for reliability under interacting constraints.

A second limitation concerns the reference set itself. The concrete literature supplied is strong on self-compacting and related advanced materials, but it does not include broader lifecycle assessment or extensive field performance studies. The intrusion detection literature is strong on modern methods, especially graph and deep learning directions, but does not exhaustively cover deployment economics or post-deployment governance. As a result, the article's conclusions are strongest at the level of technical design philosophy and weaker at the level of long-term field implementation. This is not a flaw in the article's reasoning so much as a reflection of the evidence base provided.

A third limitation is that some references are reviews or preprints, especially in the cybersecurity cluster, while others are experimental studies. This introduces uneven evidentiary granularity. However, this diversity also reflects the actual research ecosystems of the two domains. The rapid pace of cybersecurity often produces important preprint-stage conceptual contributions, whereas concrete research may move more heavily through experimental article pathways. The article has accounted for this by using preprints cautiously and relying on convergence rather than on isolated claims.

Future research opportunities emerge clearly from this cross-domain reading. In the concrete domain, more work is needed on the combined behavior of sustainable substitutions under coupled stressors rather than under single exposure modes. For example, mixes incorporating waste or slag materials could be studied not only for fresh and hardened properties, but for durability under interacting chemical and thermal conditions. Fiber behavior under such coupled exposures also warrants deeper study, especially where hydrophilic and hydrophobic interactions or interface effects may become decisive (Al-Mulla & Al-Rihimy, 2025; Gheidan et al., 2025). Emerging modifiers such as magnetized water or nanotechnology-enhanced components should also be evaluated over longer performance horizons rather than only through short-term property gains (Abbas et al., 2022; Salman & Al-Mulali, 2025).

In intrusion detection, future work should continue moving toward robustness under deployment variability. Self-supervised learning, transfer learning, and contrastive distillation are especially promising because they address generalization, limited labels, and attack evolution (Nguyen & Kashef, 2023; Huang et al., 2025). Graph-based methods also merit continued development, particularly where dynamic topology and limited annotation intersect (Duan et al., 2023; Deng et al., 2023). Explainability research should likewise expand beyond trust rhetoric toward operationally meaningful explanations that help human analysts act more effectively (Mahbooba et al., 2021). More application-specific work in domains such as smart mobility, industrial IoT, and public infrastructure would

also strengthen the field's practical impact (Huan et al., 2024; Koroniotis et al., 2020).

An especially important interdisciplinary future direction would be the study of resilience governance across physical and digital infrastructure. Although this article has not introduced external smart infrastructure references, its findings imply that future built environments will require coordinated thinking about materials, sensing, digital defense, and lifecycle management. Concrete systems may become increasingly embedded in monitored environments, while digital systems remain dependent on reliable physical substrates. Research that bridges these infrastructures conceptually and operationally could become highly valuable.

The most important theoretical contribution of this article is therefore the proposal that resilience engineering should be treated as a broad intellectual category spanning materials and algorithms alike. This does not dissolve disciplinary expertise. It strengthens it by placing specialized work within a larger pattern. Self-compacting concrete research and IoT intrusion detection research, though different in object and method, are both trying to answer the same fundamental question: how can we design systems that continue to perform when the world is variable, constrained, and adversarial? That is the question of resilient infrastructure in its fullest modern form.

CONCLUSION

This article has developed an original, publication-ready analytical synthesis of two distinct but conceptually aligned research domains: sustainable advanced cementitious composites, especially self-compacting and related concrete systems, and intelligent intrusion detection for IoT and cyber-physical environments. Based strictly on the references provided, the study has shown that these domains can be meaningfully interpreted through a common framework of resilience engineering.

The concrete literature demonstrates that modern cementitious materials are no longer designed solely for nominal strength. They are optimized through complex balancing among workability, self-compaction, durability, sustainability, thermal resistance, fiber interaction, and resource-efficient substitution. Slag, metakaolin, glass waste, polymeric fibers, basalt fibers, magnetized water, and nanotechnology-related interventions all illustrate a field seeking reliable performance through carefully structured material adaptation (Abbas et al., 2022; Al-Mulla & Al-Rihimy, 2025; Altwair et al., 2025; Awang & Aljoumaily, 2017; Benjeddou et al., 2022; Majeed et al., 2023; Ozodabas, 2018; Salman & Al-Mulali, 2025; Saand et al., 2019).

The intrusion detection literature likewise shows a field that has advanced beyond static classification toward adaptive, context-sensitive, and increasingly robust intelligence. Traditional machine learning remains relevant, but the strongest contemporary developments lie in graph neural networks, self-supervised learning, transformer-based detection, explainable AI, robustness-preserving transfer learning, and benchmark-driven evaluation for complex IoT environments (Akuthota & Bhargava, 2025; Deng et al., 2023; Duan et al., 2023; Hu et al., 2023; Mahbooba et al., 2021; Nguyen & Kashef, 2023; Huang et al., 2025; Neto et al., 2023). These methods reveal that digital resilience depends on representation quality, model efficiency, interpretability, and generalization capacity.

The central conclusion of the article is that both domains define resilience as an outcome of disciplined balance. In concrete systems, resilience emerges when sustainable substitutions, fresh-state behavior, structural adequacy, and durability under hazard are successfully aligned. In intrusion detection systems, resilience emerges when detection power, computational feasibility, trustworthiness, and robustness to evolving attack conditions are simultaneously managed. In both cases, resilience is not a single property attached to an otherwise finished system. It is the result of integrated design under interacting constraints.

This comparison also leads to a broader conclusion about infrastructure itself. Modern infrastructure is both physical and digital, and its reliability depends on advances in both material science and intelligent defense. Sustainable concrete enables durable built environments. Intelligent intrusion detection protects the data-rich and networked systems increasingly embedded within those environments. For this reason, future engineering practice may benefit from greater conceptual dialogue across these domains, even when technical methods remain distinct.

In summary, the literature supplied here supports a strong and coherent argument: sustainable self-compacting and advanced concrete systems and intelligent IoT intrusion detection systems are parallel expressions of a wider resilience paradigm in engineering. Each field seeks dependable operation under stress, uncertainty, and constraint. Each field increasingly relies on adaptive structures, auxiliary modifiers, and context-aware evaluation. Each field has moved beyond narrow optimization toward systems thinking. Recognizing this shared trajectory offers a richer intellectual foundation for future research on resilient infrastructure in both its material and digital

forms.

REFERENCES

1. Abbas, Z. K., Abbood, A. A., & Mahmood, R. S. (2022). Producing low-cost self-consolidation concrete using sustainable material. Open Engineering, 12(1), 850–858. https://doi.org/10.1515/eng-2022-0368
2. Abbas, Z. K., Al-Baghdadi, H. A., & Ibrahim, E. M. (2022). Concrete strength development by using magnetized water in normal and self-compacted concrete. Journal of the Mechanical Behavior of Materials, 31(1), 564–572. https://doi.org/10.1515/jmbm-2022-0060
3. Akuthota, U. C., & Bhargava, L. (2025). Transformer-based intrusion detection for IoT networks. IEEE Internet of Things Journal, 12(5), 6062–6067. https://doi.org/10.1109/JIOT.2025.3525494
4. Al-Mulla, I. F., & Al-Rihimy, A. S. (2025). The effect of the hydrophilic and hydrophobic behavior of polymeric fibers on some properties of reactive powder concrete. Engineering, Technology & Applied Science Research, 15(2), 21691–21694. https://doi.org/10.48084/etasr.10157
5. Al-Obaidy, H. K. A. (2017). Influence of internal sulfate attack on some properties of self compacted concrete. Journal of Engineering, 23(5), 27–46. https://doi.org/10.31026/j.eng.2017.05.03
6. Alrayes, F. S., Nemri, N., Aljaffan, N., Alshuhail, A., Alhashmi, A. A., & Mahmud, A. (2024). Distributed multiclass cyberattack detection using Golden Jackal optimization with deep learning model for securing IoT networks. IEEE Access, 12, 132434–132443. https://doi.org/10.1109/ACCESS.2024.3443202
7. Altwair, N. M., Abuzgaia, A. G., Alsharif, A. M., Sryh, L. S., Abdulsalam, S. E. A., & Swalem, K. A. (2025). Assessing the effects of Libyan iron slag on self-compacting concrete characteristics. Engineering, Technology & Applied Science Research, 15(1), 19589–19595. https://doi.org/10.48084/etasr.9337
8. Awang, H., & Aljoumaily, Z. S. (2017). Influence of granulated blast furnace slag on mechanical properties of foam concrete. Cogent Engineering, 4(1), Article 1409853. https://doi.org/10.1080/23311916.2017.1409853
9. Benjeddou, O., Katman, H. Y., Jedidi, M., & Mashaan, N. (2022). Experimental investigation of the high temperatures effects on self-compacting concrete properties. Buildings, 12(6), Article 729. https://doi.org/10.3390/buildings12060729
10. Binbusayyis, A. (2025). Innovative defense: Deep learning-powered intrusion detection for IoT networks. IEEE Access, 13, 31105–31120. https://doi.org/10.1109/ACCESS.2025.3542275
11. Borisov, V., Haug, J., & Kasneci, G. (2019). CancelOut: A layer for feature selection in deep neural networks. In Artificial Neural Networks and Machine Learning – ICANN 2019: Deep Learning (pp. 72–83). https://doi.org/10.1007/978-3-030-30484-3_6
12. Chang, L., & Branco, P. (2021). Graph-based solutions with residuals for intrusion detection: The modified E-GraphSAGE and E-ResGAT algorithms. arXiv.
13. Deng, X., Zhu, J., Pei, X., Zhang, L., Ling, Z., & Xue, K. (2023). Flow topology-based graph convolutional network for intrusion detection in label-limited IoT networks. IEEE Transactions on Network and Service Management, 20(1), 684–696. https://doi.org/10.1109/TNSM.2022.3213807
14. Duan, G., Lv, H., Wang, H., & Feng, G. (2023). Application of a dynamic line graph neural network for intrusion detection with semisupervised learning. IEEE Transactions on Information Forensics and Security, 18, 699–714. https://doi.org/10.1109/TIFS.2022.3228493
15. Gaur, V., & Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering, 47(2), 1353–1374. https://doi.org/10.1007/s13369-021-05947-3
16. Gheidan, E., Ab. Kadir, M. A., & Aluko, O. G. (2025). A thorough review of thermal and mechanical properties of fiber-reinforced ordinary Portland cement-SCC and pozzolanic-SCC. Journal of Structural Fire Engineering, 16(2), 268–290. https://doi.org/10.1108/JSFE-08-2024-0031
17. Ghorbani, A., & Fakhrahmad, S. M. (2022). A deep learning approach to network intrusion detection using a proposed supervised sparse auto-encoder and SVM. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 46(3), 829–846. https://doi.org/10.1007/s40998-022-00498-1
18. Gu, J., & Lu, S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding. Computers & Security, 103, Article 102158. https://doi.org/10.1016/j.cose.2020.102158
19. Hu, X., Gao, W., Cheng, G., Li, R., Zhou, Y., & Wu, H. (2023). Toward early and accurate network intrusion detection using graph embedding. IEEE

Transactions on Information Forensics and Security, 18, 5817–5831. https://doi.org/10.1109/TIFS.2023.3318960

20. Huan, S., et al. (2024). T-shaped CAN feature integration with lightweight deep learning model for in-vehicle network intrusion detection. IEEE Transactions on Intelligent Transportation Systems, 25(12), 21183–21196. https://doi.org/10.1109/TITS.2024.3478371

21. Huang, M., Lin, Y., Li, N., Chen, X., & Bertino, E. (2025). CARD: Robustness-preserving transfer learning for network intrusion detection via contrastive adversarial representation distillation. IEEE Transactions on Dependable and Secure Computing, 22(5), 5134–5151. https://doi.org/10.1109/TDSC.2025.3562600

22. Ismail, et al. (2022). A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access, 10, 21443–21454. https://doi.org/10.1109/ACCESS.2022.3152577

23. Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a lightweight intrusion detection system for the Internet of Things. IEEE Access, 7, 42450–42471. https://doi.org/10.1109/ACCESS.2019.2907965

24. Kamaldeep, Malik, M., & Dutta, M. (2023). Feature engineering and machine learning framework for DDoS attack detection in the standardized Internet of Things. IEEE Internet of Things Journal, 10(10), 8658–8669. https://doi.org/10.1109/JIOT.2023.3245153

25. Koroniotis, N., & Moustafa, N. (2020). Enhancing network forensics with particle swarm and deep learning: The particle deep framework. arXiv. https://doi.org/10.5121/csit.2020.100304

26. Koroniotis, N., Moustafa, N., & Sitnikova, E. (2020). A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems, 110, 91–106. https://doi.org/10.1016/j.future.2020.03.042

27. Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2018). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In J. Hu, I. Khalil, Z. Tari, & S. Wen (Eds.), Mobile Networks and Management (Vol. 235, pp. 30–44). Springer International Publishing. https://doi.org/10.1007/978-3-319-90775-8_3

28. Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access, 8, 209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728

29. Lo, W. W., Layeghy, S., Sarhan, M., Gallagher, M., & Portmann, M. (2022). E-GraphSAGE: A graph neural network based intrusion detection system for IoT. In NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium (pp. 1–9). https://doi.org/10.1109/NOMS54207.2022.9789878

30. Mahbooba, B., Timilsina, M., Sahal, R., & Serrano, M. (2021). Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. Complexity, 2021(1), Article 6634811. https://doi.org/10.1155/2021/6634811

31. Majeed, W. Z., Aboud, R. K., Naji, N. B., & Mohammed, S. D. (2023). Investigation of the impact of glass waste in reactive powder concrete on attenuation properties for bremsstrahlung ray. East European Journal of Physics, (1), 102–108. https://doi.org/10.26565/2312-4334-2023-1-12

32. Memon, N. A., Memon, M. A., Lakho, N. A., Memon, F. A., Keerio, M. A., & Memon, A. N. (2018). A review on self compacting concrete with cementitious materials and fibers. Engineering, Technology & Applied Science Research, 8(3), 2969–2974. https://doi.org/10.48084/etasr.2006

33. Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., & Ghorbani, A. A. (2023). CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors, 23(13), Article 5941. https://doi.org/10.3390/s23135941

34. Nguyen, H., & Kashef, R. (2023). TS-IDS: Traffic-aware self-supervised learning for IoT network intrusion detection. Knowledge-Based Systems, 279, Article 110966. https://doi.org/10.1016/j.knosys.2023.110966

35. Ozodabas, A. (2018). Investigation of the effect of basalt fiber on self-compacting concrete. International Journal of Research - GRANTHAALAYAH, 6(12), 38–45. https://doi.org/10.29121/granthaalayah.v6.i12.2018.1075

36. Saand, A., Jamali, K. A., Keerio, M. A., Ali, T., & Bhatti, N. (2019). Effect of metakaolin developed from local Soorh on fresh properties and compressive strength of self-compacted concrete. Engineering, Technology & Applied Science Research, 9(6), 4901–4904. https://doi.org/10.48084/etasr.3152

37. Sadia, H., et al. (2024). Intrusion detection system for wireless sensor networks: A machine learning

based approach. IEEE Access, 12, 52565–52582. https://doi.org/10.1109/ACCESS.2024.3380014

38. Sadhwani, S., Manibalan, B., Muthalagu, R., & Pawar, P. (2023). A lightweight model for DDoS attack detection using machine learning techniques. Applied Sciences, 13(17), Article 9937. https://doi.org/10.3390/app13179937

39. Salman, B. A., & Al-Mulali, M. Z. (2025). The effect of nano technology on the properties of sustainable foam concrete. Journal of Engineering, 31(6), 193–203. https://doi.org/10.31026/j.eng.2025.06.10

40. Sheng, W., & Zhigang, J. (2018). IDS classification algorithm based on fuzzy SVM models. Application Research of Computers, 37(2).