Scientific Research Publishing

International Journal of Communications, Network and System Sciences, 2026, 19(5), 79-89
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Processing, Component, and Network Architecture: A Review

Anthony Brian Mallgren

University of the District of Columbia, Washington, DC, USA
Email: anthony.mallgren@udc.edu

How to cite this paper: Mallgren, A.B. (2026) Processing, Component, and Network Architecture: A Review. *International Journal of Communications, Network and System Sciences*, **19**, 79-89.
https://doi.org/10.4236/ijcns.2026.195005

Received: April 21, 2026
Accepted: May 28, 2026
Published: May 31, 2026

Abstract

A presentative review of foundational concept and principle within a context of learning from past implementation, with aspect consideration for topic including hardware architecture, software methodology, ownership and management interest, economic, political, judicial, and societal. Based upon a proposal that savants were involved with initial innovation, which enabled exploitation of such technology in a way which eventually resulted in market congealment, an unnecessary production slow down, a primary concern may be a rearchitected solution factoring in all of these facets of implementation. While in theory, one may assume another would desire intrinsic market value, this seeming fallacy may present some difficulty in adjustment. Seems rather, some society has sunken into a slothful state and would rather not be burdened with a higher production expectation, aiming for passive income and imports, seemingly based upon what may be resource extraction and mild convenience. Premised upon development and resource management, a solution suggestion will follow herein, in an attempt to cure some prior evil.

Keywords

Computer, Architecture, Network, Culture, Society

1. Introduction

Being a solution may not exist in a complete vacuum in any known significant way, as such would at least introduce an observer paradox, it may be worthy considering a more holistic view of industry. Where implementation happens focusing on one aspect or another, exploitation by another discipline seemingly may become common. Therefore, a recommendation herein may advocate for, and hopefully practice, a multifaceted approach.

A paradigm, general method set, and initial hardware protocol in computer ar-

chitecture proposal may follow. It is noted, that in an attempt to ensure ethical employment of propertythat a non-commercial license was selected. The author would like, excluding that which may be referenced, modifying such license, releasing commercial license for any and all activity where government may be the direct and sole implementing recipient of any such property, with the reservation to reconsider.

Review Method

While some factor of system convenience and familiarity may be admitted, though, sources were selected with a primary regard to technical perspective, though seeing as how profiling may serve to mitigate potential unforeseen and yet considered issues, and enhance possible production, an individual and societal aspect was included as well. Where it may seem, technological implementation may enable activity of all sort, it may seem that all sort of activity may not be desirable by all, and where allowance, enablement, encouragement, and compel may serve society well, the primary interest of may be unfettered production.

2. Current State

While documented history does seemingly highlight at least a crude aspect of society, it seems American innovation has become especially troublesome. Fairly thorough research has been conducted into societal implications. While innovation was seemingly promoted by government [1], it seems odd that at least in America, they did not opt for a continued interest. Being government may hold a higher level of propriety in communication etiquette, one may only venture guessing why this may be. While historically, there has been some corruption occurrence, relative vulgar population, this has been relatively minimal, even given abounding resource utilization (e.g., federal and state budget). An idea which may propose government effectively disassociated with all technical infrastructure may be telling, being other critical infrastructure, e.g., road, construction, currency, et cetera, was primarily maintained by government. Why at least some European based and derived government diverged from a staked interest in development and manufacturing, an outsider may only guess.

Such government abandonment (a personal observation in American culture) seemingly shows in experience with technology. Though there has been some attempts to patch such activity [2] [3], cybercrime is a major activity in multiple nations [4]. Applications, such as social media, may possibly have adverse effect on people [5]. Frustration has also been reported [6] [7], as well as adverse emotional addition [8]. While one may assume that it may be innocent nativity, (though it seems that given a sufficient level of interest, that such driving dynamic may be scoped in targeting interest negation), based upon personal experience, human nature may speak otherwise. It was found that when pursuing foundational software development that hosting providers were not a reliable solution. Two American hosting providers, one a major corporation, another a startup, seemingly be-

came inaccessible during development; not temporarily, but persistence and long term. A United Kingdom provider had a similar result. Proceeding with foundation level research and development, account became locked, and notification received from provider instructing alternative activity and scaling down. An Austrian provider also became effectively unavailable, concluding that seemingly any given hosted solution may and do become vulnerable to attack when pursuing certain activity. What parties were involved, it is not certain, though one may assume, that at the least, infrastructure was negligently implemented, at least allowing for system malfunction. Taking into consideration that, given the state of the infrastructure, an intermediary, or perhaps providers, could have been implicated. It may be noted that malfunction seemed coincidental with critical momentum in development, though exactly what actor, if any, may have been involved. Perhaps relevant, providers were contacted, though each one was seemingly opinionated such that privacy was found of utmost regard.

Beyond hardware level, a dynamical assessment of origination and influence may be helpful in course correction. While siloed savant aspect has been covered, one may be benefited in familiarity with early dynamic. America, being an early innovator [9]., seemingly has a myriad of oddities which have presented some difficulty in implementation. First, newness of such a nation seemingly may create a sense of insecurity which may manifest as an over ascertain of pride [10], which may present numerous psychological issues, resulting in, up to and including, war [11]. First, feeling pressed for production, one may be hurried in delivery, which may cause increased error in a production process [12]. Having immature coping mechanism seemingly may cause exacerbation, and has resulted in attention being called to studying additional flexibility in copying [13]. When an error may be committed, a scapegoat seemingly may be sought after and exploited [14]. This, in turn, may lower community quality, and result in semiconscious cognitive dissonance, causing multiple individual perturbation, which in turn may manifest in almost every aspect of life (an effectual study covering more severe incident, Ubaldi M., & Picchio M., 2024 [15]).

The economic factors weigh in heavily as well. It seems that there may be a competition for resource appropriation [16]. Seemingly, all at once, speaking in terms of general population, people tend in favoring such an atmosphere, as evidenced by their information consumption tendency [17], even if it may cause additional hardship for oneself (discourse on some more severe dynamic had by LaGuardia-LoBianco A. W., 2019 [18]). Seemingly, a sort of intuitiveness may exist in people getting along better when prosecuting each other [19]; whether it be true for everyone, or not, may seemingly be irrelevant; it seems the course that is pursued in virtually all situational matter. How this may be incentivized may be noteworthy as well. Inherent quality, a type of economic value, placed upon each individual in society seemingly may bring about certain allowance against such a person, which may manifest in a variety of way and manner (a natural selection behavioral presentation by Jamieson I. G., 1986 [20]; a more general cite not readily found, though

alternative value scoped control methodology, e.g., finance [21], seem abounding in America academia).

Well known American stories considered compelling in development tell of intelligence agency ties and involvement (an example provided by Mulchandani N., *et al.*, 2022 [22]), seemingly applied to, and not for, general citizens, as well as application of the injurious incentivizing nature of American judiciary [23]. These factors seemingly set a foundation against, and not for, allowing and productively enabling, general American constitutionalized citizenship. Specific exploitation are varied, and many [24], and have brought about an entire insurance industry [25].

3. Analysis

3.1. Hardware

3.1.1. Layered Access

For such a purpose, layered access may signify an abstraction where original data, or a derivative, may be used in further derivative, whether or not the base may remain intact in any given data source.

1) Component

It seems that one of the primary issues existing today, (though other issues do exist; e.g., AlDosari F., 2017 [26]) is single function architecture, presenting an unnecessary risk. These are seemingly found in what may be considered the latest product of knowledge refinement [27]. A storage component is a storage component; a processor, no matter its internal component, is a processor; memory is memory, and so forth. This seems a peculiar implement, presenting unnecessary risk, seemingly leaving device access as a software level implement, which may create an issue where if access to a primary device may be obtained, being no hardware security mechanization, that the system, or component, may be compromised. Rather, observable interaction, isolated temporary states, and a tier formed of integration may present an improved approach. For example, a primary processor invokes a second processor, such execution may be logged, and audited, interacting with other devices. This may allow not only the hardware level component isolation, allowing for, and enforcing, a tiered execution approach, which may allow for evaluated execution and monitoring of instruction, but also may enable enhanced diagnostic analysis of system change, increasing system stability, and also providing critical diagnostic and recovery data at a hardware level, possibly deterring such behavior, promoting standardization, mitigating disaster, and increasing activity return speed. A similar approach may be applied to storage (one such security example explained, Rajeh W., 2022 [28]). Like processor isolation, in hardware level access mechanization, a tiered storage system, may be utilized safely without making the core, or tiered, system exploitatively vulnerable. This may allow for data to be stored in and accessed with hardware level harnessing, possibly preventing simple software data exploitation. This is already seen in public systems, such as libraries, where the entire patron tier is cleaned between each session, and seemingly may be ef-

fective.

2) Network

From a network perspective, multiple issues exist which could seemingly be readily resolved. First, it seems that there is a trust the next device, approach. This seemingly has not worked well (an attack example, explained by Shi S., Wang Y., Zou C. and Tian Y., 2022 [29]), for all that one may need to do is breach any single router to interfere with data, not only possibly compromising a network device, but given other vulnerability, any other system, including any vulnerable component. Expounding upon this, there may be no geographical nor path verification and validation processes. Triangulation (explained in mobile phone technology by Klimburg A., Faesen L., Verhagen P., & Mirtl P., 2020 [30]) has been readily used for quite some time now, but both the private and public sector has seemingly chosen to utilize this in selective prosecution (personal and shared community experience, though such consideration may become a moot point) rather than enabling a technology ecosystem with any sense of integrity. Major American mobile service operators were queries as to the reason for this, and if they would be willing to partake in hardening the infrastructure, but were unresponsive. A follow up with network equipment manufacturers also went without response. A noteworthy mention, where one may perform a function called a trace route, the route is seemingly dynamic, in that it can and does change, yet when an actual packet with a payload is routed, it is seemingly very difficult to ascertain the path that had been traversed, which may allow an attacker to remain somewhat unknown if and when a path may be traversed outside of a controlled network. The DDOS example above, may demonstrate how the availability of network connected systems may be compromised, putting a system, even a network, at risk. Recording path traversal may deter such behavior, and allow increased recovery efficiency and accountability reporting.

In summary, these issues may be resolved through implementing geographical triangulation, enabling the logging of payload packet routing, et cetera. Additional layering manifestation may be found in discovery and filtering mechanization.

3) Conclusion

It may be beneficial for electrical engineers to begin experimenting with such paradigm in conceptual discovering and production. Those with less resources may begin experimenting with lower cost boards, and begin implementing a driver based approach in such tactical implementation.

3.2. Software

It seems that some of the factors above, in part, have played into a strategy that is termed "building a moat", which has generally led to lengthy End User License Agreements. This has been heavily financially incentivized, as the concept of passive income is preached. In reality, what this usually results in is the perception that it is desirable to graduate from productive discipline, so one may be freed up to pursue other activities outside of virtue.

3.2.1. End User Empowerment

1) Code

Education may be an important aspect in utilizing technology. While some system theory may be covered, and some even venture into activity such as embedded development, given a general purpose device, it may result in a very low-quality experience. For example, as outlined above, frustration sets in. There seems to be an Icarus based paradigm, where one tries unsuccessful to maintain a path between two undesirable outcomes, in Greek mythology, due to hubris, where the software is just good enough to entice one into use, though seemingly comes with significant costs. A sense of congealment may be felt, in that one tries to take advantage of core hardware components, and finds them to be locked. Even given that one is able to unlock a system, it may be that, if any significant impact may result, a party of interest may be prosecuted. Using an operating system, there are multiple abstractions of convolution, usually under the guise that it may not be safe to allow hardware level access (of which, the architecture seems significantly influenced by the operating system developers). If one tries to make a contribution to the ecosystem, there are significant hurdles. It is usually that an app store has high barriers to entry, which, does not seem to be entirely merit based, but interest based. It seems if an application presents an interest conflict, that it is rejected. There may been widely publicized incidents in the news of operating system developers committing flagrant anticompetitive acts, for the entire world to see, and going without justified rebuke, correction, et cetera.

Given either government intervention (though, the rather low-quality official in government seem persuaded with relative ease, having seemingly declined into purely an opportunity to be bribed and catered to by industry elites, enabled by the identity conflicted voters looking to elect jesters into government as a faulty coping mechanism, a personal observation in American culture), or the production of more open access devices, an education in more foundational aspects of development may be beneficial. For example, bits in firmware, processor, memory, and disk, as well as pixels on a screen, and electrons over media, is relatively easy to understand and utilize. However, being abstracted into extremely convoluted ecosystems, with endless bugs, hiccups, security implications, et cetera, presents an almost endless pursuit of trying to figure out what is going on, so that some effect may be had. As a note, it seems that, given the production of some more open access devices, industry leaders tried to invest in sensationalizing the use of their product by further automating the use of their product, though the same Icarus paradigm has tried to be maintained, and some criticism has been heard that the automation is faulty in a lot of cases, presenting more trouble than solution while charging a premium for that additional trouble. The ill effects of data centers are also being debated [31].

Explorative research has been performed into the viability of adopting such paradigm. For example, a mechanism which utilized a network bootloader (U-Boot; currently available through https://docs.u-boot.org/en/v2025.01/build/source.html) to upload a device tree to a

custom TFTP server (example server used for testing currently may be access from https://github.com/abmallgren/System-Development/tree/main/RISC-V/server), which then attempted to upload the device tree into a public server, which would then be used to retrieve a custom kernel complete with foundational driver functionality was developed (since U-Boot currently reportedly requires a static IP address, and the author has not been able to find a suitable hosting service, this has not been well fleshed out). Therefore, it may be that in developing such solution, that existing infrastructure with an interest in maintaining the status quo may not be a viable solution (perhaps more development and production may be needed). Also noteworthy, it seems many that have been betrayingly exploited in the past have difficult making sense of what they have allowed and endorsed, and seemingly would rather try to press that upon the next series of entrants, rather than adopting a more productive life (personal experience in American culture), even if that means, as noted above, bringing continued and additional hardship among themself. These are seemingly presenting some difficulty in marketing, though if such effort may fail, it may seemingly be a market failure rather than a production failure, though, one may have to decide which culture they prefer.

2) Network Protocol and Functionality

The layering paradigm presented above may be utilized and expanded upon. In discovery, several principles have been founded. One, a layering approach seemed agreeable, where data may be layered upon data, and filtered. Several functionality were discovered. For example, a resource identifier, such as a Uniform Resource Locator, may be used. In testing, annotation was chained (e.g., business, social, cetera, commentary annotation available from https://youtu.be/H7xpH4JX6Nk, and content annotation available from https://youtu.be/zujs1jCvjIA), which could then be made public, private, and further scoped, and filtered upon (given any associated attribute). This is also recursive, *i.e.*, that the annotation may be assigned an identifier, and annotated upon. While this was researched in more of a content perspective, some functionality was also discovered. For example, script overriding, custom user interfacing through, further enabled by a data driven, and functionality abstraction, method, where an application may be presented as a data first, with default functionality, and presentation, could be override, either at the user end, or in abstraction from various sources.

3) Data Processing

Given data presented in such a way, some analysis of analysis was researched. Data sources, such as Wikimedia's multilingual "dumps" exist where one may seemingly establish a sufficient foundation for creating custom solution for world knowledge. Once such data source are processed in such a way that makes them operationally efficient, and cleaned (given the nature of the data, and their processing method, a large portion of the data may not be useful), additional data source may be utilized in increasing functionality, such as parts of speech taggers, and then processed, performing common association to establish symbolic morpheme relation. If sufficient momentum may be gained, additional data, such as

phonological, may be incorporated. Aggregates and step-down tables may be utilized in navigating data sets with full-fidelity, where both the breadth and depth of a data, as well as any abstraction and derivation, may be fully accounted for [32], which may allow for small and large modeling which may be applied and compared cross-dataset, eliminating biases and attributing accountable association with who is responsible, and may be credited, for data, clearing up some of the more contentious copyright issues in such a practice.

4) Artificial Intelligent

Another pattern discovered in such research was sensory evolution, where input from one or more sensing objects may be inducted in a conceptually novel way, with one such proposal, being based upon pseudo-randomization. Given a dataset, a certain degree of randomness may be introduced into data discovery, verification, and validation. For example, a method to generate an icon, index, or symbol, or for sake of example, given a dictionary, one could use a cryptographic library to pseudo randomly generate a letter. The letter could be used in a dictionary lookup. Then an array could be built of a next possible letter, which could be fed into the cryptographically random selector, and so forth until a word may be produced. This could be used to create a phrase based upon evolution. Another abstraction may take in account modeling. For example, if a noun were to be produced, a query of existing semantic structure may be built. For example, another noun could be produced in producing a congregate noun, or perhaps a verb instead. This may allow one to use an existing dataset, though variations could also be introduced. For example, a statistically method could be introduced on the probability that in introducing a new letter, or morpheme, may produce a viable new concept. Other languages may be inquired of, in such a process, or a less constrained method, so on and so forth. While such supplied example may target linguistic principle, similar may be applied in other sensory data, and even integrated.

3.2.2. Community

Community may be important as well. While government, in recent history, has been a public consumer of technology, an opportunity for integration may exist. For example, if government were involved in designing municipal grid, an inherent tax component could be implemented in productive transaction, automating an essentially passive, although adaptable, possible depending upon possibly legislative integration, revenue mechanism. Judicial proceeding could also be facilitated by facilitating evidentiary proceeding. Private, as has been the case recently, also may hold stake in such development.

4. Future Work

There are multiple research aspect which may be researched. While there still may exist highly invigorating and rewarding discipline of cutting edge and highly innovative research in physic, material, and other discipline, much fruit may be ready for a proverbial harvest in rearchitecting existing concept, finding new ap-

plication, employing ideation, optimizing, and finding further efficiencies within these core discipline. Hegel's thesis, antithesis, and synthesis may be applied once again.

4.1. Specificity

4.1.1. Electrical

The electronic component may be foundation, and a fairly dynamic conceptual discovery process. There are multiple assistive technology, including multiple traditional processor architecture, *i.e.*, static, although sometime multiple, processing width, both closed (e.g., x86,64, ARM, et cetera) and open (e.g., RISC-V), as well as more dynamic solution, such as Field Programmable Gate Array. These are fairly low cost and could serve useful.

4.1.2. Software

Based upon this foundation alone (though one may not wish limiting oneself), dynamic boot process, discovery, and integration may be fluid, flexible, and yielding activity. Coding has been a long held interest which, with conceptualization exploration in new interaction paradigm, may be renewed. Network interaction may seem an interesting workspace, with many people looking to control, refine, and integrate quality substance into their perception. Data analysis, building upon these more foundational principle, may be intriguing. And of course, artificial intelligence seemingly may present both wonder and much fanfare.

4.1.3. Community

Much work could be centered around empowerment, lobbying, policy, and orchestration, both public and private, as well an integration into infrastructure, supply chain, distribution, allocation, construction, and industry of every type.

5. Conclusion

It seems as though, after an analysis and assessment of current industry state, a tipping point may be achieved in industrial restructuring. While outspoken advocates of data synthesis based "generation" have expressed their vision of highly automated work forces, it seems that they are attempting to build upon a fault foundation, which may be readily exploited, in a society readily implicated, based upon vortex of confusion, psychological affliction, conflict, et cetera. While people volunteering for this lifestyle (though freewill debating may ensue) may be entitled to pursue such an experience, it seemingly does not have to be an experience for everyone. How ready a market be ready for adopting new principles may be the matter of another study, but ample opportunity for research, development, and production may already exist.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Haigh, T., Russell, A.L. and Dutton, W.H. (2015) Histories of the Internet: Introducing a Special Issue of Information & Culture. *Information & Culture*, **50**, 143-159. https://doi.org/10.1353/lac.2015.0006

[2] Chhabra, M., Gupta, B. and Almomani, A. (2013) A Novel Solution to Handle DDOS Attack in MANET. *Journal of Information Security*, **4**, 165-179. https://doi.org/10.4236/jis.2013.43019

[3] Nguyen, D.S.W. and Alrubie, D.F. (2025) Designing a Detection Model for SQL Injection Attack. *Journal of Computer and Communications*, **13**, 40-79. https://doi.org/10.4236/jcc.2025.138003

[4] Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. and Varese, F. (2024) Mapping the Global Geography of Cybercrime with the World Cybercrime Index. *PLOS ONE*, **19**, e0297312. https://doi.org/10.1371/journal.pone.0297312

[5] Davids, J. (2025) Social Media and Mental Health. In: Davids, J., Ed., *WIRED for Worry*: *How Smartphones and Social Media Are Harming Canadian Youth*, Macdonald-Laurier Institute, 8-14. http://www.jstor.org/stable/resrep69477.5

[6] Hertzum, M. and Hornbæk, K. (2023) Frustration: Still a Common User Experience. *ACM Transactions on Computer-Human Interaction*, **30**, Article No. 42. https://doi.org/10.1145/3582432

[7] Lazar, J., Jones, A., Hackley, M. and Shneiderman, B. (2006) Severity and Impact of Computer User Frustration: A Comparison of Student and Workplace Users. *Interacting with Computers*, **18**, 187-207. https://doi.org/10.1016/j.intcom.2005.06.001

[8] Salanova, M., Llorens, S. and Cifre, E. (2013) The Dark Side of Technologies: Technostress among Users of Information and Communication Technologies. *International Journal of Psychology*, **48**, 422-436. https://doi.org/10.1080/00207594.2012.680460

[9] LéCuyer, C. (2001) Making Silicon Valley: Engineering Culture, Innovation, and Industrial Growth, 1930-1970. *Enterprise and Society*, **2**, 666-672. https://doi.org/10.1093/es/2.4.666

[10] Brighouse, H. (2006) Justifying Patriotism. *Social Theory and Practice*, **32**, 547-558. https://doi.org/10.5840/soctheorpract200632427

[11] van Evera, S. (1994) Hypotheses on Nationalism and War. *International Security*, **18**, 5-39. https://doi.org/10.2307/2539176

[12] Kottage, B.E. (1992) STRESS in the Workplace. *Professional Safety*, **37**, 24-26. http://www.jstor.org/stable/45430468

[13] Bonanno, G.A. and Burton, C.L. (2013) Regulatory Flexibility: An Individual Differences Perspective on Coping and Emotion Regulation. *Perspectives on Psychological Science*, **8**, 591-612. https://doi.org/10.1177/1745691613504116

[14] Dorr, D. (2010) The Scapegoat. *The Furrow*, **61**, 92-97. http://www.jstor.org/stable/27808993

[15] Ubaldi, M. and Picchio, M. (2024) In the Wrong Place at the Wrong Time: The Impact of Mass Shooting Exposure on Mental Health. IZA-Institute of Labor Economics. http://www.jstor.org/stable/resrep69472

[16] Falus, K.S.M. (1974) On Economic Competition. *Acta Oeconomica*, **13**, 49-64. http://www.jstor.org/stable/40728317

[17] Moravec, P.L., Minas, R.K. and Dennis, A.R. (2019) Fake News on Social Media: People Believe What They Want to Believe When It Makes No Sense at All. *MIS Quar-*

terly, **43**, 1343-1360. https://doi.org/10.25300/misq/2019/15505

[18] LaGuardia-LoBianco, A.W. (2019) Self-Saboteurs and Ethical Relationships. *Social Theory and Practice*, **45**, 249-285. https://doi.org/10.5840/soctheorpract20197259

[19] Greenhouse, C.J. (2018) 10. Interpreting American Litigiousness. In: Starr, J. Collier, J.F., Eds., *History and Power in the Study of Law*: *New Directions in Legal Anthropology*, Cornell University Press, 252-274. https://doi.org/10.7591/9781501723322-013

[20] Jamieson, I.G. (1986) The Functional Approach to Behavior: Is It Useful? *The American Naturalist*, **127**, 195-208. https://doi.org/10.1086/284478

[21] Shiller, R.J. (2003) From Efficient Markets Theory to Behavioral Finance. *Journal of Economic Perspectives*, **17**, 83-104. https://doi.org/10.1257/089533003321164967

[22] Mulchandani, N. and Shanahan, J.N.T. (2022) About the Authors. In: Mulchandani, N. and Shanahan, J.N.T., Eds., *Software—Defined Warfare*: *Architecting the DOD's Transition to the Digital Age*, Center for Strategic and International Studies (CSIS), 21. http://www.jstor.org/stable/resrep43413.8

[23] Meyer, J. (1993) The New Lawyering: Microsoft's Bill Gates Looks at Computers' Impact. *ABA Journal*, **79**, 56-60. http://www.jstor.org/stable/27834922

[24] Harry, C.T. and Gallagher, N.W. (2019) An Effects-Centric Approach to Assessing Cybersecurity Risk. Center for International & Security Studies, U. Maryland. http://www.jstor.org/stable/resrep20424

[25] Price, J.S. and Wear, J.D. (2015) Claims Made and Insurance Coverage Available for Losses Arising Out of or Related to Electronic Data. *Tort Trial & Insurance Practice Law Journal*, **51**, 51-90. https://www.jstor.org/stable/26421273

[26] Al Dosari, F. (2017) Security and Privacy Challenges in Cyber-Physical Systems. *Journal of Information Security*, **8**, 285-295. https://doi.org/10.4236/jis.2017.84019

[27] Thomas, F., Arribas, E.G., Hetterich, L., Weber, D., Gerlach, L., Zhang, R., *et al.* (2025) RISCover: Automatic Discovery of User-Exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs. *Proceedings of the* 2025 *ACM SIGSAC Conference on Computer and Communications Security*, 13-17 October 2025, 3326-3340. https://doi.org/10.1145/3719027.3765141

[28] Rajeh, W. (2022) Hadoop Distributed File System Security Challenges and Examination of Unauthorized Access Issue. *Journal of Information Security*, **13**, 23-42. https://doi.org/10.4236/jis.2022.132002

[29] Shi, S., Wang, Y., Zou, C. and Tian, Y. (2022) AES RSA-SM2 Algorithm against Man-In-the-Middle Attack in IEC 60870-5-104 Protocol. *Journal of Computer and Communications*, **10**, 27-41. https://doi.org/10.4236/jcc.2022.101002

[30] Klimburg, A., Faesen, L., Verhagen, P. and Mirtl, P. (2020) Appendix B: Tracking through Technology. In: *Pandemic Mitigation in the Digital Age*: *Digital Epidemiological Measures to Combat the Coronavirus Pandemic*, Hague Centre for Strategic Studies, 26-31.

[31] Clemmer, S., Chavez, M., Dotson, S., Gignac, J., Sattler, S. and Shaver, L. (2026) Recommendations for Policymakers, Regulators, Utilities, and Big Tech Companies. In: Clemmer, S., *et al.*, Eds., *Data Center Power Play*: *How Clean Energy Can Meet Rising Electricity Demand While Delivering Climate and Health Benefits*, Union of Concerned Scientists, 20-23. http://www.jstor.org/stable/resrep78130.7

[32] Mallgren, A.B. (2026) Full-Fidelity Semantic Aggregation: Navigating Datasets. *Journal of Data Analysis and Information Processing*, **14**, 247-253. https://doi.org/10.4236/jdaip.2026.142012