FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 5, March, 2026, pp 170 – 9
DOI: https://doi.org/10.33003/fjs-2026-1005-4969

A SYSTEMATIC STUDY OF CYBERSECURITY MESH ARCHITECTURE

***[1]Suleman Idris Zubairu, [1,2]Rabiu Ibrahim Suleiman and [1]Aliyu Abdullahi**

[1]Department of Computer Science, Northwest University Kano State, Nigeria.
[2]Department of Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria.

*Corresponding authors' email: sulezubb@gmail.com

ABSTRACT

In recent times, technological advancements—spanning across decentralized devices, cloud platforms, widespread Internet of Things (IOT) ecosystems—have rendered traditional perimeter-centric defense systems insufficient, and this has drawn much attention. In response, Cybersecurity Mesh Architecture (CSMA) emerges as the essential framework for securing modern, distributed environments, by providing organizations with a strategic edge in protecting their digital transformation efforts. To better understand this trend, this study systematically reviews developments in CSMA researches, drawing insights from previous literatures. It examines the architecture's core components and practical implementations. Additionally, organizations benefit from increased operational efficiency through security automation, critical infrastructure and extended enterprise ecosystems. The study presents a conceptual model of CSMA and critically evaluates recent scholarly works that address its application, integration challenges (notably with legacy systems), and risk mitigation strategies. It highlights key unresolved issues and research challenges that need to be addressed to strengthen cyber security. Ultimately, this study examines CSMA's growing significance as a strategic solution in today's dynamic and challenging threat environment and its ability to transform cybersecurity practices in digitally evolving organizations. Findings indicate that the adoption of CSMA yields significant improvements in organizational security performance. Across multiple studies, CSMA is associated with enhanced threat detection capabilities, faster incident response times, and more consistent policy enforcement. Empirical evidence further demonstrates that when integrated with advanced techniques such as edge computing and adaptive policy mechanisms, CSMA contributes to higher detection accuracy, reduced response latency, and lower false-positive rates.

Keywords: Cybersecurity Mesh Architecture, Organizations, Security, Perimeter, Implementation, Challenges, Framework

INTRODUCTION

The origin of cybersecurity dates back to the 20th century, when early theoretical foundations were established by John von Neumann in the 1940s, followed by the creation of the first computer virus by Bob Thomas in the 1970s. These developments exposed vulnerabilities in emerging networked systems and underscored the need to protect digital assets (Infosec Institute, 2014; Matthews, 2022). Around the same period, the development of ARPANET —the backbone to the modern Internet—further accelerated the need for structured security mechanisms (DuPont & Fidler, 2016). Since then, cybersecurity has evolved from protecting isolated systems to securing complex, interconnected digital environments. This evolution has been driven by the rapid adoption of cloud computing, mobile technologies, and the Internet of Things (IoT), which have fundamentally transformed digital infrastructures. Traditional "castle-and-moat" security models, which relied on clearly defined network perimeters, have become increasingly inadequate in protecting distributed systems and hybrid work environments (Parast et al., 2022; Ju et al., 2024; Jianli et al., 2018). The growing frequency of ransom ware attacks, data breaches, and insider threats further exposed the limitations of these conventional approaches, necessitating more adaptive and decentralized security frameworks (Zheng et al., 2022).

In response to these challenges, cybersecurity paradigms began shifting toward identity-centric and distributed models. Advances in Identity and Access Management, such as XACML, enabled the decoupling of identity from network location, while the introduction of the Zero Trust model by John Kindervag reinforced the principle that no user or system should be inherently trusted (Munoz et al., 2008; Kotha, 2020; Ren et al., 2025). Additionally, emerging frameworks like Secure Access Service Edge (SASE) further emphasized the integration of cloud-delivered and decentralized security services (Gartner, 2025). These developments collectively laid the foundation for CSMA. Cybersecurity Mesh Architecture has emerged as a modern approach designed to address the complexities of distributed digital ecosystems. Defined as a unified framework of interoperable security tools and controls, CSMA enables the integration of modular, decentralized security solutions while maintaining consistent policy enforcement across environments (Gartner, 2025; Pallewatta and Babar, 2024).

Cybersecurity Mesh Topology

Cybersecurity Mesh Architecture lies on the foundation of Mesh Topology, a networking topology that allows the interconnection of every device with every other device thereby creating multiple paths for the transmission of data. It benefits from topologies that enhance resilience and distributed security. Star, Full mesh, partial mesh and hybrid topologies are closely associated to CSMA.

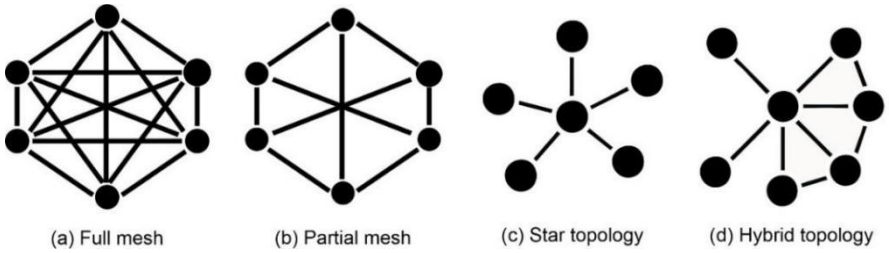

Figure 1: Illustration of Topologies That Are Closely Associated to CSMA (Kessler and Pritsky, 2009)

(a) While full mesh topologies offer maximum redundancy, they can be complex and costly. Multiple paths reduce single points of failure, so if one link/node is attacked or jammed, the network can quickly route around it. (b) Partial mesh: this type of mesh entails the connection of at least two or more devices over a network. As such, every node in the network may or may not be connected to all devices. (c) Star topology has all nodes connected to a central hub or switch. This topology is easy to install and manage, but if the central hub is compromised or attacked, there is a high chance of network disruption. (d) Hybrid topology combines two or more different topology types (e.g., star and mesh). It is flexible, scalable, and customizable, well-suited for complex and evolving networks, but more difficult to design and maintain. This topology has varied vulnerabilities, it inherits security pros and cons of its constituent topologies. For example, star components have a single point of failure, mesh components have more redundancy but more exposure (Kessler and Pritsky, 2009).

Star and Partial Mesh topologies are the more favourable for implementing cybersecurity mesh, providing a balance between redundancy, manageability and cost. Hybrid topologies are also widely used when they incorporate CSMA-relevant components (Reddy et al., 2024; Garcia et al, 2025).

Components of Perimeter-Based Security

In his book, Bishop (2004) provides a comprehensive coverage of cybersecurity, including detailed explanations of the five core components of perimeter-based security. These core 5 components include firewalls, intrusion detection systems, VPNs, access control mechanisms, and network segmentation. They are briefly summarized in the table below.

Table 1: Components of Perimeter-Based Security

Component	Function	Benefit	Limitation
Firewalls	Monitor and controls incoming and outgoing network traffic based on security rules	It blocks unlawful access and filters malicious traffic	Can be bypassed via trusted ports; Cannot inspect encrypted content or detect internal threats
Intrusion detection systems (IDS)	Monitors network for malicious behavior and policy violations	Detects known patterns of attack and anomalies; provides alerts for suspicious activity	High false-positives; It only detects and not prevent attacks
Virtual Private Networks (VPN)	Establishes secure, encrypted communication channels over untrusted networks.	Enables secure remote access and protects data in transit	Vulnerable if endpoints are compromised; may hide malicious traffic inside encrypted tunnels
Demilitarized Zones (DMs)	Isolate public-facing services (e.g., web, mail servers) from internal networks	It limits intruder access to internal systems even if public services ar compromised.	Poor configuration can expose the internal network; It adds network complexity
Network segmentation	Divides the network into zones/subnets to control traffic flow and limit breach scope.	Contains threats, improves performance, and enforces least-privilege access.	Misconfigured segmentation can cause service disruption or reduce security benefits.

Components of CSMA

CSMA is fundamentally a design framework that integrates various existing security technologies. However, there are core approaches or components commonly associated with CSMA, each serving as a critical enabler of its functionality. What key security functions or strategies that CSMA integrates to operate effectively? They include:

i. Identity and Access Management (IAM): This verifies identities and manages user access based on roles and contextual rules.
ii. Zero Trust Architecture (ZTA): It requires strict identity verification for every access attempt, assuming no trust.
iii. Distributed Security Controls: This deploys security functions across all network layers (cloud, edge, on-premises).
iv. Security Analytics and Intelligence: It uses data analytics and AI to detect, predict, and respond to security threats.
v. Dynamic Security Posture Management: Continuously adjusts security measures based on changing risks and vulnerabilities.
vi. Secure Access Service Edge (SASE): Merges networking and security into a cloud-delivered model for remote protection.
vii. Encryption Everywhere: Ensures all data is encrypted—at rest, in transit, and during use—across systems.
viii. Decentralized Security Policy Management: Enables localized policy enforcement without relying on a central authority.

Layers of Cybersecurity Mesh Architecture

These represent CSMA's architectural pillars — the internal layers or building blocks that make the framework work cohesively. What are the architectural elements that define how CSMA operates? They are as follows:

i. Security Analytics & Intelligence: Real-time data collection, behavioral analysis, and threat detection. Adaptive Security Analytics, integrating AI/ML for predictive threat intelligence

ii. Policy Management: Central control for defining security policies, with decentralized enforcement. Unified Policy Orchestration, enabling consistent security governance across hybrid infrastructures

iii. Distributed Identity Fabric: Identity providers, Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Zero Trust principles. Decentralized Identity Fabric, implementing context-aware Zero Trust access controls.

iv. Consolidated Dashboards: Unified interfaces to manage tools from different vendors, often cloud-native. Automated Compliance Enforcement, reducing manual security overhead.

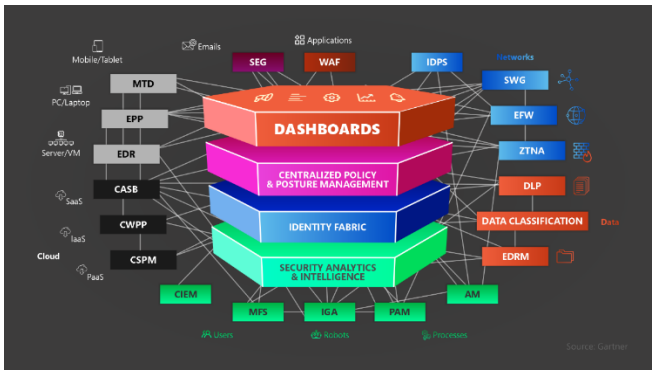

Figure 2: An Illustration of CSMA Components Obtained from United States Cybersecurity Institute (USCI, 2024)

Table 2: Technical Focus Area of the Research

Domain	Coverage Parameters	Exclusion Criteria
Architecture	Core CSMA layers	Proprietary vendor implementation
Deployment	Cloud native and hybrid implementation	Legacy perimeter security studies
Metrics	Quantifiable security outcomes	Theoretical frameworks without validation

MATERIALS AND METHODS

This study follows the widely recognized PRISMA 2020 framework. (BMJ, 2021) alongside the reporting guidelines by Dhillon (2022). These literatures were identified via targeted searching. A total of 95 records were identified through database searches. After removing duplicates, 81 records remained for screening. From these, 50 were screened and 32 full-text documents were reviewed, out of which 28 papers were included based on predefined eligibility criteria.

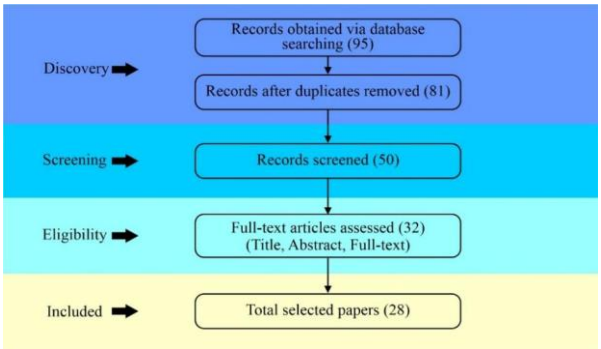

Figure 3: PRISMA 2020 Based Flow Diagram Template for Systematic Literature Reviews

Scope of the Study

This academic review, covers literatures and industry reports published in 2018-2025, with emphasis on post-pandemic studies (2020-2025) reflecting modern hybrid work challenges. The review focus is summarized as below:

Methodological Boundaries

i. Systematic review of at least 25 peer-reviewed papers from reputable databases, including:
ACM Digital Library (http://www.portal.acm.org/dl.cfm)
IEEE Xplore (http://www.ieeexplore.ieee.org/Xplore/)
MDPI Online (https://www.mdpi.com/journal)
SpringerLink (www.springerlink.com/)
Elsevier ScienceDirect (www.sceincedirect.com/)
Wiley Online Library (https://onlinelibrary.wiley.com/)

ii. Exclusion of non-English publications and pre-2018 architectural concepts

iii. Previous literatures were obtained via:
Google Scholar (http://scholar.google.com.au/)

Outline Structure of This Review

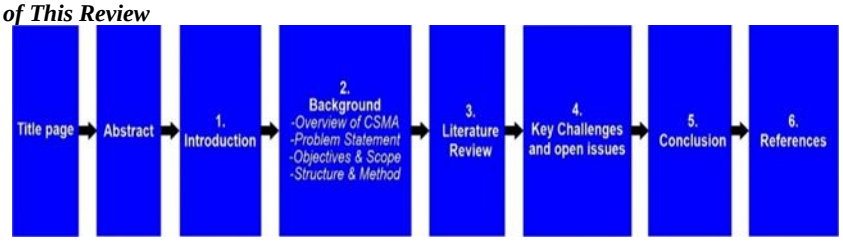

Figure 4: An Illustration of Structure of the Research

RESULTS AND DISCUSSION

Recent peer-reviewed studies, while not always explicitly labeled under "Cybersecurity Mesh Architecture (CSMA)," closely align with its core principles—such as approaches of CSMA earlier mentioned. These works collectively demonstrate the growing relevance and impact of CSMA in addressing modern cybersecurity challenges across distributed digital environments. Findings reveal that CSMA adoption yields notable security improvements, including up to 40% faster threat detection rates and response times, and as much as 90% reduced breach impacts, according to Gartner (Gartner, 2020). The table below presents other reviews that reflects key elements of CSMA and contributes to its conceptual and practical development:

Table 3: A Systematic Enumeration of Correlated Literatures

Author(s)	Title	Research Focus	Observation/Findings
Adamson K. M & Qureshi A.	Zero Trust 2.0: Advances, Challenges, and Future Directions in ZTA	ZTA vs perimeter security	Compared to perimeter security, ZTA reduced breach incidents by 73%
Aishwarya R. et al. (2025)	Cyber Security for Mobile Applications using Artificial Intelligence	CSMA vs traditional security approaches for mobile application	CSMA achieved 96.78% accuracy in intrusion detection with 0.21% error rate, beyond traditional methods
Alnaim K.A. & Alwakeel A. M. (2025)	Zero Trust Strategies for Cyber-Physical Systems in6G Networks	SDP & ZTA vs traditional firewalls	63.5% Latency Reduction
Widowati U. F. (2025)	Cybersecurity Mesh and Edge Computing on the Analytics Platform of the Indonesian Telecommunications industry	Integration of CSMA and edge computing for security	The integration achieved 75% latency reduction, 89% increased threat detection, 45% increase in operational efficiency as compared to perimeter-based security.
Cruz B. R. et al. (2024)	The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research	Analyzes how intelligent systems can strengthen cybersecurity mesh architecture.	Integrated systems within CSMA can significantly improve cybersecurity by enhancing scalability, interoperability, and resilience.
Mampilly J. A. & Midhunchakkaravarthy D. (2025)	Cybersecurity Mesh Architecture: A Framework for Enhanced Compatibility and Security in the Digital Age.	How organizations in the UAE use CSMA to unify and optimize security solutions across different sectors.	Consolidating network and security technologies using CSMA improves system efficiency, user experience, and threat defense.
Yongjun R. et al. (2025)	Zero Trust Networks: Evolution and Application from Concept to Practice	Investigates Zero Trust Networks (ZTN) as a modern cybersecurity model, analyzing its principles, technologies, applications, and effectiveness across diverse digital environments.	Zero Trust effectively addresses limitations of perimeter-based security and offers robust protection in complex settings like 6G, IoT, and cloud computing.
Asad M. & Otoum S. (2024)	Integrated Federated Learning and Zero-Trust approach or secure wireless communications	Incorporation of federated learning and Zero Trust security to strengthen wireless communication security frameworks.	Decentralized data and strict access control enhance wireless security and offer scalable, future-ready protection.
Orabi M. M., Emam O. & Fahmy H. (2025)	Adapting security and decentralized knowledge enhancement in federated learning using	Review of Federated Learning (FL) and explores how integrating it with blockchain	Blockchain effectively addresses key FL challenges—like model poisoning, data integrity, and communication

Author(s)	Title	Research Focus	Observation/Findings
	blockchain technology: literature review	can enhance security, privacy, and performance	overhead—while raising new needs around interoperability and regulatory compliance.
Feng Y. et al. (2022)	Blockchain-empowered secure federated learning system: Architecture and applications	Proposes a Blockchain-based Federated Learning (BFL) framework to improve the security, scalability, and fault tolerance of FL systems.	The proposed model outperforms standard FL methods in accuracy and resilience against malicious nodes, demonstrating enhanced robustness in IoT environments.
Unal D. et al. (2021)	Integration of federated machine learning and blockchain	The integration of Blockchain with Federated Learning (FL) to secure big data analytics in IoT systems against model poisoning and privacy breaches.	The proposed hashing mechanism effectively detects anomalies in FL-trained models, enhancing security and data integrity in simulated attack scenarios.
Zhang J. et al.	CSFL: cooperative security aware federated learning model using the blockchain	Proposes a blockchain-based Cooperative Security-aware Federated Learning model to enhance fairness, security, and privacy among participants.	The model employs a credit-based economic system and advanced encryption methods, achieving improved security and accuracy as demonstrated by simulations on real datasets.
Abuzied Y. Y. et al. (2024)	A privacy-preserving federated learning framework for blockchain networks	It presents FLoBC, a scalable, privacy-preserving federated learning framework built on blockchain to enable decentralized model training without exposing user data.	FLoBC achieves performance comparable to centralized learning systems while preserving privacy and enabling scalable, decentralized training across multiple nodes.
Ogunbadejo M. D. et al. (2025)	Overview of Zero Trust Architecture Trend and Advancement in Information Security	Zero Trust Architecture (ZTA) as a modern cybersecurity model replacing perimeter-based security by leveraging technologies like 5G, blockchain, and quantum computing	Effectively mitigates insider threats, enforces strict access control, and enhances real-time threat detection across diverse sectors.
Yang J. et al (2023)	Trust DFL: A Blockchain-Based Verifiable and Trusty Decentralized Federated Learning Framework	Decentralized federated learning framework using blockchain, smart contracts, and zero-knowledge proofs to enhance model security, integrity, and scalability.	Model poisoning and single-point failures while preserving data privacy, with IPFS integration reducing storage and communication overhead in multi-party federated learning environments.
Qammar A. et al. (2022)	Securing federated learning with blockchain: a systematic literature review	Integrating blockchain with federated learning (FL) to enhance privacy, security, and system robustness in decentralized machine learning.	Enhanced mitigating security threats, ensures transparent verification and rewards, and boosts accountability, though some challenges remain.
Arif. T. et al (2025)	A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats	Trust-centric and privacy-enhancing security techniques tailored to address the unique challenges of cloud-native architectures.	Layered security controls like service mesh and cloud-native SIEM significantly improves threat detection, reduces attack surfaces, and strengthen trust across cloud native systems.
Liu C. et al. (2024)	Dissecting zero trust: research landscape and its implementation in IoT	Trust-centric and privacy-enhancing security techniques tailored to address the unique challenges of cloud-native architectures	Analysis of tools like service mesh, cloud-native encryption, and runtime protection platforms, the study demonstrates how layered security strategies can enhance trust, resilience, and data protection across modern cloud-native environments.

Author(s)	Title	Research Focus	Observation/Findings
Theodoropoulos T. et al. (2023)	Security in Cloud-Native Services: A Survey	Security of cloud-native services, in relation to threats, security features, and supporting technologies.	Demonstrating how open-source tools can be integrated to enhance consistency, scalability, and threat mitigation across distributed infrastructures.
Sarhan M. et al. (2022)	HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection	Developing a secure, privacy-preserving, and scalable intrusion detection framework for IoT ecosystems using hierarchical federated learning and blockchain	Integrating threat intelligence sharing with secure model updates significantly improves detection performance while maintaining data confidentiality.
Garcia L. et al. (2025)	Compliant and Seamless Hybrid (Star and Mesh) Network Topology Coexistence for LoRaWAN: A Proof of Concept	Enhancing LoRaWAN-based IoT network connectivity by implementing a hybrid star–mesh topology that is fully compatible with existing systems	Dynamic topology switching based on link quality significantly improves signal strength, coverage, and transmission reliability in challenging environments.
Chen F. et al. (2021)	IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-Oriented Applications	Reviewing the security challenges of consumer-oriented smart IoT cloud systems through real-world case studies and a general ecosystem model	Current deployments exhibit significant security vulnerabilities, necessitating systematic analysis and mitigation strategies to enhance their resilience.
Rose S. et al. (2020)	Zero Trust Architecture	ZTA as a model centered on securing users and resources instead of network boundaries.	ZTA improves security by eliminating implicit trust and addressing modern enterprise challenges like remote access and BYOD.
Dindigala R. & Dandyala D. S. (2024)	Integrating Zero Trust Architecture with Service Mesh Enhanced Cloud Security in DevOps Workflows	Integrating Zero Trust Architecture (ZTA) with service mesh technology to enhance security in cloud-native DevOps environments	Embedding ZTA into service mesh improves access control, threat detection, and response time while maintaining DevOps agility.
Punia A. et al. (2024)	A systematic review on blockchain-based access control systems in cloud environment	Exploring the potential of blockchain technology to enhance access control, security, and trust in cloud computing	Blockchain enhances cloud access control by offering secure, decentralized, and tamper-proof solutions
Attkan A. & Ranga V. (2022)	Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence-based key-security	Integration of blockchain and AI for secure authentication and session key management in heterogeneous IoT environments.	Combining blockchain's decentralized key storage and AI's adaptive threat detection significantly enhances authentication, session management, and overall IoT security
Mahmood Z. & Jusas V. (2022)	Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy	Federated learning platform enhanced by blockchain, aimed at preserving data privacy across multiple security layers	Integration of blockchain adds tamper-resistant verification to federated model updates, significantly boosting privacy and system integrity while introducing minimal overhead.
Alnaim K. A. (2025)	Adaptive Zero Trust Policy Management framework in 5G networks	Proposes SecureChain-ZT, an adaptive Zero Trust framework for 5G networks that combines AI, blockchain, and real-time policy enforcement to overcome the limitations of static security models.	The model achieved 99.3% threat detection, cut unauthorized access by 87%, and reduced latency by 62.6%, showing strong real-time security for 5G.

Discussion

The outlined studies collectively reinforce the effectiveness of CSMA and reveals how its effectiveness critically addresses key limitations of traditional perimeter-based methods. Cybersecurity Mesh Architecture can be effectively applied to enhance security in the following areas (but not limited to them):

i. CSMA secures assets and workloads across AWS, Azure, Google Cloud, etc., by enforcing consistent identity and policy controls across cloud providers.

ii. The architecture enables secure access for users working from anywhere by using identity-based access, zero trust principles, and context-aware authentication.
iii. CSMA protects distributed and often vulnerable edge and IoT devices through decentralized security, device-level identity, and local policy enforcement.
iv. It applies automated and consistent security checks across the software development lifecycle, including container scanning, code signing, and access control in CI/CD pipelines.
v. The architecture supports dynamic policy enforcement and real-time threat detection across virtual networks and software-defined infrastructures.
vi. It enhances IAM by integrating adaptive authentication, privileged access management (PAM), and federated identity with granular, real-time control.
vii. It improves incident response and threat intelligence sharing by consolidating telemetry from decentralized security tools into a single analytics and response layer.
viii. It secures personal devices accessing corporate networks by applying device posture checks, context-aware access, and conditional authentication.
ix. CSMA ensures secure handling of sensitive patient data (e.g., under HIPAA) across multiple systems like EMRs, mobile apps, and remote diagnostics, through zero trust and data-centric security.
x. It protects industrial systems like SCADA, smart grids, and manufacturing plants by providing identity-based segmentation and localized threat response in environments not designed for internet exposure.

CSMA offers a comprehensive and efficient outline that adapts very well with emerging technologies and security paradigms, significantly improving security, scalability, and operational performance across diverse use cases.

CONCLUSION

This review examined Cybersecurity Mesh Architecture with some discoveries. CSMA has the potential of addressing contemporary security challenges in the present day distributed digital ecosystem and proliferation of cyber-attacks. The paradigm shift from traditional perimeter-based security models to dynamic approaches that better aligns with modern developments and environments. The architecture demonstrates significant efficacy when compared to conventional methods. However, there are pending significant issues that need to be resolved. It is uncertain on the general application of the architecture across various sectors. As such, there is a need for more research into deeper contexts and practical application of the architecture for on-the-field feedback. It is important to contrast and compare CSMA with other architectures.

As technological transition continues, CSMA emerges as a significant framework for ensuring cybersecurity. While implementation issues exist, the benefit of this architecture makes it a vital consideration for the strategic improvement an organizations security.

REFERENCES

Abuzied Y. et al. (2024). A privacy-preserving federated learning framework for blockchain networks. Cluster Computing, vol 27, pp 3997 - 4014. doi:https://doi.org/10.1007/s10586-024-04273-1

Adaptive Zero Trust Policy Management Framework in 5G Network. (2025). Mathematics: Application of Artificial Intelligence in Decision Making, vol 13(9). doi:https://doi.org/10.3390/math13091501

Adaptive Zero Trust Policy Management Framework in 5G Networks. (2025). Mathematics: Application of Artificial Intelligence in Decision Making, vol 13(9). doi: https://doi.org/10.3390/math13091501

Aishwarya R. et al. (2025). CSMA: Cyber Security for Mobile Applications using Artificial Intelligence. 2025 International Conference on Intelligent and Cloud Computing (ICoICC), pp. 1-6. doi:https://doi.org/10.1109/ICoICC64033.2025.11052002

Alnaim K. A. & Alwakeel A. M. (2025). Zero Trust Strategies for Cyber-Physical Systems in 6G Networks. Mathematics: Application of Artificial Intelligence in Decion Making, vol 13(7). doi: https://doi.org/10.3390/math13071108

Arif T. et al. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. Sensors, vol 25(2350), pages 1-30. doi: https://doi.org/10.3390/s25082350

Arif T. et al. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. Sensors, vol 25(2350), pp 1-30. doi: https://doi.org/10.3390/s25082350

Asad M. & Otoum S. (2024). Integrative Federated Learning and Zero-Trust Approach for Secure Wireless Communications. IEEE Wireless Communications, vol 31(2), pp 14-20. doi: https://doi.org/10.1109/MWC.001.2300355

Attkan A. & Ranga V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, vol 8, pp. 3559 - 3591. doi:https://doi.org/10.1007/s40747-022-00667-z

Bishop M. (2004). Introduction to Cyber Security. Addison-Wesley Professional. Retrieved June 29th, 2025

BMJ. (2021). PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews. 372(160). doi: https://doi.org/10.1136/bmj.n160

Chen F. et al. (2021). IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-oriented Applications. ACM Computing Surverys, vol 54,4, Article No. 75, pages 1 - 26. doi: https://doi.org/10.1145/3447625

Chen F. et al. (n.d.). IoT Cloud Security Review: A Case Study Approach Using Emerging Consumer-Oriented Applications. ACM Computing Surveys, vol 54(4)(article 75), 2021. doi: https://doi.org/10.1145/3447625

Cisco. (2022, November 21). Cisco Solutions. Retrieved June 24, 2025, from Securing Cloud-Native Applications - Azure Design Guide: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/scloud-azure-cn-design-guide.html

Cruz B. R. et al. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing, vol 581(127427), pp. 1-33. doi: https://doi.org/10.1016/j.neucom.2024.127427

Dhillon P. (2022, July 06). How to write a good scientific review article. The FEBS Journal, vol 289(13), pp. 3592-3602. doi: https://doi.org/10.1111/febs.16565

Dindigala R. & Dandyala D. S. (2024). Integrating Zero Trust Architecture with Service Mesh for Enhanced Cloud Security in DevOps Workflows. International Journal of Computer and Information System (IJCIS), vol 05(04), pp. 331 - 336. doi: https://ijcis.net/index.php/ijcis/index

DuPont Q. & Fidler B. (2016). Edge Cryptography and the Codevelopment of Computer Networks and Cybersecurity. IEEE Annals of the History of Computing, vol 38(4), pp. 55-73. doi:10.1109/MAHC.2016.49

Feng Y. et al. (2022). Blockchain-empowered secure federated learning system: Architecture and applications. Computer Communications, vol 196, pp 55-65. doi:https://doi.org/10.1016/j.comcom.2022.09.008

Ferretti L. et al. (2021). Survivable zero trust for cloud computing environments. Computers & Security, vol 110(102419). doi:https://doi.org/10.1016/j.cose.2021.102419

Ganapati S. et al. (2023). Evolution of Cybersecurity Concerns: A Systematic Literature Review. Proceedings of the 24th Annual International Conference on Digital Government Research, pp. 90 - 97. doi:https://doi.org/10.1145/3598469.3598478

Garcia L. et al. (2025). Compliant and Seamless Hybrid (Star and Mesh) Network Topology Coexistence for LoRaWAN: A Proof of Concept. Applied Sciences, vol 15(7), pages 1-25. doi:https://doi.org/10.3390/app15073487

Gartner Inc. (2025, June 25th). Cybersecurity Mesh. Retrieved from In Gartner IT Glossary: https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh

Gartner Inc. (2025). Secure Access Service Edge (SASE). Retrieved June 25, 2025, from Gartner: https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase

Gartner Inc. (2020, October 19). Gartner. (Gartner Inc) Retrieved June 24, 2025, from Newsroom: Press Releases: https://www.gartner.com.au/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021

Gartner Inc. (2023, January). Cybersecurity Mesh Architecture (CSMA). Retrieved June 25th, 2025, from Gartner: https://www.gartner.com/peer-community/oneminuteinsights/omi-cybersecurity-mesh-architecture-csma-guf

Infosec Institute. (2014, May 13th). A History of Malware: Part One, 1949-1988. (Cengage Learning) Retrieved July 10th, 2025, from Infosec: Malware analysis: https://www.infosecinstitute.com/resources/malware-analysis/history-malware-part-one-1949-1988/

Jianli P. et al. (2018). Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World. CODASPY '18: Eighth ACM Conference on Data and Application Security and Privacy (pp. Pages 29 - 32). New York, United States: Association for Computing Machinery (ACM). doi: https://doi.org/10.1145/3180465.3180470

Ju L. et al. (2024). Enhancing real-time intrusion detection and secure key distribution using multi-model machine learning approach for mitigating confidentiality threats. Internet of Things, 28(101377). doi:https://doi.org/10.1016/j.iot.2024.101377

Kessler C. G. and Pritsky T. N. (2009). Network Topologies, Protocols, and Design. In W. E. Bosworth S., Computer Security Handbook (5th Edition ed.). Wiley.

Kotha R. N. (2020). Network Segmentation as a Defense Mechanism for Securing Enterprise Networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol 11(3), Pages 3023-3030. doi:https://doi.org/10.61841/turcomat.v11i3.14942

Liu C. et al. (2024). Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity, vol 7(20). doi:https://doi.org/10.1186/s42400-024-00212-0

Mahmood Z. & Jusas V. (2022). Blockchain-Enabled: Multi-Layered Security Federated Learning Platform for Preserving Data Privacy. Electronics: Networks, vol 11(10). doi:https://doi.org/10.3390/electronics11101624

Mampilly A. J. & Midhunchakkaravarthy D. (2025). Cybersecurity Mesh Architecture: A Framework for Enhanced Compatibility and Security in the Digital Age. In S. C. Pon , N. Sehgal, S. Ruhela, & N. Rizvi (Ed.), International Conference on Innovation, Sustainability, and Applied Sciences. ICISAS 2023. Signals and Communication Technology (pp. pp 441-445). Springer, Cham. doi: https://doi.org/10.1007/978-3-031-68952-9_58

Matthews T. (2022, January 1st). Creeper: The World's First Computer Virus. Retrieved July 10th, 2025, from Exabeam: https://www.exabeam.com/blog/infosec-trends/creeper-the-worlds-first-computer-virus/

Munoz A., Sanchez-Cid F., El Khoury P. . et al. (2008). XACML as a Security and Dependability Pattern for Access Control in AmI environments. Developing Ambient Intelligence (pp. Pages 143 -155). Paris: Springer. doi: https://doi.org/10.1007/978-2-287-78544-3_14

Ogunbadejo M. D. et al. (2025). Overview of Zero Trust Architecture Trend and Advancement in Information Security. Journal of Information Engineering and Applications (JIEA), vol 15(1), pp. 21- 30. doi:https://10.7176/JIEA/15-1-03

Orabi M. M., Emam O. & Fahmy H. (2025). Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review. Journal of Big Date, vol 12(55). doi:https://doi.org/10.1186/s40537-025-01099-5

Pallewatta S. and Babar A. M. (2024). Towards Secure Management of Edge-Cloud IoT Microservices using Policy as Code. (M. Galster, P. Scandurra, T. Mikkonen, P. O. Antonino, E. Y. Nakagawa, & E. Navarro, Eds.) Software Architecture. ECSA 2024. Lecture Notes in Computer

Science, vol 14889, Pages 1-16. doi:https://doi.org/10.1007/978-3-031-70797-1_18

Parast K. F. et al. (2022). Cloud computing security: A survey of service-based models. Computers & Security, 114(102580). doi:https://doi.org/10.1016/j.cose.2021.102580

Punia A. et al. (2024). A systematic review on blockchain-based access control controls systems in cloud environment. Journal of Cloud Computing, vol 13(146), pp. 1-37. doi: https://doi.org/10.1186/s13677-024-00697-7

Qammar A. et al. (2023). Securing federated learning with blockchain: a systematic literature review. Artificial Intelligence Review, vol 56, pp 3951 -3985. doi:https://doi.org/10.1007/s10462-022-10271-9

Ramos-Cruz, B., Andreu-Perez, J., & Martinez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. Neurocomputing, vol 581(127427), pages 1-33. doi:https://doi.org/10.1016/j.neucom.2024.127427

Reddy V. R et al. (2024). Adaptive Vulnerability Matching Assessment: A Holistic Approach for Cyber security Resilience. Iternational Journal For Research in Applied Science and Engineering Technology (IJRASET), 2(3), pages 46 - 51. doi: https://doi.org/10.22214/ijraset.2024.59554

Ren Y., Wang Z., Sharma K. P. et al. (2025). Zero Trust Networks: Evolution and Application from Concept to Practice. Computers, Materials & Continua, vol 82(2), Pages 1593-1613. doi: https://doi.org/10.32604/cmc.2025.059170

Repetto M. et al. (2021). An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. Journal of Networks and Systems Management, vol 29(37), pages 1-34. doi: https://doi.org/10.1007/s10922-021-09607-7

Rose S. et al. (2020). Zero Trust Architecture. NIST Special Publication 800-207, pp 1-50. doi:https://doi.org/10.6028/NIST.SP.800-207

Saqid M. et al. (2025). Adaptive Security Policy Management in Cloud Environments Using Reinforcement Learning. Cryptography and Security. doi:https://doi.org/10.48550/arXiv.2505.08837

Sarhan M. et al. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering, vol 103(108379). doi:https://doi.org/10.1016/j.compeleceng.2022.108379

Theodoropoulos T. et al. (2023). Security in Cloud-Native Services: A Survey. Journal of Cybersecurity and Privacy, vol 3(4), pp 758 - 793. doi: https://doi.org/10.3390/jcp3040034

Tim M. et al. (2009). Cloud Security and Privacy: An Enterprise perspective on Risks and Compliance (Vol. First edition). USA: O'Reilly Media Inc.

Unal D. et al. (2021). Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. Computers & Security, vol 109(102393). Doi:https://doi.org/10.1016/j.cose.2021.102393

United States Cybersecurity Institute. (2024). Cybersecurity Mesh Architecture (CSMA): An Overview. Retrieved June 28th, 2025, from https://www.uscsinstitute.org/cybersecurity-insights/blog/cybersecurity-mesh-architecture-an-overview

Walling S. (2020). A Comprehensive Review on Cloud Computing and Cloud Security Issues. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), vol 6(4), Pages 483-490. doi: https://doi.org/10.32628/CSEIT206489

Widowati U. F. (2025). Cybersecurity Mesh and Edge Computing on the Analytics Platform of the Indonesian Telecommunications Industry. International Journal of Management Science and Information Technology (IJMSIT), vol 5(1), pages 183 - 191. doi:https://doi.org/10.35870/ijmsit.v5i1.3845

Xi N. et al. (2023). Decentralized access control for secure microservices cooperation with blockchain. ISA Transactions, 141, pages 44-51. doi:https://doi.org/10.1016/j.isatra.2023.07.018

Yang J., Zhang W., Guo Z., & Gao Z. (2023). TrustDFL: A Blockchain-Based Verifiable and Trusty Decentralized Federated Learning Framework. Electronics, vol 13(1). doi:https://doi.org/10.3390/electronics13010086

Yongjun R. et al. (2025). Zero Trust Networks: Evolution and Application from Concept to Practice. Computers, Materials and Continua, vol 82(2), Pages 1593-1613. doi:https://doi.org/10.32604/cmc.2025.059170

Zhang J. et al. (2024). CSFL: Cooperative Security Aware Federated Learning Model Using The Blockchain. The Computer Journal, vol 67(4), pp 1298-1308. doi:https://doi.org/10.1093/comjnl/bxad060

Zheng Y. et al. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, vol 8(4), Pages 422-435. doi:https://doi.org/10.1016/j.dcan.2021.07.006