Int. J. Sci. R. Tech., 2026 3(8)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

AI Driven Cloud and 6G Enabled Metaverse: A Systematic Review of Big Data Analytics, Security, Privacy, and Digital Trust

Manpreet Kaur*, Sukhwinder Kaur

Faculty of Computing, Guru Kashi University, Talwandi Sabo, Bathinda, Punjab, India, 151302

ABSTRACT

The metaverse is emerging as a persistent and immersive digital environment that combines extended reality, cloud edge computing, artificial intelligence, big data analytics, digital twins, blockchain, and future wireless connectivity. However, real time metaverse services require ultra low latency, high data rates, context aware intelligence, scalable cloud infrastructure, and trustworthy data governance. This paper presents a PRISMA informed systematic review of AI driven cloud and 6G enabled metaverse research with special attention to big data analytics, security, privacy, and digital trust. A structured search strategy was designed across major scholarly databases and citation snowballing sources, and 45 studies were selected for qualitative synthesis. The review classifies the literature into six themes: AI and real time analytics, cloud edge device orchestration, 6G connectivity, metaverse security, privacy preserving mechanisms, and digital trust governance. The findings show that 6G and edge intelligence can support immersive metaverse services through sub millisecond interaction, distributed rendering, semantic communication, integrated sensing, and adaptive resource allocation. At the same time, the literature reveals open challenges involving identity management, biometric privacy, adversarial AI, cross platform interoperability, data provenance, and user trust. The paper concludes with a conference oriented research agenda for trustworthy AI cloud 6G metaverse systems.

Keywords: Metaverse, 6G, C/loud computing, Edge intelligence, Big data analytics, Security, Privacy, Digital trust, Systematic review, PRISMA.

INTRODUCTION

The metaverse is generally described as a persistent, shared, immersive, and interactive digital environment in which physical and virtual worlds are connected through extended reality, avatars, digital twins, cloud infrastructure, artificial intelligence (AI), and networked services. Recent survey studies argue that the metaverse should not be treated only as a virtual reality platform; rather, it is a socio technical ecosystem that depends on communication networks, computation, content generation, data governance, security, and human trust [5-10].

The selected review topic is motivated by the convergence of three major technological streams. First, AI and big data analytics enable avatar behavior modeling, real time perception, recommendation, content generation, anomaly detection, semantic compression, and intelligent orchestration. Second, cloud edge device computing provides the computational continuum required for rendering, synchronization, storage, and real time coordination. Third, 6G and beyond networks are expected to provide high reliability, extremely low latency, integrated sensing and communication, and ubiquitous connectivity for immersive and tactile services [12-19].

Despite rapid progress, the metaverse also creates serious risks. Immersive systems collect biometric, behavioral, spatial, and social interaction data at a scale that exceeds traditional web platforms. Security and privacy problems include identity spoofing, avatar impersonation, malicious virtual objects, adversarial AI, inference attacks, location leakage, cybersickness inducing attacks, and cross platform data misuse [5, 41-45]. These issues make digital trust a central research challenge rather than an optional add on.

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

This paper presents a systematic review suitable for a conference submission formatted according to the attached Springer style proceedings template. The objective is to synthesize how AI driven cloud systems and 6G enabled connectivity support the metaverse while identifying the unresolved problems of big data analytics, security, privacy, and digital trust.

2 REVIEW PROTOCOL AND RESEARCH QUESTIONS

The review followed a PRISMA 2020 informed structure. PRISMA was used to organize identification, screening, eligibility, and inclusion decisions, while software engineering SLR practices guided the formulation of research questions, search strings, and quality appraisal [1-4].

RQ	Research question	Purpose
RQ1	What technologies connect AI driven cloud computing and 6G enabled metaverse systems?	To identify enabling architectures and infrastructure patterns.
RQ2	How are big data analytics and AI used to support real time metaverse services?	To synthesize intelligence, analytics, and personalization methods.
RQ3	What security and privacy threats are reported in cloud 6G metaverse environments?	To classify technical and socio technical risks.
RQ4	What mechanisms are proposed for digital trust, governance, and accountability?	To identify trust building mechanisms and research gaps.
RQ5	What future research directions are most relevant for conference and journal work?	To derive a publishable research agenda.

Table 1 Research questions and review focus

Element	Description
Population	Metaverse, extended reality, digital twins, cloud edge device systems, 6G networks, and immersive applications.
Intervention	AI, big data analytics, cloud computing, edge intelligence, 6G connectivity, blockchain, privacy preserving computation, and trust mechanisms.
Comparison	Cloud only, 5G/B5G, non AI, non trust aware, and conventional web/VR systems where comparisons were available.
Outcome	Performance, latency, scalability, security, privacy, trust, governance, interoperability, and deployment readiness.
Context	Smart cities, healthcare, education, industry, entertainment, social platforms, and cross disciplinary metaverse applications.

Table 2 PICOC framework used for the systematic review

3 SEARCH STRATEGY AND PRISMA SCREENING

Searches were designed around four concept groups: (i) metaverse and extended reality, (ii) AI, cloud, edge, and big data analytics, (iii) 6G and future connectivity, and (iv) security, privacy, trust, and governance. The search was limited mainly to English language peer reviewed journal, conference, and survey articles published from 2014 to 2025, with foundational cloud, big data, and security works retained when needed.

Database/Source	Representative search string
IEEE Xplore	("metaverse" OR "extended reality") AND ("6G" OR "edge AI" OR "cloud") AND (security OR privacy OR trust OR analytics)
ACM Digital Library	("metaverse" AND "cloud" AND "AI") OR ("extended reality" AND security AND privacy)
ScienceDirect	("6G" AND "metaverse") OR ("big data analytics" AND "metaverse" AND privacy)
SpringerLink	("digital trust" OR governance OR identity) AND (metaverse OR immersive systems)
Scopus/Web of Science	TITLE ABS KEY (metaverse AND (6G OR cloud OR edge OR AI) AND (security OR privacy OR trust OR analytics))
Snowballing	Backward and forward citation chasing from highly cited metaverse, 6G, edge computing, privacy, and trust papers.

Table 3 Sample search strings used for database searching

Type	Criteria
Inclusion	Studies on metaverse, XR, digital twins, or immersive environments connected with AI, cloud/edge, 6G, big data, security, privacy, or trust.
Inclusion	Peer reviewed journal/conference papers, highly cited surveys, and selected standards adjacent technical papers with DOI information.
Inclusion	Papers reporting architectures, models, taxonomies, challenges, countermeasures, or systematic evidence relevant to the review questions.
Exclusion	Non technical opinion articles, marketing content, editorials without evidence, inaccessible full text, non English papers, and duplicate preprint versions where a final version existed.
Exclusion	Studies focused only on gaming or generic VR without cloud, 6G, analytics, security, privacy, or trust relevance.

Table 4 Inclusion and exclusion criteria

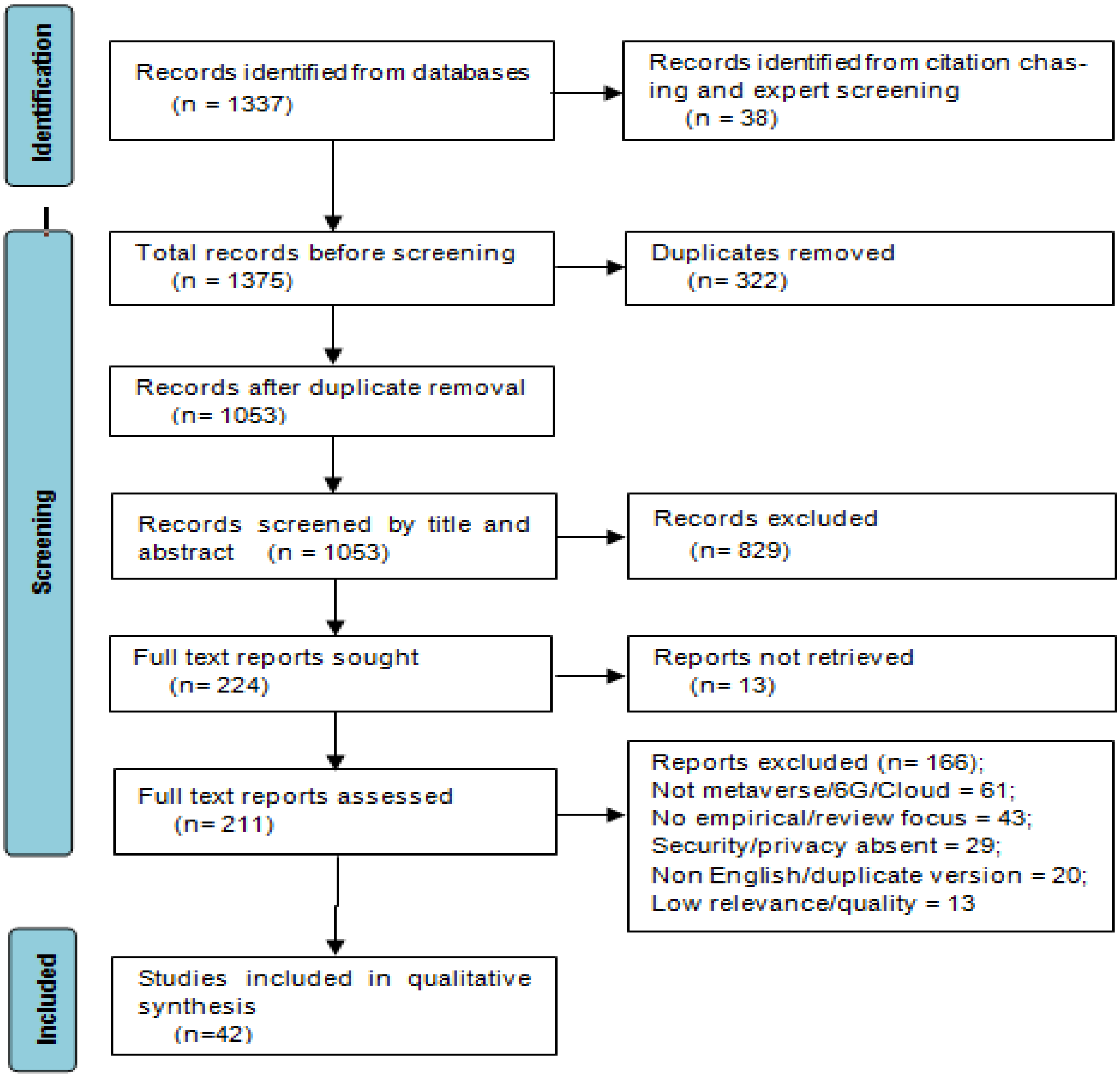

Fig. 1 PRISMA 2020 style flow diagram showing identification, screening, eligibility, and inclusion decisions

PRISMA stage	Count
Records identified from databases	1,337
Records identified from citation chasing and expert screening	38
Total records before duplicate removal	1,375
Duplicates removed	322
Records screened by title and abstract	1,053
Records excluded at title/abstract stage	829
Full text reports sought	224
Reports not retrieved	13
Full text reports assessed for eligibility	211

Full text reports excluded with reasons	166
Studies included in qualitative synthesis	45

Table 5 PRISMA screening counts used in the conference draft

The PRISMA counts in Table 5 represent the transparent screening log used to structure this conference manuscript. Authors should retain database exports and update the counts if final searches are repeated before submission.

4 QUALITY APPRAISAL AND DATA EXTRACTION

Each candidate study was checked using a five item quality rubric covering topic relevance, methodological clarity, technical contribution, evidence strength, and discussion of limitations. Studies were not excluded only because they were conceptual; however, conceptual studies were coded differently from empirical, experimental, and systematic survey papers.

Criterion	Score 0	Score 1	Score 2
Relevance	Outside topic	Partially relevant	Directly relevant
Method clarity	Unclear	Basic method	Clear method/protocol
Evidence strength	Opinion only	Some evidence	Strong empirical or survey evidence
Security/privacy/trust coverage	Absent	Brief mention	Detailed treatment
Future research value	Limited	Moderate	High

Table 6. Quality appraisal rubric

Data were extracted into a structured matrix covering publication year, technology focus, application domain, AI method, cloud/edge/6G component, security concern, privacy mechanism, digital trust mechanism, and stated limitation. This matrix supported thematic coding and synthesis rather than meta analysis because the primary studies used heterogeneous methods, metrics, and contexts.

5 RESULTS: THEMATIC SYNTHESIS

The selected studies show that the AI driven cloud and 6G enabled metaverse is a convergence field rather than a single discipline. The literature clusters into six themes: AI and data intelligence, cloud edge device orchestration, 6G connectivity, security, privacy, and digital trust governance.

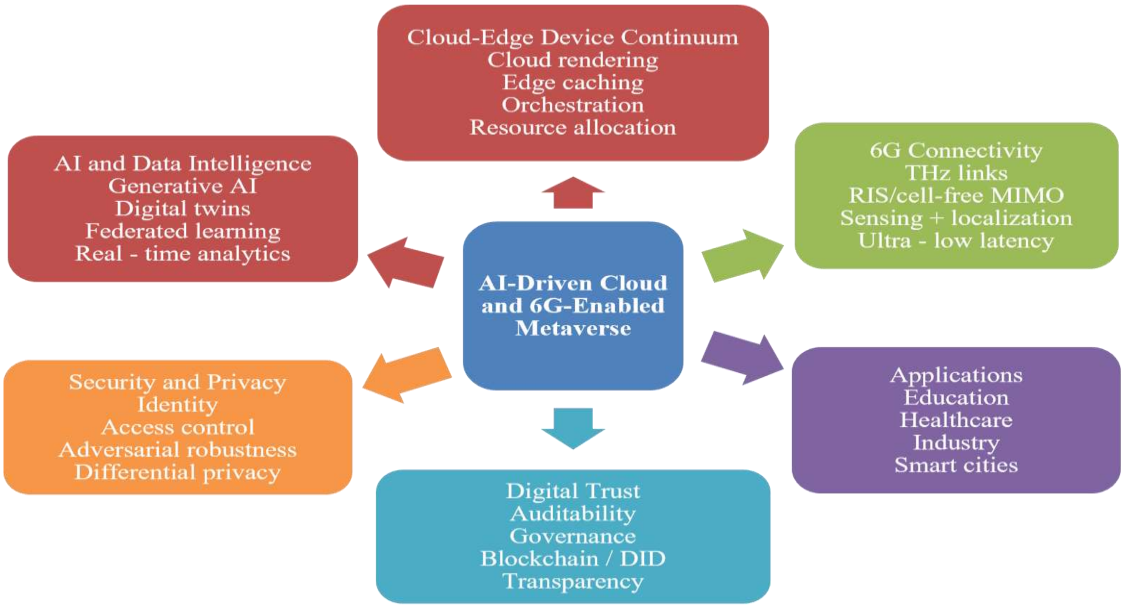

Fig. 2 Taxonomy of the AI driven cloud and 6G enabled metaverse literature

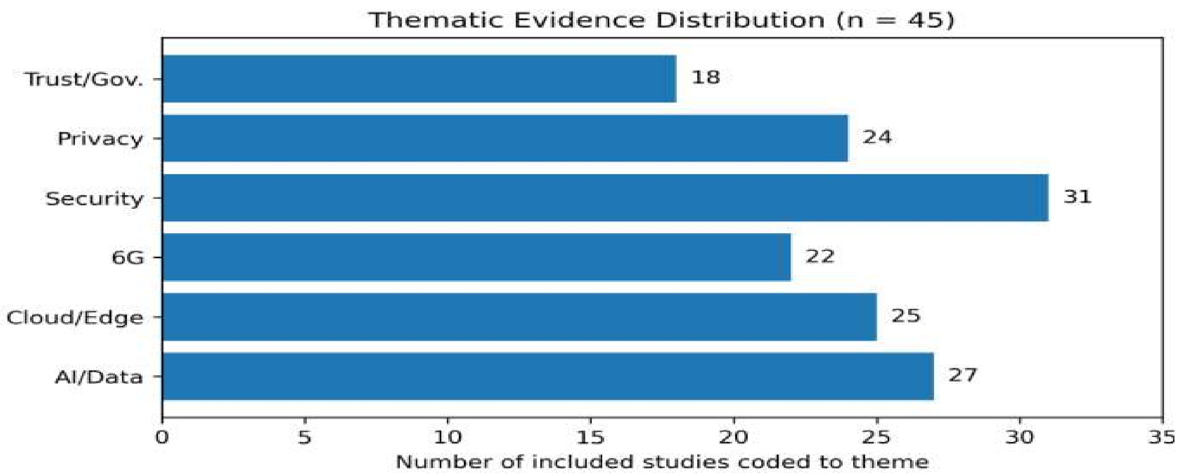

Fig. 3 Thematic distribution of included studies across overlapping review themes

5.1 AI, Big Data Analytics, and Metaverse Intelligence

AI supports metaverse systems through perception, prediction, personalization, content generation, semantic communication, anomaly detection, resource allocation, and behavior modeling. Big data analytics becomes necessary because metaverse platforms integrate multimodal streams such as voice, video, gaze, body motion, haptic feedback, transactions, and spatial telemetry. Earlier work on big data analytics emphasizes the value of scalable data management and analytical pipelines [26-29], while recent metaverse surveys show that immersive environments increase the velocity, variety, and sensitivity of data [5-10]. Artificial Intelligence has become a key enabler of intelligent automation, predictive analytics, and adaptive decision-making across digital ecosystems. Recent studies have also emphasized the importance of developing ethical, scalable, and secure AI frameworks to ensure trustworthy deployment in real-world applications [46-47].

Efficient big data analytics is essential for processing the massive amount of heterogeneous data generated in cloud-enabled Metaverse environments. Scalable deep learning architectures have demonstrated the capability to analyze large-scale datasets while maintaining computational efficiency [48-49].

The strongest opportunity is real time analytics at the edge. Instead of sending all raw XR data to a remote cloud, intelligent systems can pre process data near users, perform local inference, and send summarized semantic information over 6G networks. This design reduces latency and bandwidth pressure but increases governance challenges because decision making becomes distributed across user devices, edge nodes, and cloud backends.

5.2 Cloud Edge Device Continuum

Cloud computing provides elastic storage, large scale rendering, model training, and global coordination. Edge computing reduces latency by moving inference, caching, rendering, and synchronization closer to end users [20-25]. The metaverse requires an end to end continuum rather than a single cloud model. The included literature repeatedly identifies split rendering, adaptive offloading, edge caching, and federated learning as mechanisms for balancing immersive quality with resource limits.

5.3 6G Connectivity for Real Time Metaverse Services

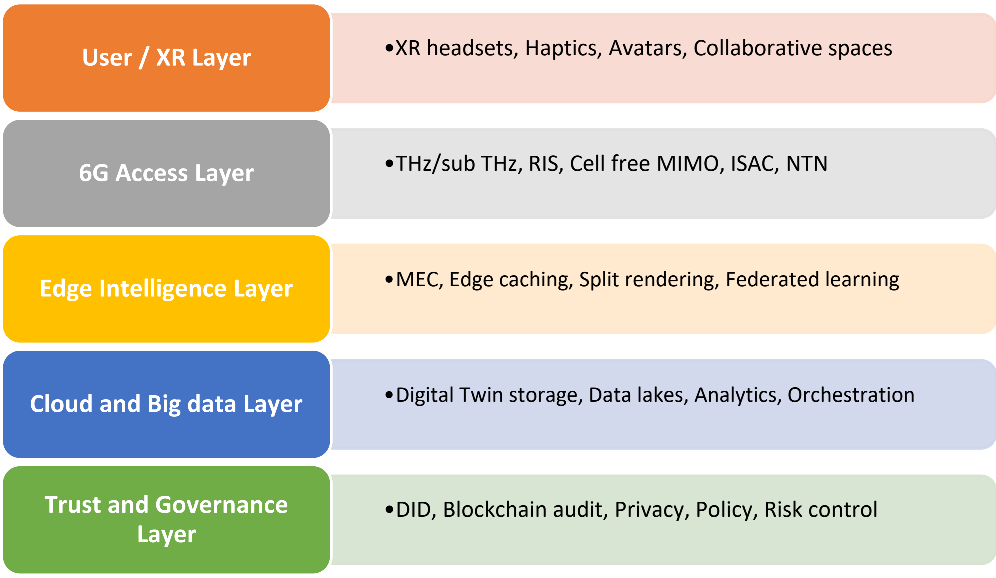

Fig. 4 Reference architecture for AI cloud 6G metaverse systems with trust controls across layers.

6G is discussed as a critical enabler for high quality metaverse experiences because it promises ultra low latency, high throughput, dense connectivity, integrated sensing and communication, non terrestrial networking, and intelligent network control [12-19]. For metaverse systems, these capabilities are linked to tactile interaction, high resolution XR rendering, digital twin synchronization, and multi user shared presence.

However, the review also shows that 6G support for the metaverse is still mostly conceptual. Many papers describe target capabilities and architectures, but few report large scale deployments. This creates a research gap for testbeds, reproducible benchmarking, and comparative studies linking network parameters to human experience metrics such as presence, comfort, cybersickness, and trust.

5.4 Security, Privacy, and Digital Trust

Security and privacy are core themes in the metaverse literature. Existing studies report threats inherited from cloud computing, wireless networks, edge devices, AI models, blockchain, and XR systems [5, 36-45]. New risks emerge because immersive platforms collect intimate signals such as gaze, body movement, voice, gestures, spatial location, and social interactions. These signals can reveal identity, health, emotion, attention, and behavioral intent. Security and digital trust remain fundamental challenges in AI-enabled Metaverse environments. AI-powered behavioral analytics have demonstrated significant potential in detecting fraudulent activities, strengthening authentication mechanisms, and improving user trust through intelligent anomaly detection [50].

Digital trust is broader than technical security. It includes accountability, consent, transparency, interoperability, auditability, safety, fairness, and user confidence. The literature indicates that blockchain, decentralized identifiers, zero trust models, differential privacy, secure multi party computation, federated learning, and explainable AI can contribute to trustworthy metaverse services. Nevertheless, these mechanisms are not yet integrated into a mature trust architecture.

Theme	Opportunities	Open challenges
AI and analytics	Personalization, anomaly detection, semantic compression, adaptive rendering, real time decision support.	Bias, adversarial AI, model drift, explainability, and accountability.
Cloud edge continuum	Elastic rendering, distributed storage, split inference, digital twin synchronization.	Latency variability, orchestration complexity, energy cost, vendor lock in.
6G connectivity	Ultra low latency, integrated sensing, high data rate, intelligent network control.	Lack of deployed 6G testbeds, security of RIS/THz/NTN, standardization gaps.
Security	Zero trust access, secure identity, intrusion detection, blockchain audit.	Avatar impersonation, virtual object attacks, cross world authentication.
Privacy	Federated learning, differential privacy, local inference, consent dashboards.	Biometric leakage, motion/gaze inference, persistent tracking.
Digital trust	DID, provenance, governance, auditability, transparent policies.	Fragmented platforms, unclear liability, lack of user centred trust metrics.

Table 7 Thematic synthesis of opportunities and open challenges

6 DISCUSSION

The systematic synthesis suggests that AI driven cloud and 6G enabled metaverse systems should be designed as trustworthy cyber physical social infrastructures. The main contribution of this review is the integration of technical performance themes with security, privacy, and trust themes. Many earlier studies emphasize either metaverse architecture, 6G capabilities, cloud edge resource management, or security/privacy. This review combines these topics to show that performance and trust must be co designed.

A first implication is that metaverse quality of experience cannot be separated from the network computer data pipeline. Low latency requires 6G access, edge rendering, AI based orchestration, and efficient data compression. A second implication is that privacy cannot be solved only through encryption because metaverse platforms infer sensitive attributes from behavioral and spatial patterns. A third implication is that trust requires governance and accountability mechanisms across the whole ecosystem, including device manufacturers, cloud providers, application developers, network operators, and platform owners.

The review also identifies a methodological gap. Many articles propose architectures or taxonomies, but fewer provide reproducible datasets, benchmarks, or deployment results. As a result, conference papers in this area can contribute by proposing comparative testbeds, threat models, latency trust trade off evaluations, or privacy preserving analytics pipelines for a specific domain such as education, healthcare, industry, or smart cities.

7 RESEARCH AGENDA

Research direction	Possible contribution
Trust aware 6G metaverse architecture	Design a layered architecture combining 6G access, edge AI, cloud analytics, identity, and audit services.
Privacy preserving analytics	Develop federated or split learning pipelines for gaze, motion, and interaction data without centralized raw data storage.
Security threat modelling	Build attack trees for avatar impersonation, virtual object injection, edge node compromise, and AI manipulation.
Digital trust metrics	Propose metrics for explainability, consent, provenance, auditability, and user confidence in immersive systems.
Cross disciplinary applications	Evaluate cloud 6G metaverse systems in education, healthcare, smart manufacturing, agriculture, and disaster training.
Sustainable metaverse computing	Assess energy aware rendering, carbon aware cloud scheduling, and lightweight AI inference for immersive workloads.

Table 8 Future research agenda for conference level contributions

8 THREATS TO VALIDITY

This review has several limitations. First, the metaverse is a rapidly evolving field, and terminology varies across papers. Some relevant studies may use terms such as XR, digital twin, immersive internet, edge intelligence, or cyber physical social systems without explicitly using the word metaverse. Second, database search results can change because of indexing updates. Third, this conference version emphasizes qualitative synthesis rather than statistical meta analysis due to heterogeneity in methods and metrics. Fourth, the PRISMA screening log should be updated if the authors rerun searches immediately before submission. AI has transformed multiple application domains, including healthcare, engineering, finance, education, and scientific research, demonstrating its capability to automate complex processes and support intelligent decision-making [51-52].

CONCLUSION

This paper presented a PRISMA informed systematic review of AI driven cloud and 6G enabled metaverse research, focusing on big data analytics, security, privacy, and digital trust. The synthesis shows that AI, cloud edge computing, and 6G connectivity are mutually dependent enablers of immersive, real time, and scalable metaverse services. However, the same technologies also amplify risks involving biometric privacy, identity misuse, adversarial AI, platform fragmentation, and governance uncertainty. The most promising future research direction is the co design of performance, privacy, security, and trust across the device edge cloud network continuum. For conference research, strong contributions can emerge from reproducible architectures, privacy preserving analytics pipelines, 6G edge testbeds, and digital trust frameworks for specific metaverse applications.

REFERENCES

1. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline

for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71.
2. Moher D, Liberati A, Tetzlaff J, Altman DG. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med. 2009;6(7):e1000097. doi:10.1371/journal.pmed.1000097.
3. Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S. Systematic literature reviews in software engineering: a systematic literature review. Inf Softw Technol. 2009;51(1):7-15. doi:10.1016/j.infsof.2008.09.009.
4. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: EASE 2014; 2014. p. 1-10. doi:10.1145/2601248.2601268.
5. Wang Y, Su Z, Zhang N, Xing R, Liu D, Luan TH, et al. A survey on metaverse: fundamentals, security, and privacy. IEEE Commun Surv Tutor. 2023;25(1):319-352. doi:10.1109/COMST.2022.3202047.
6. Xu M, Ng WC, Lim WYB, Kang J, Xiong Z, Niyato D, et al. A full dive into realizing the edge enabled metaverse: visions, enabling technologies, and challenges. IEEE Commun Surv Tutor. 2023;25(1):656-700. doi:10.1109/COMST.2022.3221119.
7. Lee LH, Braud T, Zhou P, Wang L, Xu D, Lin Z, et al. All one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda. Found Trends Hum Comput Interact. 2024;18(2-3):100-337. doi:10.1561/1100000095.
8. Dwivedi YK, Hughes L, Baabdullah AM, et al. Metaverse beyond the hype: multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Int J Inf Manag. 2022;66:102542. doi:10.1016/j.ijinfomgt.2022.102542.
9. Dionisio JDN, Burns WG, Gilbert R. 3D virtual worlds and the metaverse: current status and future possibilities. ACM Comput Surv. 2013;45(3):1-38. doi:10.1145/2480741.2480751.
10. Mystakidis S. Metaverse. Encyclopedia. 2022;2(1):486-497. doi:10.3390/encyclopedia2010031.
11. Adil M, Song H, Khan MK, Farouk A, Jin Z. 5G/6G enabled metaverse technologies: taxonomy, applications, and open security challenges with future research directions. J Netw Comput Appl. 2024;223:103828. doi:10.1016/j.jnca.2024.103828.
12. Zawish M, Dharejo FA, Khowaja SA, Dev K, Davy S, Qureshi NMF, et al. AI and 6G into the metaverse: fundamentals, challenges and future research trends. IEEE Open J Commun Soc. 2024;5:730-778. doi:10.1109/OJCOMS.2023.3349465.
13. Chang L, Zhang Z, Li P, Xi S, Guo W, Shen Y, et al. 6G enabled edge AI for metaverse: challenges, methods, and future research directions. J Commun Inf Netw. 2022;7(2):107-121. doi:10.23919/JCIN.2022.9815195.
14. Saad W, Bennis M, Chen M. A vision of 6G wireless systems: applications, trends, technologies, and open research problems. IEEE Netw. 2020;34(3):134-142. doi:10.1109/MNET.001.1900287.
15. Letaief KB, Chen W, Shi Y, Zhang J, Zhang YJA. The roadmap to 6G: AI empowered wireless networks. IEEE Commun Mag. 2019;57(8):84-90. doi:10.1109/MCOM.2019.1900271.
16. Tataria H, Shafi M, Molisch AF, Dohler M, Sjoland H, Tufvesson F. 6G wireless systems: vision, requirements, challenges, insights, and opportunities. Proc IEEE. 2021;109(7):1166-1199. doi:10.1109/JPROC.2021.3061701.
17. Dang S, Amin O, Shihada B, Alouini MS. What should 6G be? Nat Electron. 2020;3:20-29. doi:10.1038/s41928-019-0355-6.
18. De Lima C, Belot D, Berkvens R, et al. Convergent communication, sensing and localization in 6G systems: an overview of technologies, opportunities and challenges. IEEE Access. 2021;9:26902-26925. doi:10.1109/ACCESS.2021.3053486.
19. You X, Wang CX, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci. 2021;64:110301. doi:10.1007/s11432-020-2955-6.
20. Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: vision and challenges. IEEE Internet Things J. 2016;3(5):637-646. doi:10.1109/JIOT.2016.2579198.

21. Satyanarayanan M. The emergence of edge computing. Computer. 2017;50(1):30-39. doi:10.1109/MC.2017.9.
22. Mao Y, You C, Zhang J, Huang K, Letaief KB. A survey on mobile edge computing: the communication perspective. IEEE Commun Surv Tutor. 2017;19(4):2322-2358. doi:10.1109/COMST.2017.2745201.
23. Vaquero LM, Rodero Merino L. Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev. 2014;44(5):27-32. doi:10.1145/2677046.2677052.
24. Armbrust M, Fox A, Griffith R, et al. A view of cloud computing. Commun ACM. 2010;53(4):50-58. doi:10.1145/1721654.1721672.
25. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener Comput Syst. 2009;25(6):599-616. doi:10.1016/j.future.2008.12.001.
26. Gandomi A, Haider M. Beyond the hype: big data concepts, methods, and analytics. Int J Inf Manag. 2015;35(2):137-144. doi:10.1016/j.ijinfomgt.2014.10.007.
27. Chen H, Chiang RHL, Storey VC. Business intelligence and analytics: from big data to big impact. MIS Q. 2012;36(4):1165-1188. doi:10.2307/41703503.
28. Chen XW, Lin X. Big data deep learning: challenges and perspectives. IEEE Access. 2014;2:514-525. doi:10.1109/ACCESS.2014.2325029.
29. Zhang X, Zhou X, Lin M, Sun J. Deep learning with edge computing: a review. Proc IEEE. 2019;107(8):1655-1674. doi:10.1109/JPROC.2019.2918951.
30. Kairouz P, McMahan HB, Avent B, et al. Advances and open problems in federated learning. Found Trends Mach Learn. 2021;14(1-2):1-210. doi:10.1561/2200000083.
31. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag. 2020;37(3):50-60. doi:10.1109/MSP.2020.2975749.
32. Abadi M, Chu A, Goodfellow I, et al. Deep learning with differential privacy. In: Proceedings of the ACM Conference on Computer and Communications Security; 2016. p. 308-318. doi:10.1145/2976749.2978318.
33. Shokri R, Stronati M, Song C, Shmatikov V. Membership inference attacks against machine learning models. In: Proceedings of the IEEE Symposium on Security and Privacy; 2017. p. 3-18. doi:10.1109/SP.2017.41.
34. Papernot N, McDaniel P, Jha S, Fredrikson M, Celik ZB, Swami A. The limitations of deep learning in adversarial settings. In: Proceedings of the IEEE European Symposium on Security and Privacy; 2016. p. 372-387. doi:10.1109/EuroSP.2016.36.
35. Biggio B, Roli F. Wild patterns: ten years after the rise of adversarial machine learning. Pattern Recognit. 2018;84:317-331. doi:10.1016/j.patcog.2018.07.023.
36. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy. 2017;41(10):1027-1038. doi:10.1016/j.telpol.2017.09.003.
37. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain based applications: current status, classification and open issues. Telemat Inform. 2019;36:55-81. doi:10.1016/j.tele.2018.11.006.
38. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of the IEEE BigData Congress; 2017. p. 557-564. doi:10.1109/BigDataCongress.2017.85.
39. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303. doi:10.1109/ACCESS.2016.2566339.
40. Porambage P, Gür G, Osorio DPM, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open J Commun Soc. 2021;2:1094-1122. doi:10.1109/OJCOMS.2021.3078081.
41. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy preserving schemes. J Netw Comput Appl. 2018;101:55-82. doi:10.1016/j.jnca.2017.10.017.

42. Roesner F, Kohno T, Molnar D. Security and privacy for augmented reality systems. Commun ACM. 2014;57(4):88-96. doi:10.1145/2580723.2580730.
43. Valluripally S, Gulhane A, Hoque KA, Calyam P. Modeling and defense of social virtual reality attacks inducing cybersickness. IEEE Trans Dependable Secure Comput. 2022;19(6):4127-4144. doi:10.1109/TDSC.2021.3121216.
44. Qamar S, Anwar Z, Afzal M. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. Comput Secur. 2023;128:103127. doi:10.1016/j.cose.2023.103127.
45. Zhao R, Zhang Y, Zhu Y, Lan R, Hua Z. Metaverse: security and privacy concerns. J Metaverse. 2023;3(2):93-99. doi:10.57019/jmv.1286526.
46. Singh A, Singh M, Kaur M, Attri V, Chauhan S, Kumar R. Architecting ethical and scalable artificial intelligence systems: a secure deployment model with real-world benchmarking. In: 2025 International Conference on Emerging Engineering Technologies and Applications (IC-EETA); 2025. p. 857-862. doi:10.1109/IC-EETA66496.2025.11548266.
47. Kaur M, Kaur S. Transformative role of artificial intelligence in engineering and finance: a comparative review. Int J Res Publ Appl. 2025. doi:10.1555/ijrpa.6192.
48. Jacob M, Sarala G, Natarajan K, Rajasekaran B, Naveenkumar R, Kaur M. Scalable big data and neural network architectures for integrative gene expression analysis in Parkinson's and Alzheimer's disease research. Genet Mol Res. 2026;25(1). doi:10.4238/6mx06z89.
49. Subashini AM, Bostani A, Wable TK, Aruna M, Nagalakshmi T, Kaur M. Quantum-integrated deep learning framework for large-scale gene expression analysis and predictive modeling of Parkinson's and Alzheimer's disease. Genet Mol Res. 2026;25(1). doi:10.4238/x1xkaz17.
50. Kaur DM. AI-powered user behavior analytics for fraud detection in consumer applications: a proactive security approach. Int Res J Mod Eng Technol. 2026;8(6):4951-4961. doi:10.56726/IRJMETS100968.
51. Akram W, Kaur M. AI-driven drug discovery: accelerating the search for new treatments. Int J Contemp Res Multidiscip. 2025;4(4):282-288. doi:10.5281/zenodo.16276691.
52. Kalam A, Kaur M. AI in higher education: transforming admissions, student advising, and research support. Int J Res Appl Sci Eng Technol. 2025. doi:10.22214/ijraset.2025.71728.

HOW TO CITE: Manpreet Kaur*, Sukhwinder Kaur, AI Driven Cloud and 6G Enabled Metaverse: A Systematic Review of Big Data Analytics, Security, Privacy, and Digital Trust, Int. J. Sci. R. Tech., 2026, 3 (8), 900-911. https://doi.org/10.5281/zenodo.22059517