ID	Method & data collection	Sample size	Population	Metaverse Context	Mentions risks	Main risks identified	Mentions strategies	Main strategies proposed	Significant findings	Major insights
P1	Literature review	66	Research papers about the metaverse	Metaverse	True	Personal data tracking Monitoring and surveillance Unathorized use of wearables Misuse of AIDigital currency theft	True	Confusion-based privacy Identity-based security scheme for avatars Use a "knocking-a- door" strategy	True	The Metaverse's features, such as sense of immersion, super spatiotemporality, sustainable development, as well as integration may make it hard to provide security in an acceptable manner A distributed Metaverse structure, which is selfsustaining and enduring, is required in order to eliminate the only failure problem and domination by a few strong units The privacy issue is one of the most important concerns for all in-Metaverse participants
P2	Literature survey		Research articles about AR/VR, 6Gand blockchain	Metaverse arquitecture	True	Smart-contract vulnerabilities Openness vs privacy	True	IP protected digital assets Scaling AR with blockchain Creating secure virtual worlds Universal file formatting	True	Smart Contracts, if executed in public environments, are vulnerable to contract-based attacks like gas attacks, re-entrancy attacks, dead code attacks, and many more The emergence of data-driven AR/VR applications forces networks to be highly resilient, massively connected, ultra-low latency, with real-time experience
P3	Literature survey (thematic analysis)		Research articles on the metaverse	Metaverse	True	Platformisation Data-driven corporate-led technocratic governance Business models of big data companies not aligned with user/consumer privacy protection Opaque AI models	True	Institutional measures and practices pertaining to Platformisation in order to address and overcome these concerns Regulate the Metaverse as a global process and practice of Platformisation democratically, ethically, and effectively through relevant social structures and institutions while understanding the key underlying mechanisms at work	True	The Metaverse raises critical concerns about the governance of urban society due to the logic of surveillance capitalism Surveillance capitalism leads to democratic backsliding, privacy loss, and freedom erosion Governments in democracies must employ new approaches when regulating long-lasting big data technologies and their escalating rate and scale of use based on deep analysis to avoid unexpected and potentially disastrous or lethal consequences in the long run.
P4	Literature survey		Research papers about the metaverse and healthcare	Metaverse and healthcare	True	Private data leakage AR/VR device malware attack		"Clone cloud" Quantum key distribution Privacy and security by design	True	The Metaverse is more prone to security threats because of the heterogeneous components involved in the patient healthcare system, providing security for user-sensitive information is the responsibility of the healthcare provider The security patches will enhance system security to some extent but the continuous cyber-physical attack on the Metaverse surface will lead to fragile patches
P5	Comprehensive (literature) survey	9	Survey papers on the metaverse	Metaverse security & privacy	True	Social engineering attacks User's network credential theft DDoS attack Ransomware attacks Identity theft attack Impersonation attack Avatar verification and validation issue Privacy leakage in data communication and processing Misuse of digital avatar Wearable devices key management	True	Blockchain Avatar confusion and private copies Heuristic greedy method for dynamic node blocking against physical, social, and information spreading threats Digital twins & Software-defined-networking Cloud-based privacy leakage forensics scheme Advanced threat detection methods Hash-chain-based aggregate digital signature Content sharing control mechanism Zero-knowledge proof-based blockchain scheme with privacy preservation Hierarchical game for	True	Lack of research papers on security and privacy issues related to metaverse applications Before any further development of metaverse applications and expansions in use cases, the possible security threats must be mitigated

								dynamic and optimized digital twins' synchronization Quantum random number generation (QRNG) and quantum key distribution (QKD)		
P6	Model proposal			Metaverse/XR device privacy and security	True	Re-identification attack Unadequate k-anonimity privacy guarantee	True	Gaze synthesis Conditional Variational Autoencoder (CVAE) model Kalɛido mechanism	True	As more sensors become available in the future, the ability and motivation for researchers to collect experimental data and release them publicly will also increase Attention data paired with content has the potential to violate privacy expectations concerning personalized ads, revealing biases, and identifying sexual orientation There is still a gap between the large body of work on using eye movements for sensitive characterisations in ideal lab conditions, and how frequently scenarios that produce these risks would arise in every day use ofXR
P7	Experimental evaluation			Metaverse/XR device privacy and security	True	Spatial privacy interference Intrinsic descriptor matching attack Deep learning / ML attack	True	3d point cloud data transformer that modifies spatial data - simple dot-product operations over random pairs of normal vectors Real-time inference risk assessment of spaces	True	Spatial privacy risk as the 3D sensors in commercially available handheld devices, such as smartphones and tablets, are continuously being improved Surface-to-plane generalisations are not sufficient defenses against spatial inference attacks
P8	Multi-perspective approach, bring together insights from an invited list of established researchers	35	Expert researchers on the field of the metaverse	Metaverse	True	Network attack Device (hardware) attack Software attack Database attack	True	Pseudonymisation/encryption of personal information Fine-grained authentication Security by design architecture Up to date security pacthes for devices Business continuity and disaster recovery plan	True	The safety and security aspects of the metaverse is an emerging research area where the exploitation of potential vulnerabilities in the virtual world could detrimentally impact users in the physical world Increased levels of sensitive data that is likely to be collected and used within the metaverse Several contributions reference the role of technology in the reinforcement of privacy and security within the metaverse
P9	Literature survey, model proposal		Research articles on the metaverse, previous Zero-Trust Architecture (ZTA) models	Metaverse security & privacy	True	Tracking user behavior Communication framework technical risks Psychological manipulation Impersonation Authentication Disambiguation	True	4 layer Zero-Trust Architecture Model: Verified and authenticated identities of users and other entities Using trusted third- party identity management services Providing users complete control over their privacy settings Pre-defined rules and regulations outlining acceptable behavior Use of Decentralized Oracle Networks (DONs) Continuous monitoring of user interactions in the metaverse using sentinels Computing and managing trust and reputation Ability to remove users from the metaverse based on the severity of the violation	True	Cyber–physical attacks are one of the major risks to the metaverse, among all other security issues Building very precise AI systems, such as face and speech recognition that can identify sophisticated physical infiltration and impersonation strategies using deep fakes and voice simulation, is necessary A metaverse subsystem's security protocols and firewalls must be built to anticipate cyber-attacks, such as Sybil and DDoS attacks
P10	Literature survey		Research papers about 6G/Tactile	Metaverse architecture	True	Denial of Service (DoS)Spoofing Eavesdroping	True	Encryption Authentication Authorisation Auditing	True	As a result of the resource-constrained devices in IoT environments, the majority of autonomous and semi- autonomous application services restrict security, authorisation and authentication mechanisms, among other things

			Internet							Security and privacy must be both end-to-end and lightweight for the intelligent network to communicate between the cloud, gateway, and sensors securely and efficiently
P11	Model proposal			Metaverse privacy and security	True	Distributed denial-of-service (DDoS) attacks Botnets Website fingerprinting Phising Sybil attacks Frauds Virtuality-reality synthesized threats	True	Cyberspace detection and response Scenario engineering Foundation models	True	The unprecedented complexity involving multiple spaces and their interactions necessitates a new paradigm to address security concerns The design principle behind ParaDefender is to make artificial and real cyberspaces executed in parallel to mutually guide each other for enhanced security Parallel execution is scenario-driven in the sense that the scenarios originate from all possible spatial–temporal combinations of security threats in the metaverse
P12	Literature survey		Research articles about the metaverse	Metaverse privacy and security	True	Injection attacks Man-in-the-middle attacks Cross site scripting Privacy leakage Insecure deserialisation Sensory data leakage Biometrics leakage Meta user relations Third-party tracking Cross-app tracking Virtual economy security Data security and privacy in digital twin Data poison	True	End user validation Strong authentication and cryptographic protocols Attack detection and monitor Deep learning-based detection Secure programming practice K-anonymity L-diversity Differential privacy Firewall Static scan End-to-end authentication protocol Two-factor or three-factor Authentication, local storage Graph-based framework for privacy preservation Differential privacy Third-party tracking/cross-app tracking analysis tools and detection algorithms Machine learning based blocking model Blockchain NFT Cryptocurrency Federated learning Reinforcement learning	True	Social engineering attacks will emerge more since more social communications are carried out in the digitized Metaverse Social security numbers, health records, passwords, or even virtual identity, will be harvested if the Metaverse residents have no precautions or awareness Since the Metaverse is open to everyone, legit or malicious, the "Darkverse" is expected to flourish too, as long as malicious users master the necessary technique The job market may face a crisis and transition once more; some current and traditional profitable jobs may be replaced
P13	Literature survey		Research papers about metaverse and blockchain	Metaverse architecture	True	AI bots Threats to personal identifiable information	True	Data ownership through public/private key cryptography Zero-knowledge proof Decentralized storage	True	A single human error, such as the loss of a private key, has the potential to compromise the security of blockchain technology and the privacy of data in the metaverse In the metaverse, attackers can easily target third-party applications since they tend to make use of inadequate security mechanisms, resulting in the compromise of personal information The adoption of blockchain technology can assist users in the privacy preservation of their dat
P14	Model proposal	39	University community participants	Metaverse/XR device privacy and security	True	Man in the middle attack Unsecure eye tracking configuration	True	Optical defocus	True	If a user is comfortable with a moderate level of security, they can use up to $\sigma = 3.50$ of defocus without a noticeable effect on the eye animation of their social virtual avatar Participants agreed that the avatar was truthful, eye movements were natural, the avatar paid attention to them, they were comfortable with the avatar, and maintained eye contact Significance testing found a decrease in all response values indicating participants did not have a negative experience, but less positive
P15	Model			Metaverse	True	Wormhole attack	True	Intrusion detection system	True	New design for securing IoT nodes against wormhole attacks

	development and simulation			security						WD-SPRT mechanism to determine wormhole nodes from the fluctuation of neighbors caused by wormhole attacks, and this concept works in cases with different situations As the number of nodes increases, the detection success rate of the proposed model rises, indicating that both sensitivity and specificity are excellent
P16	Threat model and system design testing and implementation			AR Privacy and Security	True	Visual privacy violations Third-party app developer who intentionally creates and distributes a malicious mobile AR application Hidden operations	True	Trusted verification and signing service for computer vision models Trusted computing partition on the local device in which to run the signed vision model Expanded permissions structure to communicate desired computer vision operations	True	There is no standardized way of measuring or representing the corresponding privacy sensitivity or security threat level associated with AR capabilities It is necessary to improve the understanding of end- user privacy preferences for these capabilities and the associated contexts under which an AR capability would be considered privacy- sensitive or not Improving the permissions structures of mobile operating systems as they relate to machine learning and computer vision operations remains an open problem
P17	Literature survey		Research papers about digital twins	Metaverse applications	True	Threats to Digital-Twins data communication links Data corruption Data theft	True	Data encryption Access privileges Source code Automated scanning Penetration testing Routine checkups Blockchain	True	The use case and services envisioned for the DT can dictate the architecture of the virtual twinDT could be used as an enabler of security in the communication between the physical twin and other cloud-based services, of which DTs might make use
P18	Literature survey into security taxonomy		Research articles on virtual environments security challenges	Metaverse/VR security and privacy	True	Network exploit Display exploit Audio exploit Sensor exploit Vision sensors exploit Auditory sensors exploit Haptic sensors exploit Olfactory sensors exploit	True	Authentication Intrusion detection Cyber risk assessment Privacy preservation	True	Lack of research stuying attacks that exploit behavioural similarity where the user is deceived by supposed functionality convention instead of or in addition to visual similarity Automated intrusion response as open area for further research. The only reactive measures proposed to date relate to intrusion detection, where a system has been designed to tell whether security has been breached Progress in VR cybersecurity is hampered by the lack of publicly available datasets of normal and attack behaviour as well as the lack of access to testbeds
P19	Survey	102	"Bystanders" from relevant XR-related subbreddits, XR discord groups, XR mailing lists, Facebook groups and Twitter	VR/AR/XR privacy	True	Identity, Anonymity and Biometric ID Mental Privacy - Behaviour, Internal State, and Biometric Psychography Physiological Privacy and Health Augmented Perception and Personal Surveillance Capture, Appropriation, and Alteration of Appearance Emergent and Future Processing Data Risks	True	Develop transferable privacy norms around AR Facilitate privacy-enhancing back-channel communications between AR users and bystanders Develop P2P architectures for conveying personal/social data Opt for an integrative combination of contextual permissions, considering shared privacy preferences if available, with the option for informed withdrawal or granting of consent Employ usable and user-centered measures when designing approaches for raising awareness and obtaining consent from AR bystanders	True	Respondents were frequently unaware of key 'risky' activities pertaining to bystander privacy Respondents opt-in/out preference varied significantly, influenced by activity type and relationship to AR user Respondents showed strong preferences towards awareness of the AR headset's activity Challenges: Awareness and Consent Versus State/Societal Needs and Legitimate Interests Contextual Integrity, Everyday AR and IoT Designing Privacy-Respecting 'Requisite' AR Headset Sensing Trust, Fairness, Accountability and Morality
P20	Model proposal			Metaverse privacy and security	True	Hacker alarm Malicious email Message attack Fraud conversation	True	Bridgehead strategy AI-based linguistic computing technology to effectively process big data	True	The proposed methodology proved to be effective in protecting users from malicious infiltration of hackers within the twin space Filtering performed well for topic classification, malicious group identification, dimension management, and token classification

										strategies
P21	Literature survey		Research papers about the metaverse and AI	Metaverse privacy and security	True	Zero-effort Statistical attacks Shoulder-surfing Spoofing attacks Password leaking Mimicking attacks Voice spoofing Eavesdropping Network discrepancy Packet loss Sniffing attacks DoS attack Sybil attack Competitive data theft Median filtering attack	True	Blinkey High-fidelity pose and expression normalisation (HPEN) Cybersecurity layer SVM GaitLock Hidden Markov model (HMM) People-Centric Security Framework Attack tree Gini and ABC Model Jamming-aided covert access	True	Hackers can also make use of AI to attack the Metaverse, various types of attacks have been described using AI algorithms in several papers While artificial intelligence and machine learning can help to guard against cyberattacks, hackers can defeat security algorithms by targeting the data they use To develop AI-based Metaverse cybersecurity, collecting and classifying data is an attractive idea, as implicit intelligence algorithms require large data sets
P22	Literature survey		Research articles about metaverse and extended reality security	Metaverse security and privacy	True	Data breaches Un- authorized access threats E- fraud Unavailability attacks Integrity violation Network attacks	True	Policy and consent compliance Meta-crime investigations Defense using blockchain Confidentiality Anti-harassment controls	True	XR Security awareness training must be conducted for stakeholders XR privacy policies and security standards must be well defined for all stakeholders The existing network security applications like intrusion detection and prevention (IDS / IPS) techniques, and firewalls are not interoperable with the latest extended reality and metaverse solutions XR developers must ensure end-to-end encryption when dealing with data in transit To mitigate the associated risks of technology, the minimal information required by XR systems must be quantified After the complete transition of various industrial sectors towards the XR and metaverse, a single network failure or internet dis-connectivity will shut down the entire XR ecosystem. Additional security and protective measures must be adopted.
P23	Model proposal			Metaverse privacy and security, authentication	True	Stolen smart devices attack Offline password guessing attack Impersonation attack Platform server spoofing attack Replay and MITM attack Perfect forward secrecy Insider attack Privileged insider attack Ephemeral secret leakage attack	True	Blockchain Elliptic-curve cryptography Biohashing	True	The proposed scheme is resistant to various security attacks such as stolen smart devices, offline password guessing, and impersonation attacks The proposed scheme offers a richer set of security features than the existing schemes
P24	Phenomenological research, in-depth interview, focus groups	19	Human-Computer interaction experts	Metaverse and education	True	Openess vs privacy Sensitive information collection	True	Learner control over data privacy Learner control about data collection Enhancing security awareness	True	Potential Cybersecurity Vulnerabilities are expected in the Metaverse, with a contradicting concept of openness versus privacy Security awareness should be raised within learners and institutions, while the Metaverse should account for the privacy of learners' data, with a clear consideration of data ownership Sensitive data should be encrypted and privacy strategies for personal information collected by Metaverse platform suppliers should be established
P25	Literature survey		Research articles on Tactile Internet	Metaverse IoT	True	Terminal attacks Data transmission attacks Data processing attacks Management shortcomings Privacy loss	True	Blockchain Edge/fog computing Machine learning Software-defined networking (SDN) based design	True	Conventional security policies are usually centralized and are not effective in maintaining the security of distributed and heterogeneous IoT systems
P26	Survey	259	Pokemon	Metaverse/XR	True	Poor privacy protection	True	Increase awareness	True	Users have increasingly been educated regarding privacy risks, but

	research		GO players	and videogames		behaviour Limited knowledge		Improve self-efficacy		many of them continue to share their personal and location data publicly The results from students in this study are also in line with past research stating that while adolescents have salient concerns about privacy, such concerns have no impact on their selfie-posting activities Players may fabricate their personal information, for instance, using a false name/ID or providing incomplete information about themselves mainly because they have privacy knowledge Players may seek more information about privacy such as reading the privacy statement provided by the site or asking somebody what they should do to protect their privacy because they have high self-efficacy, particularly in the group of fulltime employees that this link is stronger
P27	Literature survey		Research articles on blockchain and metaverse	Metaverse architecture	True	Access control attack Location and digital footprint tracking Malware attack End-device data leakage Firmware vulnerabilities DoS and DDoS attack Network intrusion Sybil attack Routing attack Eavesdropping and man-in-the-middle attack Malicious injection, tampering Third-party and SPOF issues Computation data leakage and inference attack Data provenance issues Poisoning attack Resource exhaustion attack	True	Blockchain-based secure access control system Malware detection scheme Secure firmware update Privacy for wearable devices Prevention of data tracking Access control with privacy Network intrusion detection Routing scheduling algorithm Sybil attack detection Authentication handover Physical layer security (PLS) Smart contract- b a s e d AI Poisoning attack prevention Edge resource allocation Privacy preservation for federated learning Data provenance protection	True	The integration of blockchain into the metaverse is crucial to ensure the decentralisation, security, and privacy of this virtual world For future research, the idea of a multiple- metaverse architecture based on blockchain interoperability could be developed further Open challanges related to security and privacy to look for: Cross-chain vulnerability Financial risks in MetaFiBlockchain scalability and cost The ever-growing ledger
P28	Model proposal			Metaverse privacy and security attack detection	True	Unauthorized access attack Denial-of-Service (DoS) attack	True	ML models for identifying zero-day attack events Faster attack detection Validation of security and privacy attacks impact on User Immersive Experience	True	As part of future work, studies can address security and privacy attacks that target the creation of cybersickness issues amongst users The proposed anomaly detection method involved two major techniques: (i) ML-based KNN classifiers for detection of network-based attacks, and (ii) Z- score based analysis for detection of application- based attacks
P29	Model proposal			Metaverse/VR Education security and privacy	True	Disorientation attack Physical collision attack Overlay attack DoS attack Data leakage Man-in-the-room attack Unauthorized access	True	Threat modelling using attack-fault trees Translation of AFTs into stochastic timed automata (STA) Application of hardening, redundancy and principle of least privilege design principles	True	The choice of a suitable design principle pertaining to the most vulnerable threat components is significant for use in an attack mitigation strategy Implementing a combination of design principles can result in a more effective mitigation strategy
P30	Literature survey		Research papers about the metaverse	Metaverse	True	Threats to authentication/key management procedures	True	Privacy preserving key management strategies and authentication Zero Knowledge Proof	True	Faster proof of work is a difficulty that needs to be resolved in order to increase the speed and scalability of data access In public blockchains, privacy protection measures could be studied, as data is accessible to all users, which could cause privacy

						User location tracker attack Compromised wearable sensor data				problems.
P31	Threat modeling, case study			Metaverse security and privacy	True	Man in the Room (MitR) attackVR Worm	True	Safe data manipulation and proper data sanitisation Secure authentication & authorisation Cautious handling of insecure API Integrity checking Enforcing VR state sharing Brute force protection Removing development relics	True	Requirements for a successful outbreak of VR worms and their botnets: Vulnerable persistent environment Functionality for duplication of a worm Communication channel MitR attack goals: Access targeted room Connect to multimedia protocol Hide presence
P32	Literature survey		Research papers about the metaverse	Metaverse and healthcare	True	Adversarial attacks Data integrity Untrustworty AI models	True	Zero-trust architecture Federated learning De-identified datasets	True	Privacy and confidentiality are of critical importance for MeTAI ('medical technology and AI') A well- designed MeTAI system with secure computing can utilize raw data without disclosing sensitive or private information MeTAI is subject to the same safety concerns as any other software or hardware products
P33	Literature survey		Research articles about the metaverse	Metaverse privacy and security	True	Threats to authentication and access control Threats to data management Privacy threats Network related threats Physical world threats Governance-related threats	True	Enhanced authentication and access control Secure data management Privancy enhancement Situational awareness Creator economy Physical safety and social management Digital governance	True	An example of endogenous security is the quantum key distribution (QKD), which utilizes channel-based secret keys to resolve information disclosure in wireless transmissions via quantum entanglement properties Quantum-resistant cryptography (QRC) for quantum secure metaverse applications is another promising research direction The orchestration ofcloud-edge-end computing offers a potential solution by collaboratively and dynamically sharing computation, communication, and storage resources among various entities Efficient metaverse specific consensus mechanisms, redesigned block structures, as well as well- designed user incentives are required for distinct metaverse applications
P34	Literature survey		Research papers about the metaverse	Metaverse economics	True	Code exploits Illegal services and shops Fake metaverses Technical support scams 3D social engineering	True	Metaverse data analysis Metaverse transaction regulation	True	Regulation and governance rules of DAOs may not cover all the risks and security issues in the metaverse Government should pay high attention to crimes against the metaverse, prevent them from happening, guide the development of a set of universally applicable industry standards for the metaverse, and implement blockchain-based industry autonomy
P35	Literature survey		Research articles about the metaverse	Metaverse architecture	True	Data leakage Unauthorised user data-access Voice spoofing Poisoning attack Inference attack	True	Trusted execution environment Federated learning Adversarial ML	True	In practice, however, the data of users may be stored in separate edge/cloud servers It is important to consider distributed storage solutions to ensure users can traverse the physical and virtual world The Metaverse can provide encrypted addresses and address-based access models for physical and virtual entities to anonymously request immersive streaming and synchronisation services