POLITECNICO DI TORINO
Repository ISTITUZIONALE

Security Model for an Economy-Enabling Metaverse

Original
Security Model for an Economy-Enabling Metaverse / Bosi, M., Cannavo', A., Chiariglione, L., Chollet, G., James Marshall, I., Kudumakis, P.. - (2026). (2026 IEEE 5th International Conference on Intelligent Reality (ICIR 2026) Pisa (ITA) June 25-26, 2026) [10.1109/ICIR70631.2026.11628404].

Availability:
This version is available at: 11583/3011531 since: 2026-05-28T17:07:48Z

Publisher:
IEEE

Published
DOI:10.1109/ICIR70631.2026.11628404

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright
IEEE postprint/Author's Accepted Manuscript

©2026 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collecting works, for resale or lists, or reuse of any copyrighted component of this work in other works.

(Article begins on next page)

18 November 2026

Security Model for an Economy-Enabling Metaverse

Marina Bosi, *Senior Member, IEEE*, Alberto Cannavò, *Member, IEEE*, Leonardo Chiariglione, Gérard Chollet, Iain James Marshall, Panos Kudumakis, *Senior Member, IEEE*

***Abstract*—This paper proposes a comprehensive security model developed by Moving Picture, Audio and Data Coding by Artificial Intelligence (MPAI) for the Metaverse Model -Technologies (MPAI-MMM-TEC). The model enables trustworthy participation in an interoperable, economy-supporting metaverse. Motivated by the limits of perimeter-based cybersecurity in immersive, multi-stakeholder environments, the model addresses metaverse-specific risks such as cross-world identity abuse, virtual asset and economic manipulation, fraud, and IP management. The design defines functional requirements and maps them to security capabilities. These include interoperable authentication and authorization, trust establishment, verifiable provenance and integrity (for media and assets), privacy-preserving data handling, and accountability mechanisms suitable for distributed interactions. The paper describes how MMM architectural components support secure participation and trustworthy trades between stakeholders. An initial implementation and preliminary assessment are presented to demonstrate feasibility and provide a baseline for future development.**

***Index Terms*—security governance, metaverse standards, virtual economy, zero-trust, MPAI, open simulator**

I. Introduction

Digital media ecosystems and modern business environments are evolving rapidly due to pervasive connectivity, cloud services, AI-driven content creation, and data-intensive platform models. While these advances create new opportunities, they also increase security risks such as identity compromise, data leakage, fraud, IP theft, service disruption, and regulatory non-compliance across complex multi-stakeholder supply chains. These challenges are even more critical in immersive environments like the metaverse, where users, devices, virtual assets, and services interact continuously across organizational and jurisdictional boundaries. The metaverse not only amplifies traditional threats but also introduces new risks, including cross-world identity abuse, manipulation of virtual goods and economies, making traditional perimeter-based security insufficient.

Addressing these issues requires a conceptual framework that enables secure identity trust establishment as foundational capabilities, while supporting interoperable authentication and authorization. In this paper, we present a novel and comprehensive security model design for the MPAI-MMM-TEC standard [1]. The proposed model aims to provide systematic security capabilities aligned with architectural components and interactions, supporting secure participation and trustworthy exchanges across metaverse stakeholders without assuming specific technologies, see Figure 1.

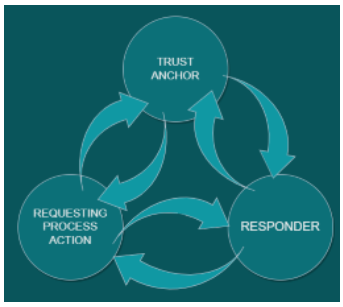


Fig. 1. MPAI-MMM-TEC Model.

The remainder of the paper is organized as follows. Section II reviews the background and current state of the art, while Section III introduces the foundational elements of the MPAI MMM-TEC framework. Section IV outlines the functional requirements for a secure, economy-enabling metaverse platform. Section V presents the proposed security model tailored to the MPAI MMM architecture, and Section VI describes its basic implementation. Section VII reports encouraging results, and Section VIII concludes the paper and discusses directions for future work.

II. Related Work

The metaverse is a technology that promises to make many tasks more effective, but its adoption, especially by organisations, is also exposing users to new security vulnerabilities that cannot be fully overcome using traditional cybersecurity models [2]. According to a recent analysis of the related literature published in [3], security in the metaverse is a research area that is actively emerging but not yet well-matured. Multiple surveys, such as [4]–[6], provide broad taxonomies of threats and possible countermeasures, thus showing that security is recognized as a key research topic. However, these works also consistently note that, despite growing interest, security and privacy research lags behind metaverse technological development and deployments [4]. In addition to well-known issues not strictly related to the metaverse, such as the lack of comprehensive studies, particularly for AI-driven

M. Bosi is with the Center for Computer Research in Music and Acoustics (CCRMA), Stanford University, Stanford, CA 94305 USA (e-mail: mab@ccrma.stanford.edu).
A. Cannavò is with Dept. of Control and Computer Engineering, Politecnico di Torino, Turin, Italy (corresponding author e-mail: alberto.cannavo@polito.it).
L. Chiariglione is with MPAI – Moving Picture, Audio, and Data Coding by Artificial Intelligence, Geneve, Switzerland (e-mail: leonardo@chiariglione.org).
G. Chollet is with CNRS-SAMOVAR, Institut Polytechnique de Paris, Paris, France (e-mail: gerard.chollet@telecom-sudparis.eu).
I. J Marshall is with the Institute Mines Telecom (IMT) and CEO of Amenesik SARL, Evry, France (e-mail: ijm@amenesik.com).
P. Kudumakis is with Standardisation Expert, London, United Kingdom (e-mail: panos@ieee.org).

and biometric-heavy systems, aimed at validating proposed solutions [6], [7], this domain also presents new challenges that are still only partially addressed.

Among the numerous challenges facing metaverse security, the unavailability of standardized models is repeatedly cited, in the literature, as a major research gap [4], [8], [9]. Several studies have attempted to address this gap by proposing different approaches and technologies. For instance, a zero-trust–based metaverse security architecture is proposed in [9]. This approach emphasized continuous authentication, least privilege, and user data control. Similarly, in [10], continuous biometric verification in social Virtual Reality applications is proposed to enforce a zero-trust authentication scheme. The authors in [11] propose a five-domain cybersecurity framework based on identity, data privacy, device/network, digital assets, and user education that was tailored to metaverse ecosystems. Another approach, considered a potential new direction for future applications, is leveraging the "secure-by-design" paradigm, i.e., embedding self-protection mechanisms and quantum-resistant cryptography into the metaverse infrastructure [4], [12]. An authentication scheme based on gamification and asymmetric cryptography is proposed in [13] to support the creation of breakout rooms in the metaverse that can only be accessed by mutually authenticated users. Works such as [6], [14] propose mechanisms driven by artificial intelligence for intrusion detection, and blockchain-based solutions for asset protection, within layered metaverse architectures.

Despite the heterogeneity of approaches and technologies, and the multiplicity of candidate solutions that current work offers, none has yet become a universally accepted, formal standard [12]. There are several reasons why a standardized security model has not yet emerged. First, the metaverse itself is not yet clearly defined or standardized [15]. Its architecture, scope, and even the criteria for what qualifies as a "metaverse" remain unclear, making it difficult to formalize a single, stable security framework.

Moreover, metaverse environments are built upon extremely heterogeneous technological stacks that integrate Extended Reality, Internet of Things, edge and cloud computing, 5G/6G networks, artificial intelligence, blockchain, digital twins, and NFT infrastructures. Each underlying technology is characterized by distinct standards, trust assumptions, and threat models. Unifying these diverse components into a single security paradigm is therefore technically complex [4].

Aspects such as interoperability and decentralization further deepen this challenge, as cross-platform identity management, digital asset ownership, and data exchange still lack common protocols and shared governance mechanisms, leading to security requirements that vary across platforms and countries [16], [17].

In addition, the industry ecosystem remains fragmented, with vendors promoting proprietary solutions and open standardisation initiatives (e.g., ISO, IEEE, OpenXR, and the Open Metaverse Interoperability Group) progressing slowly [12].

Finally, many commercial platforms have historically prioritised rapid growth, user experience, and monetisation, often retrofitting security and safety mechanisms rather than adopting a secure-by-design approach from the outset [18].

In this context, this paper introduces a novel and comprehensive security model tailored to the MMM-TEC standard. The proposed framework is designed to systematically embed security mechanisms into the architectural components and interaction flows defined by MMM-TEC, addressing the current lack of standardized solutions.

III. Foundational Elements of MMM-TEC

The MPAI-MMM-TEC V2.2 defines a Metaverse Instance (M-Instance) as a virtual entity populated by Processes that may interact with one another, as well as with Processes in other M-Instances and the Universe [1]. Processes that represent, and are under the responsible control of, a human are referred to as Users [19].

The interaction between Processes within M-Instances takes the form of Actions. The interaction with the Universe involves bidirectional communication between Universe objects and their M-Instance counterparts. This may involve either Universe object detection and reproduction in the M-Instance, or M-Instance object actuation in the Universe.

Processes requiring the assistance of other Processes invoke Process Actions (PA) [19]. A distinct workflow is specified for each PA thus ensuring the robustness of the transactions occurring between PA initiators and the involved Metaverse/Universe elements. Processes intercommunicate through message exchange. Message payloads may also include Data Exchange Metadata [20] describing the legal, security, and rights pertaining to the data, the source and destination processes.

The activities carried out by the M-Instance Processes are governed by both the Rights and the M-Instance Rules. The Rights describe permissions, obligations, and prohibitions pertaining to the PAs performed on Items, where Items represent perceptible or abstract objects in an M-Instance see also [19]. The M-Instance Rules are Rights that are applicable to classes of Processes and Items within that M-Instance. By defining Rules, an M-instance is able to influence the Data Exchange Metadata to be attached to a PA payload, or the level of control that it wishes to exert over Process activities. For instance, it may decide to record Activity Data, i.e., all PAs performed by classes of Processes. The Rules of an M-Instance shall also indicate the Penalties to be incurred by infringing Processes.

This approach offers a novel, standardised contribution to both Metaverse interoperability and security. These new elements distinguish MMM-TEC V2.2 from the previous version. The PAs indicate the type of interaction between Processes. The exhaustive list of PAs is shown in Table I. Actions indicate the scope of operations available to a Process, while Items represent the entities over which a Process may act. Examples of Actions and classes of Items specified in MMM-TEC are shown in Table II.

TABLE I
LIST OF PROCESS ACTIONS USED IN MMM-TEC [21].

Function	PA	Function	PA
Communicate	MM-Send	Import	UM-Capture
	Resolve		UM-Send
Economy	Post	Information	Authenticate
	Transact		Discover
Execute	Execute		Interpret
Export	MU-Actuate	Item Manage	Author
	MU-Add		Convert
	MU-Animate	Locate	MM-Add
	MU-Move		MM-Animate
	MU-Send		MM-Capture
Identity Manage	Hide		MM-Move
	Identify		Property Change
	Modify	Rights Manage	Rights Change
	Register		Validate

TABLE II
SELECTION OF ITEM CATEGORIES OF MMM-TEC [22].

Category	Item	Category	Item
General	Capabilities	Finance	Provenance
	Item		Fault Behaviour Report
	M-Instance		Fault Detection Report
Processes & Actions	Process Action		Licence
	Event		Service Pricing Model
	Right		Wallet
	Rule	Perception	3D Model Object
Human&User	Account	Internal State	Cognitive State
Space&Time	Time		Emotion
	Position		Social Attitude

IV. FUNCTIONAL REQUIREMENTS FOR AN ECONOMY-ENABLING METAVERSE

The latest MMM-TEC specification (version 2.2 [1]) builds on elements of previous MMM-TEC specifications [19] to explicitly support the operation of a virtual economy. Five categories of functional requirements have been identified for MMM-TEC V2.2. The first category implies that a Process claim to hold Rights on a digital asset can be verified and is defensible. This requirement involves maintaining authoritative and tamper-evident records that document an Asset's entire lifecycle, including its creation, authorised modifications, and any Right assignment. To ensure these Assets remain valuable across the ecosystem, an M-Instance must support interoperable, standard-conformant proofs that a Process holds Rights to an Item and that an Item contains undisputable proof of the Processes holding Rights to it, and that the Rights are valid across different M-Instances while strictly enforcing integrity to prevent unauthorised duplication or alteration of Assets. The second category focuses on maintaining stable and transparent virtual economic operations through consistent and predictable governance. An M-instance must define and apply clear Economic Rules regarding Asset exchange, scarcity, and value-related metadata to ensure all participants understand the market landscape. Furthermore, any modifications to these Rules must follow a transparent process, protecting the economic mechanisms from unauthorised interference while supporting the active detection and reporting of any economic irregularities. The third category concerns robust safeguards against fraud and misrepresentation to protect the community from bad actors. This requires that the architecture support specialised mechanisms to detect and signal deceptive or non-compliant behaviour, ensuring that any transaction violating established validity Rules is blocked from finalisation. Additionally, the system must provide interoperable interfaces for users to report suspected fraud and supports formal investigation and enforcement processes as defined by the overall security governance. The fourth category concerns the need for transparent and trustworthy financial transactions that prioritise Action clarity and auditability. Before any Transaction is executed, an M-Instance must provide Users with complete, standardised pre-execution disclosures so they fully understand the exchange. All Transaction records must be kept in a standard-specified format to allow for auditing, ensuring that outcomes are deterministic and verifiable while using transparent semantics to prevent hidden or ambiguous financial flows. Finally, the fifth category mandates that marketplace operations be authentic and trustworthy by verifying the legitimacy of all Users and Assets. Marketplaces must use standard-defined metadata to confirm the authenticity of digital goods, services, and sellers, while ensuring that all listings meet strict accuracy and disclosure requirements. To maintain its integrity, an M-Instance must block the distribution of Items that violate Rules and monitor marketplace behaviour to report and address non-compliant activities.

V. SECURITY MODEL FOR MMM-TEC

~~This section provides a high-level description of the MMM-TEC V2.2 specifications explicitly designed to support the identified functional requirements that enable economic activities within and across independently designed MMM-TEC conforming M-Instances~~. Formal definitions of terms can be found in MMM-TEC [1]. An Asset is an Item intended for Transaction that includes Identifier, Capabilities, Rights held by Processes, and Traceability – name of Process producing it and Time of production – but also the Identifier of the Item that spawned it, the Provenance – the list of all Transactions executed on an Asset, first and last included – and Economic Metadata – Market Classes, Value Metadata IDs, Currency, Service Pricing Model, Marketplace Policy IDs. All Rules – those with an economic impact included – carry a Version ID and an Effective Time condition.

Rules that may be established by an M-Instance include:

1) The carriage of Version ID and Effective Time condition.
2) The procedure whereby the Rules may be changed and a new Version is made effective.
3) The procedures for the investigation or enforcement of compliance with the Rules of an M-Instance.
4) The procedure used by a Process to modify its Capabilities, e.g., its own economic Rules.
5) Statistical information about the number of Assets available in a Market Class, relationship between supply and demand, frequency of time-dependent Asset exchange, and average price movement.
6) Disclosure of conflicts of interest affecting fees, rankings, or visibility.

7) Procedures for pausing markets, rolling back affected Transactions, and communicating incident status to par-
8) The types and number of Messages that a Process may send to a Centralised or Distributed Service.
9) The degree of control applied to the Actions performed by a Process (full, random, or no control) and, in case of the random selection, the selection criteria.
10) How Activity Data is recorded and In which conditions an Action can be recalled.
11) The sanctions for infringing Actions.
12) The ability of a Process to view the Rights of a Process or an Item.
13) The rendering of and access to the Identity associated with an activated Persona.
14) The conditions under which access to the Personal Profile is permitted.

MMM-TEC does not specify how an M-Instance verifies that a Process's Process Actions are compliant with the Process's Rights or the M-Instance Rules. An M-Instance may decide to verify the full set of Activity Data, to make verifications based on claims by a Fault Behaviour Report generated by a User, to make random verifications, or to not make any verification at all. The result of a verification can be recorded as Activity Data. Enforcement actions following verification are themselves Actions governed by Rights and recorded as Activity Data when required by the Rules. A Process in one M-Instance may use its local M-Instance's Resolution Service to establish a multi-M-Instance session with other Processes in other M-Instances at the same or different times. MMM-TEC V2.2 extends the support of Resolve Service to economic activities. When a Resolve Service session is active, each M-Instance shall

1) Treat Items and Assets originating from other M-Instances as if locally originated
2) Assess the Actions of a Process based on its Rules

on condition that the M-Instances involved in the Resolve session are bound by a governance/trust agreement and Items and Processes have globally unique Identifiers: the external M Instance. If a Process from a foreign M Instance does not comply with the Rules of the local M Instance, this may submit a Fault Detection Report to the M Instance to which the non-compliant Process belongs. The M-Instance and any connected M-Instances shall be informed of any Hidden Process or Item.

A Transaction Item controls the transfer of Value (an Amount expressed in a Currency) between Users, caused by the assignment of Rights by a User1 to another User2 possibly because of a Licence granted by User1 to User2. Various competing Transact Services can coexist but are bound to the use of standard Protocols. The Capabilities of a Transact Service shall disclose the currency it operates with, the fees it applies, and the Service Pricing Model relevant to a Transaction.

Transact is the Action of a User1 ("sender") requesting that a Transact Service cause changes to the Wallets of User2 ("receiver") and, if applicable, of Service Provider(s), as determined by the Transaction. A Transact Service provides the Provenance associated to the Asset being Transacted upon request of one of the Transaction parties. The Capabilities of a Transact Service include the information made available to the parties in a Transaction before executing it. Before executing a Transaction, a Transact Service makes available a Pre-Execution Disclosure – a description of the proposed Transaction – to the parties in the Transaction. A Fault Behaviour Report may be used by a User to report suspected faulty, fraudulent, deceptive, or otherwise non-compliant activities. A Marketplace Service publishes accuracy and disclosure requirements in its Capabilities.

MMM-TEC V2.2 specifies protocols enabling Process1 to request Process2 to perform a Process Action (PA) Request for a service that may be free or pay. If pay, Process1 sends its service subscription terms documented in an Service Pricing Model (SPM). The protocol allowing a Process to request a Locate Service (managing the perceived space of an M-Instance) consists of two elements:

1) Capture the portion of a Location taken from a Point of View that is comprised in a given Field of View with the Right to use it (Status=Model).
2) Grant Rights (Status=Final) to the MM-Captured Audio-Visual Scene based on the requested Rights, if the request is accepted.

Detailed specifications can be found in [1].

VI. Implementations

The high-level security architecture comprises two distinct and independent layers, the Security Governance Layer and the Security Enforcement Layer.

The centralised, yet distributed, system of security governance will be responsible for the management of all standardised Identities (H-User, A-User, M-User) and their associated standardised Rights. This governance will provide the means for the handling and storage of all life cycle events relating to each Identity, and their associated Rights, as they are created, deployed, updated and deleted, through the period of their validity for use within the metaverse platforms and systems for which they are required.

The security governance will ensure timely deployment, distribution, communication of this standardised Identity and Rights information, through certified governance connectors, to the Enforcement service components of each of the collaborating metaverse platforms.

The Enforcement services of the individual metaverse platforms are responsible for the application of these received Identities and Rights allowing authorisation and performing enforcement for all Actions performed within the corresponding metaverse, under their responsibility.

The diagram in Figure 2 depicts the relationship between the collaborating metaverse platforms, the security governance and the metaverse specific security enforcement services.

A. Unity

This implementation provides the functional foundation upon which the broader security framework could operate.

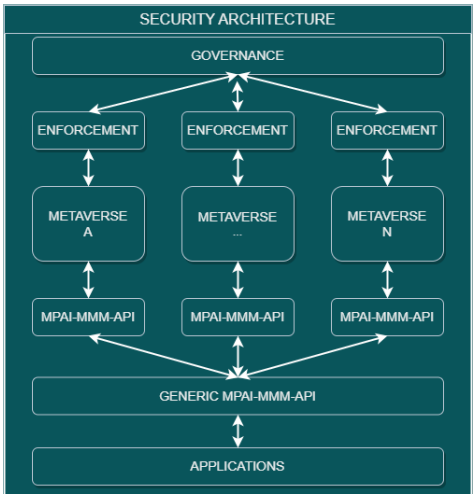


Fig. 2. Security architecture.

For instance, the Web Server and MMM-APIs may interface directly with the Security Governance Layer to validate the standardized Identities interacting with the system. Consequently, every interaction happening in the MMM-Clients and Metaverse can be subjected to the Security Enforcement Layer, which acts as a gatekeeper to verify that each action aligns with the specific Rights and Identities assigned by the governance system.

B. Open Simulator

The diagram in Figure 3 depicts the integration architecture of the MMM-TEC implementation for the OPEN SIMULATOR.

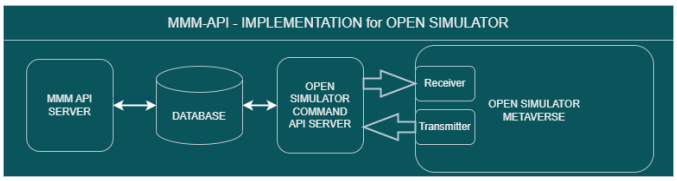


Fig. 3. Implementation of MMM-API for OPEN SIMULATOR.

The MMM-API server is listening for incoming requests from remote metaverse and other MMM-API enabled clients. These requests are processed to update the corresponding MMM-TEC metaverse object descriptions in the database and the corresponding commands for the update of the OPEN SIMULATOR metaverse. Suitably enabled RECEIVER objects, instantiated in the metaverse, issue requests for state update to the OPENSIM API server and processes the subsequent commands received and create, update or delete the corresponding IN WORLD items. Suitably enabled TRANSMITTER objects, instantiated in the metaverse, issue requests to the OPENSIM API server to update MMM-TEC metaverse object descriptions in the database to reflect changes occurring IN WORLD.

VII. Evaluation

An experimental evaluation was conducted to assess the overhead introduced by the MPAI-MMM-TEC layer via the MMM-API. During the experiment, two types of metrics were collected. The first metric (T) measures the total latency elapsed between issuing a request and receiving the corresponding response. The second metric accounts for the data volume (in bytes) of the packets exchanged between the Source and Destination Processes, specifically for the PA Request (D_1) and the PA Response (D_2). Metrics have been collected during the workflow that implements the Post Protocol, i.e., a sequence of actions to allow a User to post an Asset at the Marketplace. The sequence includes the following elementary steps: i) The user makes a Transaction to the Marketplace, paying the amount requested for posting an Asset at the Marketplace; ii) the RightsChanges PA is invoked to grant the User the Right for posting the Asset at the Marketplace, and iii) the User sends a PostPARequest including the Asset and a ServicePricingModel.

The experimental setup involved hosting the MMM-API on the Microsoft Azure Web App Service and the database on MongoDB Atlas to replicate realistic network conditions. More specifically, the MMM-API was deployed on a web server running in a Windows-based environment within the West Europe region, using the Azure Free (F1) App Service plan. The database was also hosted in the West Europe region, leveraging the MongoDB Atlas Free Tier.

For the client-side execution, the Swagger UI interface was employed to generate PA Requests and visualize the corresponding responses. To ensure a comprehensive evaluation of the network traffic, measurements were captured using the Wireshark network protocol analyzer [1]. The communication relies on the TCP transport protocol, with an application-layer security provided by TLSv1.3. This configuration allowed the study to account for the modern encryption overhead and the specific handshaking latency characteristic of secure, cloud-based architectures.

Table III presents the mean values and standard deviations for the performance metrics, calculated over 10 independent executions of the Post Protocol workflow.

The results indicate that the evaluated operations introduce only a modest latency overhead, remaining below 0.1 seconds on average despite deployment on cloud infrastructure. Among these operations, rights updates exhibit the highest latency, while POST requests for Assets and ServicePricingModels show slightly lower response times. In terms of data exchange, requests related to ServicePricingModels are associated with larger payloads.

VIII. Conclusions and Future Work

This paper has presented a comprehensive security model for MMM-TEC, specifically designed to support trustworthy, interoperable, and economy-enabling metaverse ecosystems.

[1] Wireshark: https://www.wireshark.org/

TABLE III
LATENCY AND DATA VOLUME ANALYSIS PER HTTP REQUEST

HTTP Request	$T(s)$	$D_1(bytes)$	$D_2(bytes)$
POST *api/Transactions*	0.0729 (0.0207)	14,297	6,723
UPDATE *api/Rights*	0.0960 (0.0103)	1,763	245
POST *api/ServicePricingModels*	0.0547 (0.0187)	23,903	1004
POST *api/Assets*	0.0554 (0.0202)	17,314	1,414

By embedding security as a foundational architectural property rather than an external add-on, the proposed MMM-TEC framework enables secure identity management, rights-based authorization, trustworthy transactions, verifiable asset provenance, and transparent governance across heterogeneous -albeit MMM-TEC compliant- instances.

The model introduces a unified conceptual structure based on Processes, Items, Rights, and Rules, enabling fine-grained control, auditability, and accountability of all interactions. Through the separation between governance and enforcement layers, and the integration with real-world platforms such as OpenSimulator and Unity, the proposed architecture demonstrates the feasibility of standardised, policy-driven security enforcement in multi-instance, cross-domain metaverse environments.

The performance analysis indicates that the MPAI-MMM-TEC layer introduces only a modest overhead, supporting its suitability for practical deployment. This makes the work a concrete step toward addressing the lack of formal, standardized security models in current metaverse developments.

Several directions for future research emerge from this work. Firstly, the current framework should be tested to validate a broader set of market-oriented use cases underlining the pertinence of the model in complex economic scenarios. In parallel, further use cases related to the core concepts of the paper—such as inter-verse asset trading, interoperable digital marketplaces, and distributed service orchestration—should be specified. From the security perspective, we are focusing on strengthening the robustness of enforcement mechanisms by completing the development of a new standard of which the Data Exchange Metadata is already a component. Future work should also address the definition and management of Profiles, explicitly avoiding recursive dependencies, in order to improve identity handling and policy expressiveness. Finally, the applicability of the proposed standard in real commercial contexts will be investigated, in collaboration with stakeholders, to assess performance, adequacy, scalability, and integration with existing enterprise systems.

ACKNOWLEDGMENT

The authors would like to acknowledge the contribution of people from different MPAI groups that have contributed to make the MPAI-MMM-TEC standard possible. MMM-TEC has been developed by MPAI and its scope falls within the activities being carried out to further develop IEEE Digital Reality (https://digitalreality.ieee.org/).

REFERENCES

[1] MPAI, "MPAI Metaverse Model (MPAI-MMM)-Technologies (MMM-TEC) V2.2," https://tinyurl.com/385xpkru, accessed: 2026-04-30.
[2] S. Vasudevan, A. Piazza, L. Rajendran, and S. Duraivel, "Mapping the metaverse minefield: a tips framework for security-conscious business adoption," *Computers & Security*, p. 104710, 2025.
[3] K. Kostelić and D. Etinger, "Securing the metaverse: A bibliometric analysis of cybersecurity challenges and research trajectories," *IEEE Engineering Management Review*, vol. 53, pp. 93–109, 2025.
[4] Y. Wang, Z. Su, N. Zhang, D. Liu, R. Xing, T. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Communications Surveys & Tutorials*, vol. 25, pp. 319–352, 2022.
[5] M. Pooyandeh, K. Han, and I. Sohn, "Cybersecurity in the ai-based metaverse: A survey," *Applied Sciences*, 2022.
[6] Y. Otoum, N. Gottimukkala, N. Kumar, and A. Nayak, "Machine learning in metaverse security: Current solutions and future challenges," *ACM Computing Surveys*, vol. 56, pp. 1 – 36, 2024.
[7] A. Awadallah, K. Eledlebi, M. J. Zemerly, D. Puthal, E. Damiani, K. Taha, T.-Y. Kim, P. D. Yoo, K.-K. R. Choo, M.-S. Yim, and C. Yeun, "Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 27, pp. 1008–1052, 2025.
[8] N. Ramolia, P. Tank, R. N. Ravikumar, B. Zeb, M. Kumar, and S. Singh, "Futuristic metaverse: Security and counter measures," *ICCK Transactions on Intelligent Systematics*, 2025.
[9] S. Sharma, J. Singh, A. Gupta, F. Ali, F. Khan, and D. Kwak, "User safety and security in the metaverse: A critical review," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 5467–5487, 2024.
[10] R. Cheng, S. Chen, and B. Han, "Toward zero-trust security for the metaverse," *IEEE Communications Magazine*, vol. 62, pp. 156–162, 2023.
[11] M. Alauthman, A. M. Ishtaiwi, A. A. Maqousi, and W. Hadi, "A framework for cybersecurity in the metaverse," *2024 2nd International Conference on Cyber Resilience (ICCR)*, pp. 1–8, 2024.
[12] M. Z. Aloudat, M. Barhamgi, E. Yaacoub, and D. Aoun, "Security in metaverse markets: Challenges and solutions—a comprehensive review," *Expert Systems*, vol. 42, 2025.
[13] F. De Lorenzis, A. Visconti, M. Marani, E. Prifti, C. Andiloro, A. Cannavò, and F. Lamberti, "3dk-reate: Create your own 3d key for distributed authentication in the metaverse," in *2023 IEEE Gaming, Entertainment, and Media Conference (GEM)*. IEEE, 2023, pp. 1–6.
[14] V. T. Truong and L. B. Le, "Security for the metaverse: Blockchain and machine learning techniques for intrusion detection," *IEEE Network*, vol. 38, pp. 204–212, 2024.
[15] A. Cannavò, A. Visconti, L. Chiariglione, P. Kudumakis, G. Chollet, H. Sansen, P. Menezes, and F. Lamberti, "Implementing the mpai metaverse model architecture," in *2025 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 2025, pp. 490–494.
[16] S. Qamar, H. Tahir, Z. Anwar, N. Ahmed, S. Tahir, and M. Aleem, "A defensive model and implementation baseline for the metaverse and extended reality systems," *PeerJ Computer Science*, vol. 11, 2025.
[17] M. Tukur, J. Schneider, M. J. Househ, A. H. Dokoro, U. I. Ismail, M. Dawaki, and M. Agus, "The metaverse digital environments: a scoping review of the challenges, privacy and security issues," *Frontiers in Big Data*, vol. 6, 2023.
[18] S. Liu, "The security challenges of the "metaverse"," *Secur. Saf.*, vol. 2, p. 2023010, 2023.
[19] L. Chiariglione, A. Cannavò, G. Chollet, P. Kudumakis, H. Sansen, M. Bosi, and P. Menezes, "A metaverse standard based on ai data coding," in *2025 IEEE 4th International Conference on Intelligent Reality (ICIR)*, 2025, pp. 1–9.
[20] MPAI, "MPAI-AIF V3.0 Data Types – Security Technology Taxonomy," https://tinyurl.com/32manrps, accessed: 2026-04-29.
[21] MPAI, "MMM-TEC V2.2 – Process Actions," https://tinyurl.com/yedzbsmk, accessed: 2026-04-30.
[22] MPAI, "MMM-TEC V2.2 – Items," https://tinyurl.com/2txdj7k2, accessed: 2026-04-30.