2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)

2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT) | 979-8-3503-4649-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/DCOSS-IOT58021.2023.00086

Trusted Virtual Reality Environment for Training Security Officers

Anastasios Pantazidis[1], Alexandros Gazis[1], John Soldatos[1], Marios Touloupou[1,2], Evgenia Kapassa[1,2], Sophia Karagiorgou[3]

[1] Research and Development, INNOV-ACTS Limited, Nicosia Cyprus,
{tpantazidis, agazis, jsoldat, mtouloupou, ekapassa}@innov-acts.com
[2] Department of Digital Innovation, University of Nicosia, Cyprus,
{touloupos.m,kapassa.e}@unic.ac.cy
[3] AI/ML Department, UBITECH Limited, Limassol, Cyprus,
skaragiorgou@ubitech.eu

***Abstract*—Virtual Reality (VR) applications are increasingly used to support ergonomic and safe training activities, including serious games for training security officers and other security related professionals. Nevertheless, they do not exploit opportunities for trusted and secure management of digital assets, which are typically offered by the blockchain infrastructures of emerging metaverse environments. This paper introduces a novel interactive and realistic VR-based serious game for training law enforcement officers in the analysis and understanding of terroristic activities. The game is driven by pragmatic models of terroristic actions and teaches its users how to predict and anticipate indicators of terroristic attacks. It also provides the means for generating datasets to train Artificial Intelligence (AI) modules that could help analyzing and predict potentially terroristic activities. Moreover, the paper provides an outlook for the evolution of the game in metaverse environments, where blockchain infrastructures can be used to both boost the cyber-resilience of the game and to safeguard the trustworthiness of the data generation process.**

Keywords*— *Virtual Reality, training, security, law enforcement, blockchain, metaverse, serious games

I. Introduction

Serious games have been introduced in the literature and are used for training purposes in various sectors including human resources [1], vocational training [2], healthcare [3], emergency management [4], and security [5]. Security games have been developed as a result of many cybersecurity training objectives, including cybersecurity awareness [5], and forensics [6]. Many security games are implemented in Virtual Reality (VR) environments and offer ergonomic VR interfaces [7]. This is very typical in the case of training complex security processes like emergency management and critical infrastructure protection [8], [9]. Moreover, VR platforms have been developed to train Law Enforcement Agencies (LEAs) in various security processes and environments (e.g., [10], [11]). VR gaming environments are well suited to LEAs training, as they enable the simulation of security and law enforcement scenarios in physical settings like urban environments. VR games boost the safety and cost-effectiveness of training activities, given that they obviate the need for training users in harsh and complex field training environments, which is quite expensive and associated with safety risks.

The analysis and prediction of terroristic activities are among the most challenging security processes that are hardly addressed by state-of-the-art VR training games. One of the main challenges relates to the proper modeling of such activities. Terroristic modelling has been addressed by security and counter-terrorism researchers based on the specification of proper ontologies for terroristic activities [12]. Such ontologies describe sequences of events, along with the social networks of terrorists and their organization. Moreover, they represent relationships within networks of individuals and organizations, which is particularly useful towards detecting and tracing the evolution of communities. There are security applications that use general purpose ontologies for situation awareness [13], which are deployed in multi-source data fusion applications [14]. Beyond general purpose ontologies, there are also specialized counter-terrorism ontologies, which reflect theoretical concepts of terrorism and represent events, assets, and terroristic activities [15], [16]. Moreover, there are models and taxonomies that capture actions, events, and relationships for terroristic activities [15], [16]. These taxonomies consider the semantics of prominent terroristic attacks (e.g., the 911 attack in New York).

Terroristic modelling is also a key prerequisite towards automatically analyzing terroristic information by means of Artificial Intelligence (AI) algorithms, such as Machine Learning (ML). There are works that collect information about indicators of terroristic activities to predict such terroristic indicators by means of data analytics and ML algorithms (e.g., [17], [18]). However, most VR games do not combine strategic and tactical level tasks that collect and analyze historical data in conjunction with operational-level information. State of the art games make limited use of AI and ML algorithms, also given the lack of datasets for training such algorithms. Serious games can alleviate this lack of data, through generating data based on play activities. Specifically, by engaging expert users in the play activities it is possible to generate realistic datasets that match pragmatic scenarios. Such datasets can open opportunities for training ML/AI algorithms that could enhance the intelligence of the gaming activities, based on automatic detection of abnormal/suspicious behaviors and terroristic activities prediction. Moreover, similar AI systems could act interpedently of the gaming activities to assist LEAs in their counter-terrorism analysis activities.

To ensure that the AI algorithms are trustworthy, it is important to ensure that their training is based on trusted data. For instance, tampered training data could lead to poisoning

2325-2944/23/$31.00 ©2023 IEEE
DOI 10.1109/DCOSS-IoT58021.2023.00086

attacks that compromise the operation of AI systems and lead to malicious outcomes [19]. Data provenance and traceability across the entire lifecycle of a data asset is one of the best ways for ensuring the trustworthiness of AI data [20]. Distributed ledger technologies (i.e., blockchains) offer several advantages when it comes to implementing data provenance and traceability infrastructures [21]. Specifically, they are tampered proof infrastructures that operate in a decentralized fashion without the need for a third party trusted authority. As such they do not have a single point of failure and are less susceptible to cybersecurity attacks. Moreover, they are well suited for tracking and tracing distributed data produced in the scope of distributed, virtualized, multi-player environments. Blockchain infrastructures are an integral element of emerging metaverse environments [22], which makes them an excellent choice for implementing data provenance in the scope of VR environments for security training [23]. However, this opportunity is missed, as most VR applications for training security professionals do not leverage metaverse infrastructures and functionalities.

This paper introduces a novel VR application for training LEAs and security professionals in the analysis and prediction of potentially terroristic activities. The presented VR application incorporates state of the art terroristic modelling concepts to provide realistic training functionalities. At the same time, it serves as a data generation tool, which produces data for training AI analysis modules. Emphasis is given on the description of the following innovative aspects of the game: (A) Its ergonomic and realistic VR environment for the training of LEAs on terroristic indicators, events and their interrelationships, in-line with relevant literature about terroristic activities modelling (e.g., [15], [16], [17]). The implemented VR environment extends the work of the authors in [24]; (B) Its data generation features that enable the development of AI modules for the analysis and anticipation of terroristic activities. Specifically, the game serves as a first-of-a-kind data generator that can drive the training of AI/ML applications; and (C) The design of a blockchain infrastructure for provenance and traceability of digital assets of the game, including training data, AI analytic outcomes, as well as game artifacts. The blockchain infrastructure reinforces the cyber-resilience and overall trustworthiness of the game while being in-line with the emerging concept of the metaverse.

The remainder of the paper is structured as follows: Section 2 presents the concept, the technical architecture and the design of the game. Section 3 illustrates the implementation of the VR-based serious game, including its VR elements, scoring mechanisms, game control, and data generation features. Section 4 introduces the game's blockchain infrastructure and its provenance and traceability functionalities for key data assets. Section 5 concludes the paper by providing the plans of the authors for future work.

II. Theoretical Background and Game Design

A. *The Terroristic Attack Cycle*

One of the most popular theoretical concepts behind the planning and launch of terroristic attacks is the Terroristic Attack Cycle (TAC). The TAC describes the structure and the interrelationships of the activities that lead to the preparation and execution of a terroristic attack. It classifies these activities into various categories like preoperational surveillance, procurement of weapons, testing of security alarms, testing of other security measures, as well as test runs of the attack activities (Fig. 1).

The TAC was introduced several years ago, yet it is still relevant when it comes to modelling terroristic activities. It provides a taxonomy of potential actions, which can be used to develop game scenarios involving combinations of actions. Such scenarios can be elicited based on the combination of a variety of actions that collectively lead to the execution of all the types of activities of the TAC. The TAC drives the definition of game scenarios as the combination of different actions of the cycle. Specifically, gaming scenarios can be specified based on combinations of actions from the following categories: (a) Preoperational surveillance actions, such as photographing an area, taking videos of a target, surveillance of a target using some vehicle(s), deployment of cameras in the vicinity of the target and more; (ii) Procurement of weapons, such as purchase of guns, manufacturing of bombs in a hiding place, or acquisition of stolen weapons from other terrorists; (iii) Testing of security alarms, through violating security rules and precautions inside the target or even initiating gunfire; (iv) Test runs of the attack activities, such as deployment of terrorists in the target location.

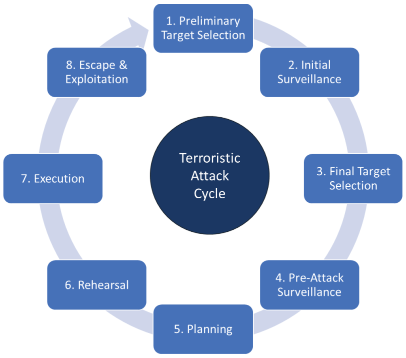


Fig. 1. The Terroristic Attack Cycle [25]

B. *Technical Architecture*

Fig. 2 illustrates the high-level technical architecture of the game, which consists of the following modules:

- A set of Input/Output (I/O) modules that enable users' interactions with the game. Multiple interaction modalities based on different devices are supported, including mouse, keyboard, and VR handsets-based interactions.
- A database that keeps track of information about the play activities, including the moves of the players, the terroristic actions, and the indicators of terroristic activities. The database is designed in-line with the terroristic modelling approach of the system, which is fully aligned with the earlier presented TAC cycle.
- Functional modules that implement the management of the flow of the game, the scoring mechanism of the game, as well as the generation of datasets for training AI modules. These modules are implemented within the Unity platform.
- AI analytics modules that are trained based on the generated datasets. Several modules have been

implemented based on different machine learning algorithms, including for example modules for predicting terroristic actions and identifying abnormal behaviors.

- A blockchain infrastructure, keeps track of metadata about the generated data and other information that resides in the database of the game. These metadata provide decentralized data provenance and traceability functionalities that boost the trustworthiness of the data used by the AI modules.

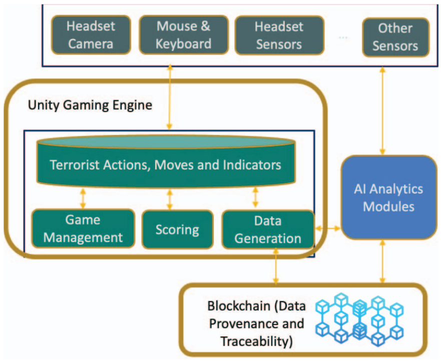


Fig. 2. VR Game Architecture and Building Blocks

The decentralized blockchain infrastructure interacts with the rest of the game by means of a proper API (Application Programming Interface). The latter facilitates reading and writing of metadata to the blockchain infrastructure.

C. *Functional Overview*

From a functional perspective, the game involves players (i.e., users) that have one of the following two roles:

- **Terrorist**: This role represents a terrorist or activist group. It aims at successfully completing a series of actions (i.e., TAC actions) towards launching a terroristic attack. The terrorist collects points based on successful actions and wins the game when it successfully completes all the actions of the TAC and manages to launch the attack.

- **LEA officer**: This role is a representative of the LEA agency. Players that have this role aim at identifying terroristic actions towards preventing the attack. The LEA officer collects points based on the successful identification of actions and wins the game if/when he or she prevents the attack.

LEA officers assume both of the above roles when playing the game. Hence, they get acquainted with terroristic activities, as well as the counter measures that can repel them. Specifically, the serious game is played towards the following ultimate objectives: (i) Training LEA officers in understanding the various indicators of terroristic actions and attacks, as well as in methods for correlating and analyzing the latter; (ii) Generating data that can be used to train/develop AI modules for analysis and correlation of terroristic actions.

The terroristic model that has driven the design and implementation of the game's database is inspired by the TAC. It specifies that terrorists operate according to a well-defined plan, which includes a range of prerequisite actions that they should carry out prior to the launch of a terrorist attack. For example, these actions fall typically in the following categories: (i) Actions towards pre-operational surveillance of the potential target, which enable terrorists to gather information for purposes of planning their attack; (ii) Seeking and elicitation of information about the target, which complement the information gathered during the pre-operational surveillance; (iii) Probing and testing security measures of the target, in order to understand the security measures of the LEAs; (iv) Acquisition of supplies, including collection of weapons and materials that are necessary for launching the attack; (v) Practice sessions (e.g., dry or rest runs of the attack) in order to identify flaws and potential unanticipated situations that could happen during the course of their actual attack. In the scope of the game, a terrorist attack involves all the above steps. When LEAs identify and synthesize information associated with the above-listed actions, the level of their alert about potential terrorist activities is raised. As part of the game, specific actions are associated with each one of the above types of activities. For instance, persons or vehicles seen in the same location on multiple occasions can be a sign of pre-operational surveillance. As another example, a series of false alarms requiring emergency services response can be an indication of security measures probing.

III. Virtual Reality Implementation

A. *Game Structure and Main Elements*

The VR implementation of the game has been carried out on the Unity platform. It comprises the following elements: (i) Objects of the VR environment, which represent different cyber elements of the play environment; (ii) Quest objects, which represent the various missions that must be completed by the player in order to advance and ultimately win the game; (iii) Game management and control objects that manage and control the flow and plot of the game; (iv) Game time management objects, which manage the time that is available the users in order to complete the game; (v) Scoring objects, which assign scores to the players based on their moves and performance; (vi) Data generation objects, which manage the generation of datasets based on the play activities.

B. *Game Objects*

The Virtual Environment of the game comprises of several objects, including among others buildings, cars, helicopters, cameras, UAVs (Unmanned Aerial Vehicles), the safehouse of the terrorists, waypoints, phone booths and many others (Fig. 3). The game environment includes a configurable number of Non-Playable Characters (NPCs) including LEA officers (e.g., police patrols), which are grouped around the targets and civilian NPCs i.e., citizens moving in various parts of the city (Fig. 4).

Fig. 3. Examples of Game Objects (Police Car, Buildings)

There are also control objects, which are in charge of controlling the operation and conduct of other objects as well as user activities. For instance, there are control objects that enable users to make phone calls and to escape from certain locations, as well as objects that ensure the movement of the players in-line with physics laws.

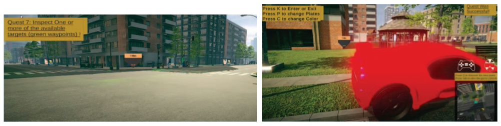
Fig. 4. Sample Views of NPCs

C. Quests

Quests are among the most important objects of the game. They represent mini missions that must be completed for the player to complete a specific phase of the TAC. In this direction, the game stores information concerning the quests. It also keeps track of on-going and completed quests. Players with the role of the terrorist interact with quest objects to identify the mission that they need to complete next. In this direction, the game provides the player with informative messages about the scope of the quest i.e., what should be done for the quest to be completed (Fig. 5). Moreover, the game informs the player regarding the status of the quests. For instance, whenever a quest is completed, the user/player is instructed to move to the next quest.

TABLE I. SUPPORTED QUESTS

List of Quests
Quest 1: Locate and inspect safehouse location
Quest 2: Check MiniMap and acquire supplies
Quest 3: Deliver the materials to the Safehouse
Quest 4: Call a partner using the phone booth
Quest 5: Change Car Plates
Quest 6: Enter the car to drive around
Quest 7: Inspect One or more of the available targets
Quest 8: Go back and enter inside the safehouse to prepare a bomb
Quest 9: Approach one of the available targets and place the bomb
Quest 10: Buy an evasion ticket at the kiosk
Quest 11: Escape! Take a bus/taxi



Quest 7: Inspect One or more of the available targets (green waypoints) !

Press K to Enter or Exit
Press P to change Plates
Press C to change Color

Quest Was Successful!

Fig. 5. Sample Quests within the VR game

Table 1 outlines a list of Quest(s) that are supported in the game. The design and implementation of these quests have been inspired by the TAC-based terroristic modeling. Specifically, each quest is mapped to a phase of the TAC. Hence, when completing a quest, the game considers the corresponding part of the TAC cycle as completed as well. Examples of this mapping follow:

- The "Initial Surveillance" phase of the TAC is supported based on foot surveillance (e.g., Quest 1 in the table). Specifically, the player with the terrorist role must inspect the target on foot (e.g., Central Alley, Public Library, Public Park). Similarly, a vehicle surveillance quest is supported as well, i.e., a quest involving the use of a car to monitor one of the available targets and collect information about it. The player can drive the car and direct it to any location.
- The "Planning" phase of the TAC relates to a Quest that is concerned with the acquisition of supplies (e.g., Quest 2 in the table). Specifically, the player acquires the supplies required to build the bomb. In this direction, it interacts with specific game objects (e.g., boxes) that signal the procurement of specific materials in the game context. Furthermore, another Quest (e.g., Quest 8 in the table) enables the player to return to the safehouse and place the acquired materials to the table of the safehouse.
- The "Pre-Attack Surveillance" phase of the TAC is related to an "information seeking" quest. To this end, players can navigate around the targets by following the green waypoints. Moreover, an orange waypoint pinpoints the safehouse location. Furthermore, they can also interact with LEA officers and civilian NPCs in order to obtain information about the target(s). The process is statistical i.e., probability of obtaining information depends on the interacting NPC.
- The "Rehearsal" phase of the TAC relates to a Quest that is destined to test the alarms of the target. Specifically, the game includes waypoints that enable the player to reach the target(s) towards the evaluation of their security measures.
- The "Escape" phase of the TAC relates to Quests (e.g., Quest 11 in the table) that enables the player to escape from the attack location using a bus or taxi. In this direction, the player can use the mini-map and interact with the vehicle to escape. To enable the escape, a quest that enables the player to buy an evasion ticket is supported (e.g., Quest 10 in the table).
- The "Execution" phase of the TAC relates to a Quest (e.g., Quest 9 in the table) that enables the player to follow specific waypoints to approach the target and place a bomb.

D. Game Management and Scoring

The game must be completed within a fixed, yet configurable time limit (currently 20 minutes gameplays). This means that the game ends when the player wins or when the time is up. To manage the time limit, a proper Timer object has been implemented in the Unity platform. The value of the count-down timer is displayed on the VR interface of the game. Time freezes in certain occasions, for example: (i) When the player reads the game instructions; (ii) When the player selects waypoints; and (ii) When the player selects to "pause" the time based on a relevant comment.

The scoring mechanisms of the game aims at rewarding the player for successfully completing relevant actions that are in-line with the quests that the player must complete. The player gathers points for advancing to the right direction i.e., to a winning direction. At the same time, the points serve as a pool of resources that the player can spend to complete his/her mission. For instance, points may be spent for seeking information or acquiring supplies. These scoring mechanisms can incentivize users to improve their understanding of the terroristic and counter terroristic activities i.e., to boost the effectiveness of their training and interaction with the game. From a technical perspective, the scoring mechanisms of the game are based on the implementation of two functions within a script of the Unity environment. These functions implement score raise and score reduction functionalities. The script is configurable and attached to each game object in order to enable the addition or substruction of points in-line with one or more actions that are associated with the object.

The player starts the game with an initial number of points. In case the points of the game reach zero because of unsuccessful actions, the game ends with the player as the losing party. Every successful quest completion rewards the player with a predetermined, configurable number of points. Moreover, the game provides the means for scoring specific missions in a statistical and probabilistic way on probability distribution functions. For instance, during information seeking and the making of phone calls, the player can spend points that follow a probability distribution function.

E. Data Generation

To support the generation of data for AI module training, a set of data management scripts has been developed. Data generated through the game are initially persisted in a DBMS (Database Management System). The latter comprises the following main entities: (i) Game actions, which comprise data about the actions of the player; (ii) Surveillance objects, which comprise surveillance information, including information about the activities of LEAs and information collected from the cameras' functionalities; (iii) Avatar moves, which is populated with data of the players' movements (e.g., data about the trajectories of the avatars of the players); (iv) NPC_k moves (where K>=1 and K<=N) i.e., N tables with the movements (e.g., trajectories) of each NPC of the game. As already outlined the parameter k is configurable, which means that the amount of NPC data is configurable as well.

The database population is based on various scripts, which are attached to game objects (e.g., NPCs). Data generation sampling rates are also configurable. On the one hand, it is worth noticing that the tables of the player's movements include both the trajectory of the players and their orientation (e.g., what the player is seeing). As such, this table has the highest sampling rate. On the other hand, the surveillance and the action entities do not require a specific sample rate as their values are generated during gameplay i.e. when the player performs certain actions. Data generation about these entities is driven by triggers i.e., data are not generated continually as in the case of avatars and NPCs.

F. AI Modules Development and Predictions

The generated datasets are used to train AI modules that provide analytics insights in two complementary directions (Fig. 6):

- Predictions of the (future) locations of the players during the evolution of the game.
- Predictions of the future actions of the players.

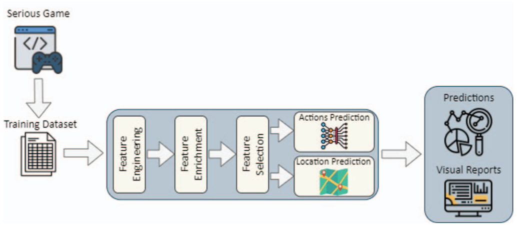


Fig. 6. Development and Integration of AI Pipelines in the Game

Different models have been trained and tested for the above-listed tasks, based on a variety of datasets, including different numbers of objects and NPCs. The use of multi-class classifiers was deemed to provide quite accurate results for the prediction of the actions of the terrorist. Likewise, the use of the popular Long Short Term Memory (LSTM) deep learning model provides a very accurate prediction of the next locations of the terrorists, leading to almost zero Mean Squared Error (MSE) after some training epochs. Overall, the results are quite promising and can be integrated into the game in order to provide predictive insights on the play moves of the terrorists to allow the player to determine how to best confront them.

IV. Blockchain Based Trusted Data Management

Blockchain technology is a promising paradigm for enhancing the trustworthiness of data generation and data management processes in VR-based games [26]. As already outlined, a blockchain infrastructure is a tamper-proof place to store data that allows for the secure and decentralized tracking and tracing of digital assets in-line with the architecture presented in Fig. 2. In this context of the game, storing game's metadata on the blockchain, we are able to track and trace the training data used, the AI analytics produced from different gameplays and the corresponding game artifacts. The latter is depicted in Fig. 7.

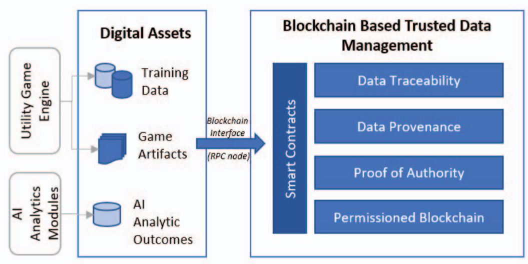


Fig. 7. Blockchain Based Trusted Data Management Architecture

A. Blockchain Architecture

The use of blockchain technology is integral to the design of the serious game. A permission blockchain is utilized, allowing interaction with authorized users. The latter permits data sharing and collaboration between authorized users while ensuring that data on the blockchain is secured and unchangeable. Moreover, the Proof of Authority (PoA) consensus algorithm is used towards minimizing the resources required to deploy the blockchain in comparison to other proof-based consensus algorithms [27]. Also, smart contracts are employed to control how training data sets, game artifacts, and digital assets are utilized throughout their lifecycle during a gameplay. Among others, a smart contract outlines the conditions where a digital asset can be updated, erased, or modified, which ensures transparency, immutability, and trust. Regarding the digital assets, a unique identifier is assigned by the game to each, with both the identity and the item's cryptographic hash stored on the blockchain. Thus, it is ensured that the game assets cannot be altered or tampered in any way. Overall, the use of blockchain technology as part of the VR application's architecture provides a secure and resilient infrastructure for tracking and tracing digital assets generated by the game, while also supporting efficient data sharing and collaboration.

B. *Data Provenance and Traceability*

One of the key requirements for the trustworthiness of the AI data of the VR application is the provision of data provenance and traceability across the entire lifecycle of the data asset of the game. Data provenance refers to the origin and history of data and its lineage, starting from its creation, ownership, and usage. In the context of the serious game, each recorded event is timestamped, cryptographically protected, and connected to prior occurrences by integrating the game's data creation and storage processes with a blockchain network. This results in a clear and temper-proof record of the data's background. Anyone with the blockchain access can verify the data's reliability and trustworthiness, promoting confidence and transparency. Data traceability is therefore an essential component of the scientific investigation and technological development of the game [30].

On the other hand, data traceability monitors and traces the data provenance across its entire life cycle, including the preservation, processing, and access stages. Data traceability is especially important for serious games, where immersive virtual worlds and AI analytics play a key role. To this end, the blockchain infrastructure of the serious game intends to achieve complete data traceability by rigorously documenting and auditing all data created during gaming, from its generation to its final use for training or research. Monitoring the information flow between various architectural components, (e.g., game objects, the VR environment database, and AI analytics modules) is required. Data traceability maintains the integrity and trustworthiness of generated game data by developing systems to record metadata, timestamps, and contextual information at each stage.

The incorporation of data provenance and traceability into the serious game infrastructure improves accountability, transparency, and credibility. Blockchain technology has been employed to keep a verified trail of asset transactions, assuring data authenticity and traceability [28]. The triggering VR object timestamps and cryptographically signs each transaction on the blockchain, giving a credible history of the data asset's creation and evolution. Modifications to digital assets are also recorded on the blockchain, including each new transaction carrying a digitally signed hash of the changed asset in addition to a reference to the preceding transaction. This ensures that changes to data assets are noticed and ascribed to the right user. Access control methods, enforced using smart contracts and digital signatures, further protect the data assets' integrity by enabling only authorized users to access and alter them.

C. *Smart Contracts*

Smart contracts are another component of the blockchain architecture of the serious game. They provide a safe and automated mechanism to govern the lifecycle of digital assets. Smart contracts are self-executing programs that enable the automation of complicated procedures (e.g., the game's quests) and the execution of conditional transactions on the blockchain network. Smart contracts define the rules and prerequisites governing the development, alterations, and removal of digital belongings on the blockchain. They also apply access control limitations [29]. This is performed by using encrypted keys in order to certify the identity of the objects and ensure that only the approved ones can communicate with the VR application. They also enforce the guidelines and requirements for the execution of conditional transactions on the blockchain in addition to controlling the data assets produced by the game. For instance, a smart contract provides the terms for a transaction's automated execution when certain criteria are satisfied, such as the successful fulfilment of a particular quest or the attainment of a particular score in a game.

V. Conclusions

VR-based serious games provide excellent opportunities for creating ergonomic, safe and secure training environments. The emerging metaverse era is expected to enhance the functionality, trustworthiness and intelligence of such environments based on two main technology enablers, namely AI and blockchain technologies. Specifically, AI technologies can provide the players' insights into the evolution of the game (e.g., predictions about their next moves), while blockchain technologies can add a novel security and trust layer to the game that will ensure the integrity of digital assets. The serious games can benefit further from leveraging blockchain technology in metaverse environments, which provide secure and transparent platforms for creating and exchanging digital assets. Metaverse environments are virtual worlds that are created and maintained by decentralized blockchain networks, providing a secure and transparent platform for the creation and exchange of digital assets, enabling a more immersive experience for users.

This paper has presented a practical implementation of a VR game for training Law Enforcement Agencies, including its AI and blockchain functionalities. The development roadmap of the game includes the integration of more AI insights in the game, along with their interpretations based on explainable AI technology. We also plan to integrate the blockchain and smart contracts infrastructure towards enhancing the reliability of the data assets of the game, including play activities data, AI insights, and other digital assets of the VR game. Once we have integrated the infrastructure, it will be also feasible for the serious game to take place in a distributed way. After the integration of blockchain infrastructure, we plan also to evaluate whether the platform has value and meets the expectations regarding training security officers. To do so, we plan to define the necessary evaluation metrics that will be used to measure the effectiveness of the serious game platform on top of the blockchain infrastructure. To further enhance the platform evaluation, we aim to split officers into two groups: those with classical training and those who trained using the proposed platform, comparing the results obtained. Finally, the use of blockchain technology in metaverse environments is a promising area for the development of serious games for security training and is likely to play an increasingly important role in the future of virtual reality and blockchain-based applications.

ACKNOWLEDGMENT

Part of this work has been carried out in the scope of the LAW-GAME Project, which has received funding from the European Commission under the H2020 programme (contract No. 101021714). The authors acknowledge the support and contributions from all partners of the project.

REFERENCES

[1] P. Gebhard et al., "Serious Games for Training Social Skills in Job Interviews," in IEEE Transactions on Games, vol. 11, no. 4, pp. 340-351, Dec. 2019.

[2] A. Hamza, P. Pernelle, C. Ben Amar and T. Carron, "Serious games for vocational training: A compared approach," in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1-8.

[3] J. Guo, N. Singer and R. Bastide, "Design of a serious game in training non-clinical skills for professionals in health care area," in 2014 IEEE 3nd International Conference on Serious Games and Applications for Health (SeGAH), 2014, pp. 1-6.

[4] G. Jacob, R. Jayakrishnan, and K. Bijlani, "Smart fire safety: Serious game for fire safety awareness," in Information and Decision Sciences. Springer, 2018, pp. 39-47.

[5] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education,". Computers and Security, 95, [101827].

[6] J. Yerby, S. Hollifield, M. Kwak, and K. Floyd, "Development of serious games for teaching digital forensics," Issues Inf. Syst., vol. 15, no. 2, pp. 335-343, 2014.

[7] S. V. Veneruso, L. S. Ferro, A. Marrella, M. Mecella, and T. Catarci, "CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues," in Proceedings of the International Conference on Advanced Visual Interfaces (AVI '20), 2020, pp. 1-8.

[8] J. Molka-Danielsen, E. Prasolova-Førland, M. Fominykh, and K. Lamb, "Use of a Collaborative Virtual Reality Simulation for Multi-Professional Training in Emergency Management Communications," in 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 2018, pp. 408-415.

[9] J. Haskins et al., "Exploring VR Training for First Responders," in 2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), 2020, pp. 57-62.

[10] P. Caserman, P. Schmidt, T. Gobel, J. Zinnacker, A. Kecke and S. Gobel, "Impact of Full-Body Avatars in Immersive Multiplayer Virtual Reality Training for Police Forces," in IEEE Transactions on Games.

[11] J. Bertram, J. Moskaliuk, and U. Cress, "Virtual police: Acquiring knowledge-in-use in virtual training environments," in 2011 IEEE International Symposium on VR Innovation, 2011, pp. 341-342.

[12] A. Mannes and J. Golbeck, "Building a terrorism ontology," University of Maryland, College Park, 2005.

[13] M. Kokar, C. Matheus, and K. Baclawski, "Ontology-based situation awareness," Information Fusion, vol. 10, no. 1, pp. 83-98, 2009.

[14] C. Matheus, M. Kokar, and K. Baclawski, "A core ontology for situation awareness," in Proceedings of FUSION 03, 2003, pp. 545-552.

[15] Department of Homeland Security, "Strategic Framework for Countering Terrorism and Targeted Violence," September 2019, available at: https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf. [Accessed: May 16, 2023].

[16] B. T. Bennett, "Understanding, assessing and responding to terrorism: Protecting critical infrastructure and personnel," Hoboken, NJ: John Wiley & Sons, 2007.

[17] R. Sormani, J. Soldatos, S. Vassilaras, G. Kioumourtzis, G. Leventakis, I. Giordani, and F. Tisato, "A serious game empowering the prediction of potential terrorist actions," Journal of Policing, Intelligence and Counter Terrorism, vol. 11, no. 1, pp. 30-48, 2016.

[18] R. Sormani, F. Archetti, and I. Giordani, "Criticality assessment of terrorism related events at different time scales," Journal of Ambient Intelligence and Humanized Computing, vol. 8, no. 1, pp. 9-27, 2017.

[19] C. Hu and Y.-H. F. Hu, "Data Poisoning on Deep Learning Models," in 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2020, pp. 628-632.

[20] J. Soldatos and D. Kyriazis (eds.), "Trusted Artificial Intelligence in Manufacturing: A Review of the Emerging Wave of Ethical and Human Centric AI Technologies for Smart Production," Boston-Delft: now publishers, 2021.

[21] S. D'Antonio and F. Uccello, "Data Provenance for healthcare: a blockchain-based approach," in 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 2022, pp. 1655-1660.

[22] A. M. Al-Ghaili et al., "A Review of Metaverse's Definitions, Architecture, Applications, Challenges, Issues, Solutions, and Future Trends," in IEEE Access, vol. 10, pp. 125835-125866, 2022.

[23] T. Huynh-The, T. R. Gadekallu, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. da Costa, and M. Liyanage, "Blockchain for the metaverse: A Review," Future Generation Computer Systems, vol. 143, pp. 401-419, Jun. 2023.

[24] J. Soldatos, A. Pantazidis, K. Margariti, P. Velanas, and B. Gornea, "Virtual Reality Training of Law Enforcement Officers in Predicting Terroristic Attacks Indicators," in 2022 International Conference on Interactive Media, Smart Systems and Emerging Technologies (IMET), Limassol, Cyprus, 2022, pp. 1-4.

[25] Stratfor, "Defining the Terrorist Attack Cycle," February 23, 2012. [Online]. Available: http://www.stratfor.com/sample/image/defining-terrorist-attack-cycle. [Accessed: May 16, 2023].

[26] J. Soldatos, I. Konstantinou, A. Zaslavsky, and A. Romanovsky, "Blockchain Based Data Provenance for Trusted Artificial Intelligence," in Trusted Artificial Intelligence in Manufacturing, 2021, pp. 1-1.

[27] M. Touloupou, M. Themistocleous, E. Iosif, and K. Christodoulou, "A Systematic Literature Review Towards a Blockchain Benchmarking Framework," IEEE Access, vol. 10, pp. 3557-3575, 2022.

[28] A. Kalafatelis, et al., "ISLAND: An Interlinked Semantically-Enriched Blockchain Data Framework," in Economics of Grids, Clouds, Systems, and Services: 18th International Conference, GECON 2021, Virtual Event, September 21-23, 2021, Proceedings, vol. 18, pp. 207-214, Springer International Publishing, 2021.

[29] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," Future Generation Computer Systems, vol. 105, pp. 475-491, 2020.

[30] R. V. George, H. O. Harsh, P. Ray, and A. K. Babu, "Food quality traceability prototype for restaurants using blockchain and food quality data index," Journal of Cleaner Production, vol. 240, p. 118021, 2019