# Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey

Ivaylo Vladimirov[1], Maria Nenova[2], Desislava Nikolova[3] and Zornitsa Terneva[4]

*Abstract* – **In this scientific research, a survey of different security and privacy protection issues and flaws in the context of reconstruction of 3D models real people is made. The intent of this analysis the threats that a realistic digital clone AKA avatar of a person can have in the wrong hands. This paper will also offer different approaches that can be used in overcoming this privacy problem.**

*Keywords* – **3D Reconstructed Models, Security, Privacy Protection, Internet, Metaverse;**

## I. Introduction

In this day and age, practically all people in the advanced countries are immersed to some amount in digital technologies even if they are unaware of it. At the moment, nearly 3.8 billion people in the world own a smartphone, accounting for 48.53 percent of the world's population, a figure that is only expected to rise as digitalization becomes more readily accessible. [1]

We have developed ourselves and our communities into the next social evolutionary stage- a "digital society". A Digital Society is an interdisciplinary research topic as well as a type of progressive society that has emerged as a result of modern technology' adaptation and integration with culture and society. There are numerous new conceptions that fit under the Digital Society umbrella, such as Smart Cities, Holoportation, the Metaverse and a plethora of other smart and advanced concepts. These services are based on popular technologies like: 5G and 6G, Internet-of-Things (IoT), Big Data, Computer Vision and many more. [2][3]

A metaverse is a collection of permanent, cross-user, shared, 3D virtual places that are linked to the physical world and integrated to form a cohesive and eternal virtual cosmos. People access the multiverse as avatars that may engage with each other, goods and items, tools, services, and enterprises included within. In its core it is, a technologically enabled, cyber-physical Web 3.0 capable of outperforming the current Internet paradigm. The idea of the metaverse as the next developmental leap in both our physical and virtual network interfaces consequently in our social lives. Which explains exactly the tremendous hype and sporadic attention that surrounded the metaverse. [4][5]

These trending and relatively new topics (like the Metaverse) are still in their development stage, and while some researchers try to better the architecture of this new alternate reality, others are focused on the idea of finding its weaknesses and flaws in order to capitalise on them.

While a new technology is developed the most important subjects of discussion are the privacy and security of the people and their personal information. When talking about 3D Reconstructed Models of People on the internet, in the Metaverse or in a different environment like a mobile application the main focus in the avatar. In the context of this study by avatar or virtual human copy or twin, virtual Me it is described a realistic and metrically accurate virtual copy of a user/person/client of an application. [6]

In general, protecting one's privacy has been a basic human right. In communications, privacy entails the preservation and, more importantly, the proper use of the user's personally identifiable information (see Fig.1). Customers' expectations should be met by this utilisation. Privacy usually attributes to the utilisation of laws, standards, policies and processes by which private details are handled. [7]

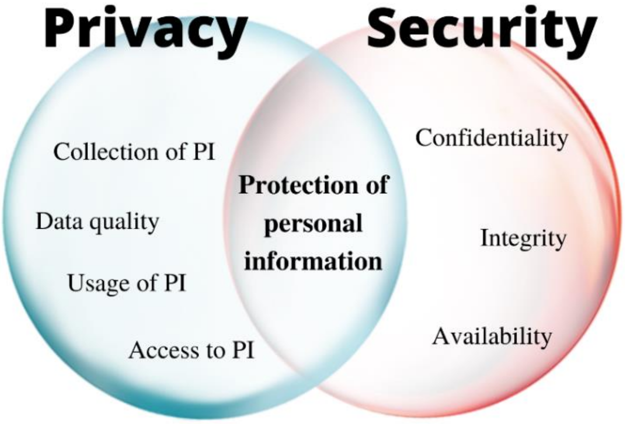

Fig.1 Fundamental aspects of privacy and security

The notion of security refers to information and cyber security, which is described in detail by the ISO 27001 standard as the protection of confidentiality, integrity, availability as well as accountability, authenticity, reliability and non-repudiation can also be involved (see Fig.1). Confidentiality and privacy are frequently conflated in the minds of certain security specialists. [8]

[1] Ivaylo Vladimirov is with the Technical University of Sofia, Faculty of Telecommunications, Dept. Communication Networks, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: ivladimirov@tu-sofia.bg

[2] Maria Nenova is with the Technical University of Sofia, Faculty of Telecommunications, Dept. Communication Networks, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: mvn@tu-sofia.bg

[3] Desislava Nikolova is with the Technical University of Sofia, Faculty of Telecommunications, Dept. Radio Communications and Video Technology, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: dnikolova@tu-sofia.bg

[4] Zornitsa Terneva is with the Technical University of Sofia, Faculty of Telecommunications, Dept. Communication Networks, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: zterneva@tu-sofia.bg

## II. The Security and Privacy Problem

### A. The current situation

We saw the proliferation of digital content in the shape of of viral images and video with the emergence of the social Web. Internet 3.0 will eventually be a experience involving more than one sense. It is exactly this perspective on the metaverse as an interface that will usher us further into Internet 3.0 age. [9]

This unparalleled level of immersion and inter-serviceability has an unintended consequence: an increase in the quantity and quality of risks related with the available technologies that will be used to materialise the architecture behind this new digital cloned world. Such dangers are particularly relevant to the privacy and security of the users and businesses that want to operate in it. [10]

In terms of customer confidentiality in the astral planes, three aspects stand out: personal information (PI), behaviour, and communications. PI obtained through social networking platforms is already being used for doxing—the practise or threat of releasing a victim's private information for the purpose of extortion or online shame. Given that such a will reveal considerably more PI about its consummers, not just to platforms, and even to fellow account holders. More connectivity suggests more interpersonal exchanges, which increases the quantity and ways in which information may be acquired and abused, and cyber-crime can be committed. [11][12]

Regarding security, the innovative synthesis of various advanced technologies that will come into play in the not so far in the future will unleash plenty of security risks, in addition to the privacy concerns already mentioned. As a practical and relevant problems are the security issues of content integrity and user authentication. [10]

### B. Possible cyber-attacks

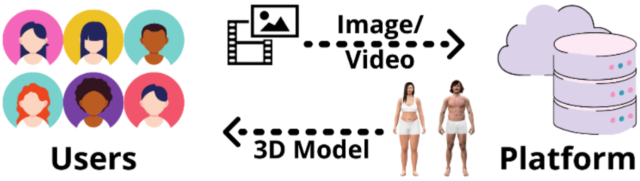

Fig.2 Concept model of an online service for 3D reconstruction

This research was conducted due to the fact that our future work is focused on the development of an online service that will allow a user to create a realistic avatar of himself, applicable in all kinds of enviroments like games, social platforms, business platforms, the metaverse, etc. The basic model of the concept can be observed in figure 2. If a person wants to have the opportunity to use the 3D reconstruction service, an account needs to be created first. The reconstruction process is performed on a separate server, and in order for a user to access the created realistic avatar, he/she/they need to log in to his/her/their account.

When dealing with personal information: a high-definition scan of a person and his private sensitive features (his eyes, face), confidentiality is of utmost importance.

In figures 3 and 4, we have outlined the most likely cyber attack scenarios applicable to the service's idea model.

"Example Scenario A" (see figure 3) shows how an attacker can get a hold of the PI of a user. The hacker can rely on cyber attacks like man-in-the-middle (MITM). MITM is a type of attack in which a malicious third party stealthily interferes and gains control over the communication session between two or more terminals. The MITM attacker has the ability to block, manipulate, or modify the data traffic of the victims. Such attacks are: spoofing-based, false base station-based, SSL/TLS-based [13]. Side-channel attacks are also applicable here. They exploit the hardware vulnerabilities of a system by measuring the power consumption and searching for patterns in the collected data. [14][15]

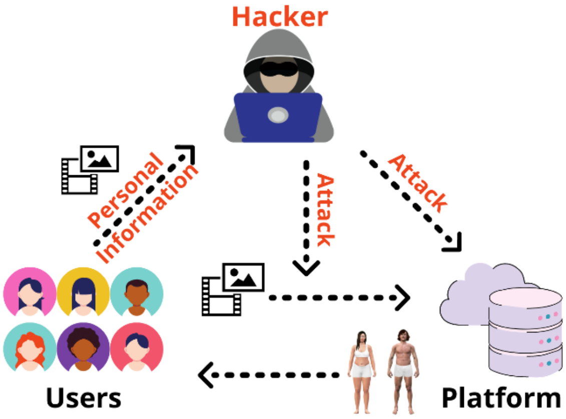

Fig.3 Example scenario A: The hacker gaining access to the user's PI

"Example Scenario B" (see figure 4) shows how an attacker can get a hold of the personally identifiable information (PII) of a user and afterwards use it to gain access of their 3D avatar. Here, the hacker can use social engineering attacks like the well-known phishing [16] or techniques like Cross-site scripting (XSS) - a web attack in which malicious web program is transferred or launched from the victim's computer's browser, commonly in script form [17].

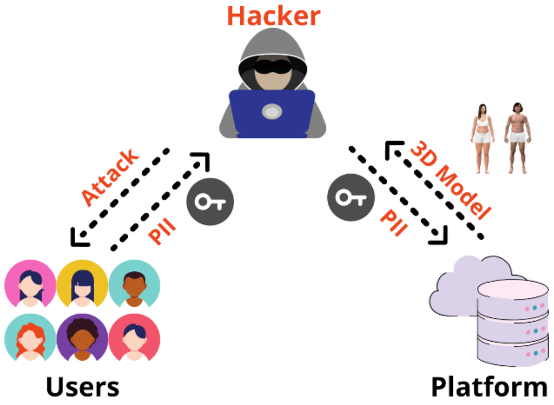

Fig.4 Example scenario B: The hacker gaining access to the 3D reconstructed avatar

## III. POTENTIAL SOLUTIONS

Addressing the importance of building trusted ecosystems within the new up-and-coming technologies is a vital consideration. These trustworthy ecosystems will include the incorporation of algorithms, structures, guidelines, regulations, and rules into hardware and software construction and improvement cycles in order to handle the different elements of protection, privacy, and security well within technology's DNA. [18]

### *A. Solving Scenario A*

The intrusion problem presented in "Example Scenario A" can be tackled by incorporating a Network Intrusion Detection System (NIDS). NIDS is a structure that protects against web-based cyberattacks, misuse, and negligence. Traditional approaches, however, are unable to extract correct aspects of intrusion activity from high bandwidth samples and process the large amount of data quickly because to the dynamic, complex and time-varying internet environment. To address the data-driven modern internet era it is better to use a deep learning approach-based system. [19]

GAN is a non-parametric model that generates data in a lower dimension using a small number of parameters. It is flexible and versatile, allowing it to be turned into a variety of configurations to meet a diversity of requirements.[20]

Such a network is the deep convolutional generative adversarial network (DCGAN) architecture that is based on a pre-processing algorithm established for complex, multidimensional cyber threats. It can be used to extract features straight from the raw information and then learn from that data to generate a new training datasets, in which long short-term memory (LSTM) is utilised to automatically learn the features of network intrusion behaviours. [21]

### *B. Solving Scenario B*

When addressing "Example Scenario B", the focus is on the security authentication aspect of the communication process. The hacker relies on the user and his human nature to get a hold of the login information needed. Most thwart techniques require prevention actions to be taken by the user of the service. We will focus on methods based solely on the server's side of the service:

PhishPreventer: A new authentication protocol to prevent phishing attacks that uses the encryption technique of the Elliptic Curve Digital Signature Algorithm (ESDSA) to generate and verify digital signatures and Elliptic Curve Integrated Encryption Scheme (ECIES) to encrypt and decrypt the messages between the user's and the server's devices. [22]

Nemesis: A method for automatically determining when a system securely authenticates users by monitoring the flow of user's login details through the runtime utilising Dynamic Information Flow Tracking (DIFT) methods. Nemesis auto-ensures that only properly logged-in users are given access to any classified resources or data by combining user credentials with programmer-supplied access requirements on database entries. [23]

### *C. Solving both scenarios*

The incorporation of a fully homomorphic encryption is a privacy-preserving solution, that allows to exchange data between devices without sending any information until it is ensured that the transfer is safe. [24][25] This protocol can be used in both directions: to send the preliminary image/video to the served and the resulting 3D model back to the user. Figure 5 depicts the protocol used as follows:

1. **Encrypt Data and send with Context**: The user's device pre-processes the image/video and encrypts it. The encrypted data and context are transferred to the server, which is attempting to establish that they were both present across a mutually authorised TLS connection.
2. **Compute Similarity**: All of the required similarity scores are calculated by the server.
3. **Return Results**: The encrypted resulting scores are send back to the decision-making user.
4. **Decrypt and Decide**: The user decrypts the received resulting data and compares it.
5. **Send Video**: If the decision-making user is satisfied, the image/video is send to the served.

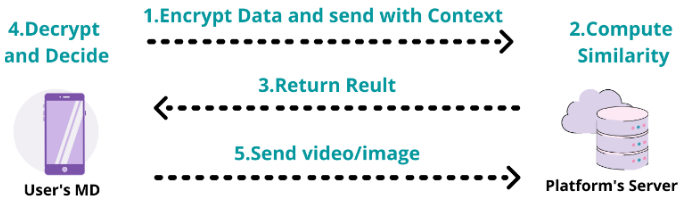

Fig.5 Homomorphic protocol; MD-mobile device

Another possible, but more complex, solution is to combine multiple algorithms. Li et al. [26] have fused a plethora of programmes to produce a method for removing people from images of landmarks and then using them for 3D reconstruction of buildings. When applied to the problem in our hands, we can suggest the following methodology for full privacy protection:

1) **Detection and segmentation of a person's private features**: In the first step the private areas in the image/video recorded by the user need to be indicated [27] and replaced by blank pixels or blurred out. [28] It is best to use a deep convolutional neural network (DCNN).

2) **Transporting the ambiguous data**: The now privately protected information is sent from the client's device to the service's server.

3) **Repairment of the alternated pixels**: After the server receives the image/video information, the blank/blurred regions need to be adjusted and prepared for the 3D reconstruction process. A GAN-based image completion method can be used to adapt the null pixels by substituting them based on the surrounding ones.[26]

4) **3D reconstruction and generation of a look-a-like avatar:** This algorithm is still a work in progress. [29]

## IV. Conclusion

Securing communication material appears to be a "simple" challenge, especially when compared to securing computations and devices. However, it has become clear that even when strong cryptography is utilised, most communications are unsecured, and the threat standerised models that have typically been considered are too weak.

To maintain privacy, how data is transferred within digital environments will need to be more thoroughly examined. The elimination of biases that will contribute to a non-inclusive or malevolent adaptation of the actual world is a second dimension to be examined within the privacy issues of the metaverse's development. Breach of privacy and security are channels that can jeopardise the safety of operations, users and their avatars.

## Acknowledgement

This scientific research is part of a contract №222ПД0016-07 for a research project to help doctoral students: "Development of algorithms for reconstruction and visualization of deformable 3D models of people and clothing in an online environment" of the Technical University of Sofia, Bulgaria Research Sector.

## References

[1] A.Gunn, “Living in a digital world: the causes and the consequences”, Online Article by Medium.com, 2020;

[2] P.Prantosh, P.S.Aithal, "Digital Society: Its Foundation and Towards an Interdisciplinary Field.", Proceedings of National Conference on Advances in Information Technology, Management, Social Sciences and Education, 2018;

[3] C.Montag, S.Diefenbach, “Homo Digitalis: Important Research Issues for Psychology and the Neurosciences at the Dawn of the Internet of Things and the Digital Society.”, Sustainability, 2018;

[4] D.Grider, M.Maximo, “The Metaverse: Web 3.0 Virtual Cloud Economies”, Grayscale Company Research, 11.2021;

[5] C.Moy, A.Gadgil, “Opportunities in the Metaverse: How Businesses Can Explore the Metaverse and Navigate the Hype vs. Reality”, Onyx by J.P.Morgan Company, 2022;

[6] S.Sahmim, H.Gharsellaoui, “Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review”, International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, 2017;

[7] A.A.Abba Ari, O.K.Ngangmo, C.Titouna, O.Thiare, Kolyang, A.Mohamadou, A.M.Gueroui, "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges", Applied Computing and Informatics Journal, 2020;

[8] “ISO/IEC 27001:2005”, Specification for an Information Security Management System, 2005;

[9] M.Kosinski, D.Stillwell, T.Graepel, “Private traits and attributes are predictable from digital records of human behavior”, Proceedings of the National Academy of Sciences, vol. 110, 2013;

[10] R.Di Pietro, S.Cresci, "Metaverse: Security and Privacy Issues", 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, 2021;

[11] B.Falchuk, S.Loeb, R.Neff, “The social metaverse: Battle for privacy,” IEEE Technology and Society Magazine, vol. 37, 2018.

[12] P.Snyder, P.Doerfler, C.Kanich, D.McCoy, “Fifteen minutes of unwanted fame: Detecting and characterizing doxing”, Internet Measurement Conference (IMC’17), 2017;

[13] M.Conti, N.Dragoni and V.Lesyk, "A Survey of Man In The Middle Attacks", IEEE Communications Surveys & Tutorials, vol. 18, 2016;

[14] I.Vladimirov, D.Nikolova, Z.Ternva, "Hardware Implementation and Comparison of CRA and TRA when Trying to Recover the AES-128 Key", 55th ICEST, 2020;

[15] D.Nikolova, I.Vladimirov, Z.Terneva, "Software Implementation of CRA and TRA to Recover the AES-128 Key using Side-Channel Signals with Python3", 55th ICEST, 2020;

[16] Z.Alkhalil, C.Hewage, L.Nawaf, I.Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", Frontiers in Computer Science 3, 2021;

[17] G.E.Rodríguez, J.G.Torres, P.Flores, D.E.Benavides, “Cross-site scripting (XSS) attacks and mitigation: A survey”, Computer Networks, Volume 166, 2020;

[18] C.Li, F.Lalani, “How to address digital safety in the Metaverse”**,** Davos Agenda 2022 The World Economic Forum, Jan 2022;

[19] N.Shone, T.N.Ngoc, V.D.Phai, Q.Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, 2018;

[20] I.K.Dutta, B.Ghosh, A.Carlson, M.Totaro, M.Bayoumi, "Generative Adversarial Networks in Security: A Survey," 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020;

[21] J.Yang, T.Li, G.Liang, W.He, Y.Zhao, "A Simple Recurrent Unit Model Based Intrusion Detection System With DCGAN," IEEE Access, vol. 7, 2019;

[22] S.Bojjagani, D.Brabin, P.V.Rao, “PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification”, Procedia Computer Science, 2020;

[23] M.Dalton, C.Kozyrakis, N.Zeldovich, “Nemesis: preventing authentication and access control vulnerabilities in web applications”, 18th Conference on USENIX security symposium, 2009;

[24] U.Goswami, K.Wang, G.Nguyen, B.Lagesse, "Privacy-Preserving Mobile Video Sharing using Fully Homomorphic Encryption", IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2020;

[25] B.Lagesse, G.Nguyen, U.Goswami and K.Wu, "You Had to Be There: Private Video Sharing for Mobile Phones using Fully Homomorphic Encryption", IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2021;

[26] Q.Li, Z.Zheng, F.Wu, G.Chen, "Generative Adversarial Networks-based Privacy-Preserving 3D Reconstruction", IEEE/ACM 28th International Symposium on Quality of Service (IWQoS), 2020;

[27] L.C.Chen, G.Papandreou, F.Schroff, H.Adam, “Rethinking atrous convolution for semantic image segmentation", Conference on Computer Vision and Pattern Recognition (CVPR), 2017;

[28] K.Yang, J.Yau, L.Fei-Fei, J.Deng, O.Russakovsky. "A study of face obfuscation in imagenet", arXiv preprint arXiv:2103.06191, 2021;

[29] I. Vladimirov, D. Nikolova and Z. Terneva, "Overview of Methods for 3D Reconstruction of Human Models with Applications in Fashion E-Commerce," 56th ICEST, 2021;