Metaverse: An Amalgamation of Digital Technology and Social Media

Taran Singh Bharati
Department of Computer Science,
JamiaMilliaIslamia, New Delhi, India
Taran4100@gmail.com

Abstract: Today digital technology is a very powerful tool for doing common works i.e. social media, e-shopping, e-trading, fund transferring, and for communication to the connected people. The technology is used by the people of the society for the purposes. It depends on the persons for what they use it for the benefit and for defaming the other. This is a special innovation which is serving the people conveniently at low price to fulfill the requirements. Despite of a very useful medium in the society, the same tool is being misused by some ones destructively in the society. This paper insights you how people use the medium for and how they cheat people. This paper also lets you learn about the Metaverse, a bundle of technology to let the people explore the environment and enjoy and its security, privacy, applications, how to counter measure the losses.

Keywords— Digital technology, social sites, online trading, security, malfunctioning, cheating, privacy

1. INTRODUCTION

Today people prefer using digital technology because it is convenient, worldwide accessible, reliable, time saving, etc. Nowadays everybody has everythings except the time. That is why people prefer doing online shopping, give online interviews, explore the social media sites for getting updated, depositing fee, bill, digitally. Even jobs are given digitally. There is no need to come physically and employers give advertisement digitally, people apply digitally, interviewed, results, and everything is done digitally. Since Corona-19 time, people were offered to perform their duty/work from home wherever is possible. This strategy is very effective for the employers as well as to employees. As the speed of communication system and internet is increasing day by day all such digital activities are booming. We know that every new technology brings some challenges, so digital technology is not the exception. Some new technological as well as non technical investments are needed to offer and avail contents online. Some security and privacy issues are also reported that is why clear cut guidelines are supposed to be available because they operate worldwide and keep no single controlling authority.

For the naïve people, it is very easy to be trapped by cunning attackers who are technically sound and aware off the latest technical trends. That is why inadvertent events are seen in digital technology, media, social sites, and in digital transactions.

Actual reality (AR) and virtual reality (VR) techniques are deployed as interactive technology. It is large amount of information, so there are chances of information stolen.

Attitude of the users depends on age brackets [7], 65% 50-64 age group of people used online social sites; 46% adult use OSN 65 and more aged people;70% people see Facebook daily (increasing day by day), of which 45% visit Facebook several times.

This paper provides you insights regarding the positive application, advertent misuses, and viable suggestions and solution for mitigation of losses and damages incurred.

2. DIGITAL TECHNOLOGY

Digital technology is good for human welfare, for spreading awareness of good causes, SMS, information regarding any scheme, hazards, natural calamity, regarding any stampede, atrocity, etc.Continuous improvement in its speed, convenience, accessibility,

and affordability they are becoming more powerful tool in the society.Nowadays most of the daily works are seen/ controlled digitally via internet, i.e. CCTV camera, digital watches.

2.1 Flaws of Digital Technology

On the contrary, the technology is being misused for doing digital frauds, campaigning, spreading rumors, etc. Daily online business frauds are reported about e-business sites, gaming sites, etc. Sometimes they show something and deliver some different product at home. Some of the frauds are:

i) **Cheating in Delivery:** Sites upload good quality pictures of the products. When user purchases and products are delivered to home addresses. Some low quality products are delivered.

ii) **Cheating in Prices of products:** Some companies display only the prices of theproducts to be sold. People purchase them. When these product reach home their cost become different. On asking company clarifies regarding other taxes like VAT, GST, etc. Solution: companies should be asked show/upload the all inclusive prices of the products so consumer latter should not face any difficulty.

iii) **Cheating in Tracingthe Companies:** There may be some companies which are seeing online. But if any person traces these companies once persons are deceived by their business. But companies becomeuntraceable. The address they give on websites does not exist.**Reason:**There are so many people either they are naïve or don not want to be indulged in such cases, or they may be busy in doing other businesses.

iv) **People are forced to use Digital Technology:** Whenever new technology comes sometimes is given to people get aware of it. Thereafter you in compulsion to use it whether you are willing to use it or. As innocence, people come in trap.

v) **Companies/ Organizations:** Many tomes companies increase their tariff and costs of products in favor of all the new technology. For example TC recharges and mobile recharges are increase by telecom companies against new advanced technology , digital, full HD set top boxes,4G, 5G,

2.2 Effects on Society's Character

Because technology revolution these technologies have become accessible to common people, TV Mobile, social sites, lot of material is available for everyone. TV contents are reaching to remote areas also. People are seeing videos, TV serial for frauds, crime, cheating, etc and misusing the technology. In one sense crimes and frauds have increased due to digital technology.

i) **Malfunction/Misuse of Power:** To increase the reporting of fear of violence of fear war, and image defamation or image building of some people is done by crowd source.

a) **Crowd Sourcing:** It is used for misusing the social media for the cause to criticizing the policies. Someone, by taking small data and visualizing the same to the people may set the agenda. Sometimes deliberately fake news or fake information is spreaded to instigate the emotions of the public and to divert the people from the main issues. The reporting is done by the media. This misleads to the naïve public, not all, but some people trap in the propaganda. Efforts are made so that common public can distinguish fake propaganda.

ii) **Passive Crowd Sourcing**: This is done by the state intelligence agencies for the security purposes. They keep monitoring the social media to check for violence, crime, fake, instigating news. The agencies after ensuring the involvement in nuisance activities, they nab the people to prosecute under defined law. This crowd sourcing is always done for valid tasks.

2.3 Proposed Solution of Crowd Sourcing

i) **Crowd Seeding:** Instead of considering all the reports, see, consider only authentic violence repots.
ii) **Analyzing the Violence Data:** Spatial bias and geographic violence may be covered.
iii) **Demographic Bias in Social Media Access:** There are some special tools and other facilities available in certain countries, the people of rest of the world may not ne such fateful. They can be analyzed on the bass of availability, affordability, awareness, ability, accessibility, etc.

Measurement of errors due to nature and characteristics of fear and violence: Nature, intensity, configuration and complexity, temporability.

2.4 Impact of Social Media on Privacy

People are crazy of having accounts on the social media. People knowingly or unknowingly disclose their personal information which may be misused by the hackers or attackers to decrypt the passwords and other authentic information like there location of city, age, school name, friends and mutual friends. Some information of from mutual friends can also be guessed. This leads to backward exploring of personal information. That may be useful to download documents and to make requests for documents updates without the consent of authentic users [3].

2.4.1 Proposed Solutions

i) Flood of information is available. People do not aware of technicalities, settings, and details. Old, sometimes doctored information/videos are got viral on social media. People are shown manipulated wrong facts.
ii) Affect the mental health of people: Being a social, people are forced to waste and consume their minds and hamper health by the nuisance things. Excessive use of it is very hazardous to the eyes, sleep, and overall health.
iii) Social media is making the people now unsocial. Because people have now curtailed the physical visits to their kith and kin.
iv) There are nuclear families in metro cities and parents are left no more time to look after their kids. They provide them electronic gadgets so that they can be busy in playing with gadgets and parents can obey other responsibilities. By that way kids keep busy playing with gadgets which is not good for the overall development of the minds, eyes, etc., as many kids are not willing to go for outdoor activities.

3. METAVERSE

It is the technology bundle that lets you feel and adjust your future identity. It is just like a game which allows you to enter in future and control your future [4]. This is the combination actual reality through virtual reality. This science combines, artificial intelligence, cloud, interactive technology, blockchain, and digital twins technology. The security and privacy of metaverse uses blockchain for making consistency and correctness of nodes data, smart contract to control users' assets, avoid fraud, transparency, and encryption to check the authenticity.

3.1 Features of Metaverse and Layers

Seven layers are recorded for metaverse; infrastructure, interface, decentralization of control, spatial computing, creator economy, exploring, and experience [22], [23], [27]. Some of the main metaverse features are [5]:

i) **Immersiveness:** The generated environment lets users feel psychologically and emotionally live or enjoy other virtual environment. Users interact others with senses of the bodies smells and others things. The people feel that they are fully immerged in the environment and actually feel and realize the virtual reality.
ii) **Hyper spatiotemporality:** The system is made boundary less unlike the finite real world. Users can cross the boundary and enter in space to realize the effects.
iii) **Sustainability:** Apart from the openness, it provides the economic loop and consistent high system value.

iv) **Interoperability:** It is the movement of the users and the use of the digital assets.

v) **Scalability:** Its efficiency does not get worst when number of concurrent users or avatars is increased.

vi) **Heterogeneity:** It involves the many different technologies like physical devices, sensors, communication tools, visualization and sound effect tolls, etc.

3.2 Metaverse Framework of Technologies

Metaverse keeps the AI technology, app development, human editing as framework. Metaverse is bundle of the following technologies [25]:

i) **Intearactivity:** Augmented and missed reality via AR and VR for creating interactive environment. To experience and simulate the similar or dissimilar environment from the real world environment.

ii) **Avatar:** It is icon or node which represents the character of object in computer game.

iii) **Digital Twins:** For representing the real world objects, processes, scenarios, and systems. The objects work in synchronization with the real world.

iv) **Networking:** Connecting the devices for connecting people.

v) **Artificial Intelligence:** Tool of problem solving, searching, learning, etc. knowledge graph, natural language processing, algorithms, data processing pipeline.

vi) **Human Editing:** Knowledge editing tools, standard specifications, web crawler, software.

vii) **App Development:** Website, mobile app, data storage management, server operations and maintenance, is done.

viii) **Ubiquitous Computing:** Computing by handy hand held computing devices.

ix) **Blockchain:** A public shared ledger which records all operations about which everybody in chain, is aware of [21].

3.3 Metaverse as Data World

It is a reservoir of data, received from various IoT devices. The data is processed to analyze and derive the unknown sensitive information. Following processes may be followed by metaverse to infer the unknown information [24]:

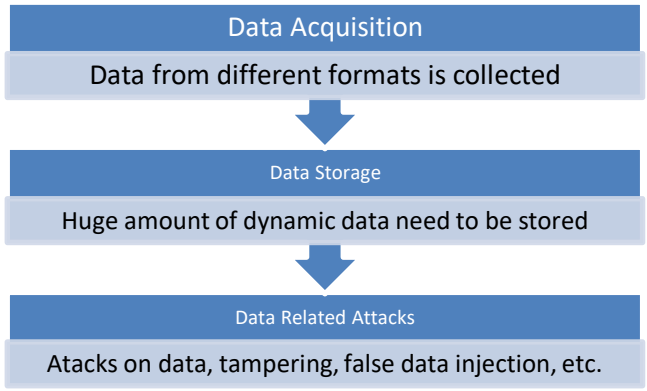

Figure: Metaverse Framework

3.3.1 Existing Applications of Metaverse

Metaverse have many applications in education, culture, telecom, real state, social goods, military, virtual events, medicine, business, manufacturing, smart city, etc., but some of the important applications are [26]:

i) **Games:** Games such as Horizon worlds, Roblox, and Fortnite are some of the popular movies.

ii) **Social Experience**: Aggregates the traditional media (text, audio, images, video) to futute online networking sites like Meta, Twiter, etc.

iii) **Online Collaboration:** New avenues for collaboration of technology for this virtual reality

iv) **Simulation and Design:** Promising 3D simulation and visualization things for objects are needed.

v) **Creator Economy:** All let the economy boom the company who develops these VR applications.

vi) **Metaverse in Medical Education:** First is augmented reality for location based services. People are connected to GPS-WiFi enabled devices like smart phone to link their location. Second is lifelogging to visit for the daily

routines of people like Twiter, Facebook, Instagram, etc. Third is mirror world to transfer the objects in mirror images.

4. SECURITY AND COUNTERMEASURES

With the technology, many people misuse and take advantage of awareness and technical superiority. By the security point of view, following security threats may be encountered [10], [11], [12], [13], [14]:

i) **Identity Theft:** People hide the actual identity for launching security attacks and it becomes very difficult to guess whose messages are received.
ii) **Impersonation Attack:** Impersonate someone else's identity to send bogus messages to consume the resources of the user.
iii) **Avatar Authentication Issue:** Judging the authenticity of intended nodes is an issue. For which we may use authentication protocols and message authentication codes (MAC).
iv) **Trusted and Interoperable authentication:** Trustworthy environment knowledge and trust of parties is good for security countermeasures.

4.1 Some Strategies are for Inferring the Personal Information

Methods to know the private information from the people via physical interaction as [6]:

i) Research question are asked to people and they can be requested to answer the questions honestly. In the answers of the questions lot of desired information is imbibed.
ii) From the questionnaires information one can identify the persons.
iii) Later we physically interact with people to see some symptomatic information and rest is acquired by asking questions to the persons.
iv) Data collected in previous steps is analyzed for making planning and strategies.

4.2 Access Control

Before allowing the user to access and use the services its identity is checked and the same is done by checking the rights assigned to the users. Some of the threats to accessibility are as**:**

i) Unauthorized access
ii) Misuser/ avatar data
iii) Self sovereign identity; identity controlled by individual users.

Some of the countermeasures of the access control areas as as centralized Identity - managed by trusted central authority, federal Identity -digital identity managed by several institutions.

Theory reasoned action (TRA): Which controls the behavior of the user. It suggests the variations in which one's normal belief affect the actual behavior. It requires attitude and subjective norms to get behavior intensions which finally makes the behavior of the people.

Theory of the planned behavior (TPB): It says that intension of the person influences the behavior of the person. The intension keeps the attitude, subjective norms for the target behavior, and perceived behavior control. Perceived behavior is sense as the individual sense. TPB includes attitude, subjective norms, perceived behavior control and these form behavior intensions and finally behavior.

Social media behavior intension = attitude+ subjective norms+ perceived behavior control.

Behavior in terms of privacy and security: Since OSN are worldwide, people interact, spare more time and share their thoughts and personal information. People develop some sense of trust between them and connect themselves emotionally and sometimes stay in relationships away from their home states. Many times they share the confidential information, i.e., pins, SSN numbers, Aadhaar card numbers, PAN numbers. From this, information about foreign partner can be accessed and see the personal information about his (her) partner. The same may accesses and misuses the information to go beyond their rights. That causes the security and privacy lapses for the national databases for banks, railways, government, and other things.The parents of the persons may be related in foreign

country. Social media security based on education, determine, evaluation, enable basis [8], [9]:

i) **Educate:**
   a. First educate the people about the cons and pros of the social media uses.
   b. Make them aware about the possible misuses, vulnerabilities and security breaches.
   c. Teach them about the privacy leakage of personal information.

ii) See the data share policy and see how much and what to share is good for you.
   a. Check the profile, review it for security settings, and see the status of the information

i) **Evaluation:**
   a. Evaluation for improving the privacy and security.
   b. Assess your privacy control mechanisms and assess its risk.
   c. Evaluate the risk and take the countermeasures.

5. SOCIAL MEDIA and DIGITAL TECHNOLOGY CREATED METAVERSE

Social media and digital technology cover some of the topics which create metaverse for the public. So many issues are raised, discussed and populated in society to place the people in metaverse, away from reality. Issues which have no more importance social media tries to divert the mind of public so that they can be busy thinking in virtual environment.

6. INFERENCES AND INDICATIONS

Because on online things, malicious software are launched to hack, spy, infect your information on the host computer. We don't know who is snooping and spying us. Because these spy software are sent by hackers and simple naive users do not aware of about them. Later such naïve users may be caught by the regulating agencies. Sometimes naïve users unintentionally go beyond their rights and they may be sacked later. People nowadays prefer using the digital gadgets minimally to feel calm and relaxed. While digital technology gives so many ease like; recordkeeping, transmission, storing, preserving, low maintenance cost, easily carrying, easily updating, cleanliness. It has difficulties; difficulty in knowing the originality of the date, reduction in employment, relying on the technology, training tools and infrastructures. Chances of manipulations are to make several copies. Vulnerable to be accessible by the Google server and it may be corrupted by the malicious code [17], [18], [19], [20].

7. CONCLUSIONS

As digital technology brought so many conveniences to ease of our daily work, so it keeps many technical glitches also. The state or agencies must educate public and spread awareness so that innocence people should not face difficulty. Metaverse is amalgamation of digital technology, AI, VR, and social media having lot of applications and difficulties. State can issue broad guidelines to both public as well as to metaverse companies to enforce them. If still there are some issues left, a timelime must set for the redressal. After that limit public must be given the compensation of their losses or damages.

References

[1.] Roberts T, Marchais G. Assessing the role of social media and digital technology in violence reporting. Contemporary Readings in Law & Social Justice. 2018 Jul 1;10 (2).

[2.] Coyne SM, Rogers AA, Zurcher JD, Stockdale L, Booth M. Does time spent using social media impact mental health?: An eight year longitudinal study. Computers in Human Behavior. 2020 Mar 1; 104: 106160.

[3.] Liu Y, Tse WK, Kwok PY, Chiu YH. Impact of Social Media Behavior on Privacy Information Security Based on Analytic Hierarchy Process. Information. 2022 May 31; 13(6):280.

[4.] Chen Z, Wu J, Gan W, Qi Z. Metaverse security and privacy: An overview. arXiv preprint arXiv:2211.14948. 2022 Nov 27.

[5.] Wang Y, Su Z, Zhang N, Xing R, Liu D, Luan TH, Shen X. A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials. 2022 Sep 7.

[6.] Zulfahmi M, Elsandi A, Apriliansyah A, Anggreainy MS, Iskandar K, Karim S. Privacy protection strategies on social media. Procedia Computer Science. 2023 Jan 1; 216:471-8.

[7.] Grace TL. *The Effects of Age on Users' Attitudes Toward Security and Privacy in a Social Media Environment: A Quantitative Study* (Doctoral dissertation, Capella University).

[8.] Cengiz AB, Kalem G, Boluk PS. The Effect of Social Media User Behaviors on Security and Privacy Threats. IEEE Access. 2022 May 30.

[9.] Yankson B, Delgado EC, Al-Jabri A, Gitin N, Davidson S. Social Media Privacy Using EDEE Security Model. International Conference on Cyber Warfare and Security 2022 Mar 2 (Vol. 17, No. 1, pp. 366-374). Academic Conferences International Limited.

[10.] Bharati, T.S.; Kumar, R., (March, 2015) "Secure intrusion detection system for mobile adhoc networks," in Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on , vol., no., pp.1257-1261, 11-13 March 2015, ISSN 0973-7529; ISBN 978-93-80544-14-4

[11.] Bharati, Taran Singh. "Enhanced Intrusion Detection System for Mobile Adhoc Networks using Mobile Agents with no Manager." International Journal of Computer Applications vol. 111 issue 10, pp. 33-35, (Feb, 2015), New York, USA, ISSN 0975 887, IF 0.704

[12.] Taran Singh Bharati , R. Kumar (Dec, 2015) . Intrusion Detection System ForManet Using Machine Learning And State Transition Analysis. International Journal of Computer Engineering & Technology (IJCET).Volume:6,Issue:12, Pages:1-8.ISSN Print: 0976 6367, ISSN Online 0976 6375, IF 8.9958, Sr No. in UGC-list: 45405

[13.] Bharati, T. S., & R. Kumar. (April, 2016). Enhanced Key Management for Mobile Adhoc Networks, International Journal of Engineering Science and Computing (IJESC), vol. 6, issue 4, pp.4184--4187, ISSN 2321 3361, IF: 5.611

[14.] Taran Singh Bharati, "Agents to secure MANETs", International Journal of Advance Engineering and Research Development (IJAERD) , Vol.: 4, Issue: 11, pp. 1267-1272, Nov, 2017, ISSN(o): 2348 4470, IISN (p): 2348 6406, IF: 4.72

[15.] Bharati T.S. (July-Aug, 2018). MANETs and Its' Security. International Journal of Computer Networks and Wireless Communication (IJCNWC), vol. 8 issue 4, pp. 166-171, ISSN 2250 3501, IF:.765,Sr No. in UGC-list:63076

[16.] Bharati T.S. (Jun, 2019). Trust Based Security of MANETs. International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8 issue 8 ,ISSN 2278 3075, pp. 792-795, IF:5.54, Scopus

[17.] Bharati T.S. (Jun, 2019). Security and Privacy of Internet of Things. International Journal of Innovative Technology and Exploring Engineering(IJITEE) , 8(8), ISSN 2278 3075, pp 2740-2743, IF: 5.54, Scopus

[18.] Bharati T.S. (Aug, 2019). Security Enhancement and Privacy Preserving of Big Data. International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.8 issue 10, ISSN 2278 3075, pp 1754-1758, IF: 5.54, Scopus

[19.] Bharati T.S. (Oct, 2019). Internet of Things (IoT): A Critical Review. International Journal of Scientific & Technology Research (IJSTR), vol.8 issue 9, ISSN 2277 8616, pp 227-232, IF: 7.11, Scopus.

[20.] Bharati T.S. (Feb, 2020). Challenges, issues, Security and Privacy of Big Data. International Journal of Scientific & Technology Research (IJSTR), vol.9 issue 2, ISSN 2277 8616, pp 1482-1486, IF: 7.11, Scopus.

[21.] Bharati, T. S. (Dec, 2021). Blockchain Technology: Architecture, Enabling Technologies, Security and Privacy. Journal of Xidian University (Scopus Indexed), Vol.15, issue.12, pp. 23-53, ISSN: 10012400, IF: 5.4, Scopus, Doi: https://doi.org/10.37896/jxu15.12/004.

[22.] Park SM, Kim YG. A Metaverse: Taxonomy, components, applications, and open challenges. Ieee Access. 2022 Jan 4;10:4209-51.

[23.] Njoku JN, Nwakanma CI, Amaizu GC, Kim DS. Prospects and challenges of Metaverse application in data-driven intelligent transportation systems. IET Intelligent Transport Systems. 2022 Aug 6.

[24.] Sun J, Gan W, Chao HC, Yu PS. Metaverse: Survey, applications, security, and opportunities. arXiv preprint arXiv:2210.07990. 2022 Oct 14.

[25.] Zhu H. MetaAID: A Flexible Framework for Developing Metaverse Applications via AI

Technology and Human Editing. arXiv preprint arXiv:2204.01614. 2022 Apr 4.

[26.] Kye B, Han N, Kim E, Park Y, Jo S. Educational applications of metaverse: possibilities and limitations. Journal of Educational Evaluation for Health Professions. 2021 Dec 13;18.

[27.] Cai Y, Llorca J, Tulino AM, Molisch AF. Compute-and data-intensive networks: The key to the Metaverse. arXiv preprint arXiv:2204.02001. 2022 Apr 5.