WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Web 3.0: The Risks and Benefits of Web 3.0 no Web 2.0, Web 1.0

Akshar Patel[1], Deep Thakar[2], Dhairya Patel[3], Akshay Dave[4], Dr. Dipesh M Patel[5], Prof. Brijesh Shukla[6]

[1,2,3,4,5,6]D.A.Degree Engineering

DOI: https://doi.org/10.55248/gengpi.2022.31203

A B S T R A C T

The internet as the most important international data media through which purchaser can percentage, read, and composes information thru pcs related to internet. In maximum current couple of years, net has had a number of development from web1.0 to web 3.0. The fundamental emphasis of the web or web 1. 0, in any other case referred to as the Exemplary net, confirmed up in 1991. Web1. 0 become tied in with associating and getting statistics at the net. Then, at that point, got here internet 2.0, empowering clients to peruse as well as make and convey content. because of the read and compose functionalities of net 2.0, there was a fantastic development within the at the web, uniquely in digital amusement close by net based totally enterprise. Web3.0 is by using and big viewed as the development of the semantic internet, wherein pc will creating and thinking new information in preference to human beings. utilizing man-made awareness and AI advances, clients will really want to speak with facts. The Metaverse is the destiny emphasis of the net. it'll consolidates numerous distinct virtual spaces that gives admittance to an assorted collection of diversion and undertakings using the overall scope of elevated reality.

Keywords:Web1.0, Web2. 0, Web3.0, Metaverse, multiplied fact, 3-D universe, virtual space, protection and safety, records secrecy. introduction The Metaverse is the destiny emphasis of the net. it'll consolidates numerous distinct virtual spaces that gives admittance to an assorted collection of diversion and undertakings using the overall scope of elevated reality. Index terms — Web1.0, Web2. 0, Web3.0, Metaverse, multiplied fact, 3-D universe, virtual space, protection and safety, records secrecy.

Introduction

Thenet and the web is not synonymous each are two separate but related issue. net is truly a community of networks in which tens of tens of millions of pc are globally related forming a network wherein any computer can speak with any other pc. worldwide extensive net is a manner of gaining access to statistics over the medium of the net with the aid of showing web pages on a browser, records are connected by using links, can incorporates textual content, pix, audio, video.

Web1. 0 is the primary generation of the internet, also regarded as informational net, which developed from 1991 onwards, following its invention with the resource of timberners-lee in 1989-1991. customers can most effective observe and proportion records on net pages in this environment. Web 1.0 became essentially an information deliver created with the aid of a small quantity of authors for a massive amount of particularly oblivious customers. It inside the fundamental consisted of static webpages with little room for authentic interactivity. Web2. 0 is the environment in which we are able to create, share, and adjust the content. The term web 2. 0 first came into use in 1999 due to the fact the net pivoted inside the path of a gadget that actively engaged the consumer. The time period web 2. 0 became tremendous after the primary O'Reilly media internet 2. 0 convention in 2004 [10]. web 3.0 is the 3rd era of the net wherein web sites and apps will be capable of technique statistics in a smart human-like way thru technology like gadget learning (ml), huge statistics, decentralized ledger technology (DTL), and so on. net three. 0 grow to be at the start known as the semantic internet via world huge net inventor timberners-lee, and turned into aimed toward being a more self enough, smart, and open internet.

on the facet of the evolution of the web3. 0, large tech structures look inside the direction of the augmented truth as the following computing platform shift. The mixing of things of the bodily and digital worlds through digital fact, augmented truth, gaming and immersive online organizations is contributing to the upward push of a extra decentralized net 3. 0. As a cease end result, the fusion of several technologies along with software application, hardware gadgets, and ar/vr/mralong side particular sound and geospatial capabilities create a new generation of generation called metaverse.

2. Web1.0 to web3.0 - evolution of the internet

Theprimary generation of the web represents the net 1.0, which, in keeping with berners-lee, is the "read-first-class internet". net 1.0 began as an records area for organizations to broadcast their facts and best allowed users to search for data and examine it via net pages. right here consumer can't have interaction with the content material of the page (no remarks, no responses, no expenses, and plenty of others).

A. The Benefits about Web 1.0

it has single get admission to, due to this that first-class the content material creator can make changes to it. As a stop result, with out the author's permission, the contents are left untouched. pupil autonomy, actual materials and scenarios, multiliteracies publicity, and a restricted diploma of interactivity are all advantages of internet 1. 0.

B. The terrible approximately Web 1.0

net programs, especially dynamic internet programs, require a immoderate degree of interactivity. We may require vehicle refresh content material retrieved from a database, in order to permit clients to get entry to up to date content in seconds. because this type of interactivity is crucial for applications, Web 1.0 failed on this vicinity, permitting simplest clicks and internet web page refreshes. wealthy individual critiques will now not be possible with Web 1.0, and we will have to refresh every time we need to test the content. furthermore, internet 1.0 packages couldn't be loaded in cell browsers (that is known as web browsing. This is but each different disadvantage of Web 1.0 era.

C. The Risks about Web 1.0

Web 1.0, with the large majority of customers being content fabric purchasers. To create their website, the creators wanted get entry to a server, want sturdy programming capabilities, and have to write huge and complicated code for creating contents. moreover, in web1.0, the facts can't be edited by way of customers, and the target market can't engage with it. As a result, there may be plenty much less visitors at the net and much less marketing and advertising and marketing. Advertisers are seeking out new approaches to hook up with their aim audiences using conventional media.

To be extra unique, Web 1.0 is a easy records portal in which users accumulate records while not having the opportunity to submit, evaluate, or offer comments. It's usually a closed website that isn't very person-high-quality. close to defining internet 2. 0, there are some things to recall. The time period refers to internet programs that permit human beings to percent and collaborate on the equal time as moreover allowing them to specific themselves on-line. in preference to web1. 0, web2.0 permits customers to now not best study however additionally write, adjust, and update content on-line. It also encourages collaboration and facilitates to gather collective intelligence.

D. The Benefits about Web 2.0

Web 2.0 facilitates great user interaction by allowing users to easily navigate through options. Web 2.0 technology, such as social networks, blogs, forums, and Second Life, could be used to achieve this simple and effective way of publicizing things.

Web 2.0 technologies allow a teacher to become a facilitator of learning rather than a distributor of information. It has the potential to create more interactive and powerful learning environments in which learners can create, produce, edit, and evaluate knowledge [13]. Web 2.0 facilitates social interactions and collaboration among students, teachers, subject matter experts, professional from various fields, and a variety of others who share common interests. With the introduction of Web 2.0 technologies, a paradigm shift has occurred from teachers and teaching to students and learning [1], resulting in "student-centered" learning [3].

Advertising on electronic media can be expensive, but using Web 2.0 technologies such as web blogs and social networks, we can reach thousands of people for less than a dollar. Companies have gained business benefits in several areas of operation as a result of using Web 2.0 technologies. It is now easier to conduct business due to improved ability to share ideas, increased access to knowledge experts, and lower costs of communication technologies, travel, and operations. Web2.0 tools have 3 also reduced the amount of time needed for marketing and expanded the marketing domain's scope. It enables businesses to more easily disseminate product information and, perhaps more importantly, to invite customer feedback and even participation in product development. The explosion of online business, or e-commerce, has resulted from Web 2.0. This prompted a number of companies to launch e-commerce ventures that make use of Internet banking, payment gateways, SEO experts, cloud product marketing, digital marketing, and other services that are now integrated into supply chain trans- actions. An increased level of employee satisfaction as well as significant improvement in customer relationship management is also observed. This was due to the companies' ability to form stronger bonds with their

customers, resulting in increased brand awareness and recall. Similar improvements can be seen in relationships with suppliers and partners. Moreover, the health and medical sector is slowly but surely beginning to embrace Web 2.0 technologies and tactics such as social networking, blogging, and sharing health information, such usage may become an everyday occurrence. This new trend is emerging under the umbrella of Health 2.0, and it has significant implications for the future of medicine. Unlike traditional e-Health technologies, that only allow web users to accept information passively, Health 2.0 provides web users with the ability to actively modify web information. Furthermore, Web 2.0 has the potential to significantly improve the state of e-health in rural communities. A comprehensive list of medical Web 2.0 applications (e.g., VesDimov's Clinical Cases and Images Blog; Ask Dr. Wiki; Ganfyd; and PubDrug) can be found in the Giustini [5] research work. Information about best Web 2.0 applications in medicine (e.g., PatientsLikeMe; Sermo; DoubleCheckMD; Vitals.com; Carol.com; and MyMedLab) can be found in research article by richardmacmanus [12]. Besides various medical websites and portals offering different medical and health services, there are various kinds of e-health systems focusing on:

- Virtual communities and online support groups are created where people can share their experiences and information about numerous diseases, while also providing emotional support to one another.
- Open source, web based Electronic Health Records (EHR) system, with a Web 2.0 facilitated e-learning component for supporting continuing medical education and promoting public awareness.
- Telehealth/Telemedicine allows doctors to see and treat patients virtually. With virtual doctor visits, people can see a doctor online and get medical advice along with necessary prescriptions. Web2.0 is rapidly becoming an important source of information for international travellers seeking travel advice and tourism supplier recommendations. Along with the web2.0 trend, the concept of "Tourism 2.0" was created to describe a new and modern way of tourism. Web 2.0 technologies, such as social networks (Facebook, Twitter, MySpace), podcasting, RSS, and others, have enabled many people who travel for tourism to obtain information and interact with tourism service providers at any time, without incurring high costs, and in a variety of ways, ranging from writing in chat rooms to audio-visual elements related to tourism demand and supply. Apart from the aforementioned areas, web2.0 has made a significant contribution to various sectors such as agriculture, online education, financial services, and so on. On the other hand, according to Billy Hoffman, lead engineer at Web security specialist SPI Dynamics. "People are buying into this web2.0 hype and throwing together ideas for Web applications, but they are not thinking about security, and they are not realizing how badly they are exposing their users."

E. The Risks about Web 2.0

Web 2.0 has are venerable to vandalism as many people have the capability to own and control data that is on the web 2.0 site. A person can intentionally damage or destroy the contents of the website including impersonation of other websites which can lead to distorted information which has raised questions on the credibility of information that is available on the sites [14].

Today's web2.0 [9] applications are openly accessible and dynamically generated; this feature of web2.0 makes it more interesting, but it also increases the risk of security breaches. Many website owners frequently re- quest that developers concentrate on functionality rather than security. As a result, developers may not always take precautions such as validating user input on web pages. As a result of their popularity and the fact that security vendors have reduced the effectiveness of other, more traditional attack vectors like e-mail attachments, these pages are attractive to hackers.

Hackers have taken advantage of Web 2.0 to distribute worms that carry out harmful operations outside of the browser, leaving users completely unaware of their actions. They also post malicious content that appears to be legitimate on social media. This could happen, for example, a User/Hacker may upload content that contains code or malware that can be used to carry out a malicious task. Sometimes hackers will upload software 4 that is supposed to be virus removal software but instead loads a Trojan horse to social networking sites like face- book (Now-a-days people are too addicted to facebook or other social networking sites and users are blindly clicking each and every link and every application and hacker takes advantage of this stupidity) or any other web sites. Hackers may upload malicious code, such as key loggers, which record victims' keystrokes, including credit card information and passwords, and send them back to the hacker.

Furthermore, since vendors have improved browser security, according to Fred Cohen, research professor at the University of New Haven and founder of the information-security consultancy Fred Cohen Associates. As a result, hacker intrusions into systems are not limited to browsers; applications like Flash, QuickTime, and inZip, which are used in many Web 2.0 sites to play video clips, view documents, and otherwise handle files, are also used by hackers.

F. The Ugly About Web 2.0

Web 2.0 is causing a splash as it stretches the boundaries of what Web sites can do. But in the rush to add features, security has become an afterthought, experts say. As a results, if a user visits an infected site, Web 2.0 worms can spread in the background of the user's browser without being visible in an open window. Web 2.0 worms like the Samy worm, which is a cross-site scripting worm (XSS worm) hit MySpace in October 4, 2005 and within just 20 hours of its release, over one million users had run the payload making Samy the fastest-spreading virus of all time.

In 2006, a new worm that targets Yahoo e-mail users is on the loose, taking advantage of one of the web2.0 tools (JavaScript) flaws. The Yamanner worm targets all versions of Yahoo Web-based mail. Yamanner arrives in a Yahoo mailbox bearing the subject header "New Graphic Site." The

computer becomes infected once the message is opened, and the worm spreads to people on the Yahoo e-mail contact list. The collected e-mail addresses are also sent to a remote online server, which Symantec believes will be used for spam campaigns.

Typically, social platform attacks gain access to users' accounts by stealing their authentication credentials when they log in .This information is then used to collect personal data from users' online friends and colleagues in a stealthy manner. A recent Stratecast study states that 22% of social media users have fallen victim to a security-related incident, and recent documented attacks support the numbers. More than 2 million user passwords were stolen by the Pony botnet, which targeted Face- book, Google, Yahoo, and other social media sites. The position of the most banned types of hacking is depicted in Fig. 2 [6]. According to Facebook, between 50 million and 100 million of its monthly active user accounts are fake duplicates, with up to 14 million of those deemed "undesirable" on the platform. moreover, businesses are also expected to use social platforms for "reconnaissance attacks," either directly or through third parties, in order to gather valuable user and organization information about competitors. Businesses can use this information to gain a competitive advantage in future business ventures (see Fig.2), and these attacks are expected to increase in 2014.

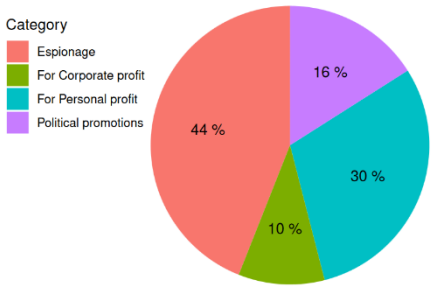

Fig. 2. Various types of hacking attacks carried out in 2021

According to a recent report, impersonation or stolen identities accounted for 91.6% of data breaches (see Fig.3). Geo-tagged photos have become increasingly popular in recent years. People tag their pictures with their geographic locations and share them on social media. Some applications have a Geo-tagging feature that automatically tags the user's current location inside a photo until the user turns it off manually. This can reveal personal information such as where one lives and travels, posing a threat to one's normal livelihood. Moreover, people who spend more time on social media are more likely to like their friends' posts. This trust is exploited by the cybercriminals. Hacking technique like Likejacking, clickjacking, etc., in which attackers place fake Facebook like buttons on web pages, phishing sites, and spam emails, is one of the most common social media attacks. The percentage of internet users in the United States who have shared their online account passwords with friends and family is shown in Fig. 4. It's broken down into age groups. According to the survey's findings, the age group of 18-30 has shared their 5 credentials, while 74% of those aged 65 and up do not share their online passwords with family or friends. With the advancement of internet tools and applications, the theft of user information and credentials is becoming more common. As of November 2020 [8], the collection of the most significant online information breaks via social media around the world is presented in Fig. 5

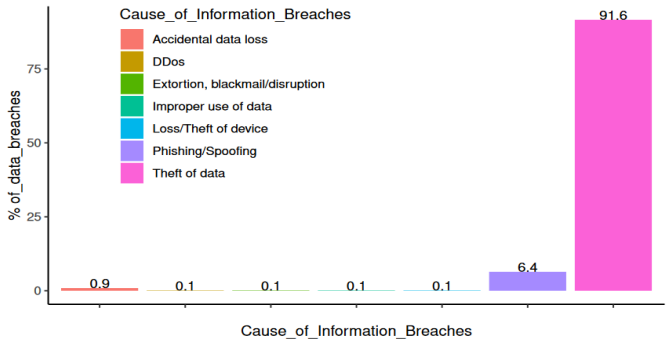

Fig. 3. Represent the most common reason for databreaches in 2020.

Fig. 4. Users who have shared passwords online with family or friends in 2020, US

The client-server architecture is one of the most significant flaws of Web 2.0 and Web 1.0. This centralized system possessed all of the data and was in charge of the lives of the users in a variety of ways. As a result, this scene poses a significant risk to people's privacy. On the other hand, a decentralized network is free from the threat of data breaching. Nobody has authority over your personal information. There won't be any centralized server. The data will be dispersed across the entire network. With the revolution of the cryptocurrency, blockchain is taking this infrastructure to a whole new level. We can now move on to decentralizing data structures from our traditional centralized system. As result, people's personal data will no longer be sold as a commodity.

G. Web 3.0- A Decentralized Web

Web 2.0 and earlier versions had centralized servers, whereas Web 3.0 has a decentralized network that is more user-centric(see Fig. 6). Web3.0 manifests itself through new technologies like cryptocurrencies, virtual and augmented reality, artificial intelligence, and more. The Web3.0 movement is being driven by a shift in how we, as a society, view and value the Internet, which is being aided by new technologies. The goal of Web3.0 is to create an Internet that works for the people and is owned by them. Web3.0 is about re-engineering existing the inter- net services and products to benefit the peoples. It can be considered as an open internet, built on open protocols and transparent blockchain networks that is accessible to all the users. Blended applications that provide convenient ways to interact with the underlying technologies could be used by consumers to interact with these protocols. It will fundamentally alter the way humans and machines interact by enabling secure data transfers, automated cryptocurrency payments, and simple ownership transfers.

H. The Benefits about Web 3.0

Despite the lack of a standardized definition for Web 3.0, it does have a few distinguishing characteristics.

- Semantic Web: Web 3.0, also known as the Se- mantic Web (as coined by Tim Berners-Lee), is the next step in the evolution of the internet, allowing it to process information with near-human intelligence by leveraging the power of Artificial Intelligence 6Centralized System Decentralized SystemDistributed System

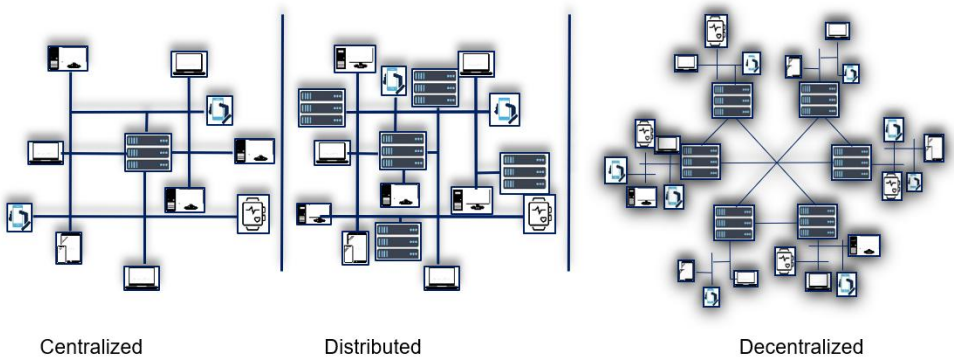

Fig. 6. Centralized vs. Distributed vs. Decentralized Systems (AI).

As a results, rather than processing text, a ma- chine can process knowledge itself, using processes similar to human deductive reasoning and inference, resulting in more meaningful outcomes. They can learn what users are interested in, help find what people want faster and understand the relationship between things.

- **Ubiquitous:** Web 3.0 will allow us to access the Internet at any time and from any location. Web- connected devices will no longer be limited to computers and smartphones at some point in the future, as they were in web 2.0. Technology will enable the development of a plethora of new types of intelligent gadgets as a result of the Internet of Things (IoT).
- **Decentralized nature:** Web 3.0 will give creators and users more freedom in general. By utilising decentralized networks, Web 3.0 will ensure that users always have control over their online data. The next version of the internet is also expected to be more reliable due to its decentralized nature, which eliminates the possibility of a single point of failure.
- **Trustless governance system:** With Web3.0, we can overcome the limitations of our traditional governance system. Our current governance system uses legal contracts to guarantee the delivery of goods and services. However, enforcing these con- tracts is a time-consuming and costly process that involves intermediaries at every step. So, while a le- gal agreement protects you, the system is inefficient and prone to mistakes and delays. Web 3.0 can address this problem by implementing a trustless (i.e. users can interact publicly and privately on the network without having to go through an intermediary, which could put them at risk) governance system based on smart contracts. Smart contracts are open-source pieces of code that have conditions that both parties agree on before they start. The contract is automatically executed once the predefined conditions are met. Using smart contracts makes services verifiable and easily enforceable. User can get services from anywhere in the world, and can pay for them directly and automatically based on the contract's. This would drastically reduce the cost of contract monitoring and transaction auditing.
- **Blockchain technology:** Web3.0 offers unprecedented levels of security and privacy to the user data. The spread of a user's data across multiple computers can raise privacy concerns. Web 3.0 solves this problem through blockchain, as there is no single point of failure. Because each node in the network has a copy of the data ledger, a hack would require the hackers to have simultaneous access to a large number of nodes. Breaching that level of security is extremely difficult and costly.
- **Digital identities:** Secure digital identities, which are a new feature of Web 3.0, also help to protect data privacy. Digital identities will be fully encrypted, anonymous, and cross-platform. User consent will be coupled to these digital identities, which means that, unlike Web 2.0, users may be asked if they want to see advertisements or not.
- **Tokenization:** Moreover, the key to the innovation in Web 3.0 is the digitization of assets via tokenization. Tokenization is the process of converting assets and rights into a digital representation, or token, that can be used on a blockchain network. Cryptocurrency and fungible tokens are forms of 7 digital currency that can easily be exchanged across networks, driving a new business model that democratizes finance and commerce. Non fungible tokens (NFTs) are units of data that represent unique assets such as avatars, digital art, or trading cards, that can be owned by users and monetized for their own gain.
- While the web 3.0 vision presents numerous opportunities for growth and development, it also raises security concerns.

I. The Risks about Web 3.0

Web3.0 has ushered in a new class of cyberthreats. While decentralized data and services reduce single points of attack, they also increase the risk of data being exposed to a wider range of threats. These involve traditional threats, as well as tactics unique to blockchain networks and interfaces.

- **Lack of oversight:** According to experts, decentralization will exacerbate the issues associated with monitoring and regulating Web 3.0. This may lead to an uptick in cybercrime, online abuse, and other issues.
- **Smart contract hacks:** Smart contract logic hacks, that targets the logic encoded in blockchain ser- vices. Attackers create their own malware, which is then distributed on the blockchain as malicious smart contract code. Malicious smart contracts have all of the standard smart contract functions, but they act strangely. Interoperability, crypto-loan services, project governance, and wallet functionality have all been targeted by these hacks. Smart contract logic hacks also raise serious legal issues, as smart contracts are often not protected by the law or are fragmented across jurisdictions.
- **Seed phrase attack:** Social engineering attacks like cloning wallets account for the vast majority of security incidents affecting Web 3.0 users. Hackers pose as customer service representatives and offer to respond to users' publicly posted Twitter or Discord server requests. Criminals will keep an eye on these channels and contact users to offer "assistance", eventually convincing them to share their seed phrases. Anyone with access to a cryptocurrency wallet's seed phrase (private key) can clone it and use it as their own.
- **Partial decentralization of dApps:** The Ethereum network, which powers the cryptocurrency ether (ETH) and provides access to thousands of de- centralized Applications (dApps), is currently the largest community-run decentralized network. How- ever, Decentralized Applications (dApps) are typically not distributed; instead, they are simply re- act websites with state and permissions stored on the blockchain rather than a centralized database. According to Moxie Marlinspike, the creator of signal and co-author of the signal protocol, point out that OpenSea, the largest NFT marketplace, removed one of his NFT, he created with no justification needed or provided, bringing light to the issue that even NFTs, a shining star of the web3.0 blockchain world, are controlled by web2.0 companies (centralized organizations). For instance, user-controlled cryptographic key management is a common feature of many blockchain technologies. User have a private key for their wallet, application, authentication server. It's devastating to lose this key, or to lose possession of this key. So many people use platforms (web2.0 platforms) such as Coinbase to act as a custodians or intermediaries to manage users private keys and

wallets. That is to say, we are not fully equipped to work with a decentralized web, but a consideration for security experts in web 3.0 will be the management of many cryptographic keys without relying on centralized organisations. Moreover, most dApps today do not authenticate or sign their API responses, imagine a decentralized bank app that doesn't do API authentication or response signing.

- **Information quality:** In Web 1.0, accuracy was based on the reputation of publishers. Web 2.0 lowered data quality, leading to the efficacy of mis- and disinformation on the web. Will accuracy checks be included in the consensus to accept machine-managed data in web 3.0? Who makes the decision, what qualifications do they have, and what motivates them to be fact-based rather than pushing an agenda?

J. The Ugly About Web 3.0

There are multiple types of attacks in the web3.0 world. The technology is still nascent, and new types of attacks may emerge. Some attacks look similar to traditional credential attacks observed on web2.0, but some are unique to web3.0. Following that, we'll go over the various types of security risks associated with web3.0.

- **Wormhole Bridge:** During the relatively short lifespan of the underlying technologies, blockchains have already seen some significant security breaches. The Wormhole Bridge is a blockchain 8 interoperability protocol that allows users and de- centralized applications to transfer assets between blockchains, create a great deal of concern among web expert.
- **Data manipulation:** Intentional manipulation of data that will be used to train AI is a major concern in terms of cybersecurity. People can make up bad data to get the results they want, making AI the largest disinformation system on the planet. For example, When Microsoft decided to train their chatbot "Tay" by allowing it to learn from Twitter, malicious tweets were sent to the machine, training it to be racist. Imagine what a nation-state could do to cause havoc by feeding AI false data or altering the meaning of words. How will cybersecurity experts identify, block, and remove data intended to deceive?
- **Data confidentiality:** Data breaches compromise confidential information constantly. On top of that, content can be released inadvertently or stored in an insecure location. When machines scan data and store it in their knowledge base, the chances of private information being found and used in- crease dramatically. To prepare for a system that has the potential to spread confidential information faster than ever before, cybersecurity leaders must strengthen their defences.
- **Enhanced spam:** In a Web 3.0 world, the vast library of integrated and interconnected metadata will create more dangerous channels through which spam attacks can spread. With websites, search engines and applications using the entire inter- net's resources as databases to serve responses to users, adversaries can target, exploit and pollute specific resources to distribute spam. These spam campaigns could deliver malicious JavaScript code or ransomware to every user by embedding it in an application. Other potential spam risks include nation-states manipulating data on web pages in an attempt to feed disinformation to AI algorithms, which then spreads to a country's citizens.
- **Cryptojacking:** With the advancement of web3.0, the risks of cryptojacking will increase. Crypto- jacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Cybercriminals hack into devices to install cryptojacking software. The software works in the background, mining for cryptocurrencies or stealing from cryptocurrency wallets. Hackers have two main methods for secretly mining cryptocurrencies on a victim's device. Firstly, by convincing the victim to click on a malicious link in an email that instalscryptomining software on their computer. Second, by infecting a website or online advertisement with JavaScript code that executes automatically once the victim's browser is loaded.
- **Rug Pull:** Rug pulls are a lucrative scam in which a crypto developer promotes a new project—usually a new token—to investors, and then disappears with tens of millions or even hundreds of millions of dollars. This particular type of fraud accounted for $4 billion in lost money for victims [4], or 38% of all cryptocurrency scam revenue in 2021, according to Chain analysis [2], a blockchain analysis company. It's a fairly straightforward process to create new tokens on Ethereum or another blockchain, and get that token listed on decentralized exchanges (DEXes), or peer-to-peer marketplaces for crypto traders, without a code audit, according to the Chainanalysis [2]. Some of the most popular rug pull scam are Squid game rug pull, which is cryptocurrency token associated with the hit Netflix series went from $2,586 to a penny [15], SnowDog rug pull [7], Mercenary rug pull [11], etc.
- **Ice phishing:** The "ice phishing" technique doesn't involve stealing one's private keys. Rather, it entails tricking a user into signing a transaction that dele- gates approval of the user's tokens to the attacker. Using an ice phishing attack, the attacker can gather approvals over time and then quickly drain all of the victim's wallets. This is exactly what happened with the Badger DAO attack that enabled the attacker to drain approximately $121 million in November- December 2021

CONCLUSION

This paper talks about the evolution of internet has been done over the Web1.0 to Web 3.0(Metaverse) . We go over each generation's strengths and weaknesses in detail. After 1989, the web has developed significantly, and it is now on its way to becoming a Huge web of highly intelligent

interaction platform. The story don't ends here . Web 1.0 is the "read-only Web," (eCommerce, Search engines, etc.) . It was a time where we use to one use search engine and get information from the internet . Afterwards the internet evolved and it takes new for called 2.0 . Web 2.0 is the "participative social Web," Web 2.0 has resulted from the Applications that they are totally built and based on the interactive Web (blogs, wikis, social networks, etc.) . Web 2.0 made communication easy and it connected the whole world virtually . Evolution of 2.0 was the one of the best evolution that happened on this earth , but still there are many disadvantages has been left in whole system we call it loop holes . So , to solve that problems and change that disadvantages into advantages scientists are developing Web 3.0 . Web 3.0 is the "read, write, execute Web." It is based on cutting-edge technologies such as Cryptocurrencies, virtual and augmented reality, AI, and More. Likewise, the Artificial intelligence is the latest addition to The emerging technologies that is most likely to grow at a rapid pace in coming years. Along with AI the concept of Metaverse is mostly likely to come in recent years or from the next decade . Nowadays the giant companies like Meta and Microsoft has started working on Metaverse and along with it they are also developing the AI so with the help of that there working has been become so easy and fast going , aside from giant companies people are starting new startups and they are also coming into the race of Metaverse . Biggest evolution of 3.0 is that , right now the world is on 2D but after Web 3.0 the whole world will be on 3D with the help of Metaverse and Web 3.0 .

Additionally , with the advancement of web technologies, There has been an increase in the number of people who Use the internet. So , due to that the data privacy and the security became the concern . Cyber attack has been increased and the world is facing lot of problems because of cyber attacks and cyber crimes . Maintaining security and privacy of data is big challenges for the companies and midst of this the Metaverse is emerging . However, with the potential for development it presents, it is crucial to address and make sure that the data privacy and security issue within the metaverse.

REFERENCES

[1] S. A. Brown, "Seeing web 2.0 in context: A study of academic perceptions," The Internet and Higher Education, vol. 15, no. 1, pp. 50–57, 2012.

[2] Chainalysis, "The 2022 crypto crime report."

[3] W. D. Chawinga, "Taking social media to a university classroom: teaching and learning using twitter and blogs," International Journal of Educational Technology in Higher Education, vol. 14, no. 1, pp. 1–19, 2017.

[4] J. Eyers, "The 'rug pull': crypto investors lose $4b in new scam," https://www.afr.com/companies/financial-services/therug-pull-crypto-investors-lose-4b-in-a-new-scam-20220111- p59nan/, Jan 11, 2022 – 1.23pm, [Online; accessed 02-May2022].

[5] D. Giustini, "How web 2.0 is changing medicine," pp. 1283– 1284, 2006.

[6] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex & Intelligent Systems, vol. 7, no. 5, pp. 2157– 2177, 2021.

[7] Joe, "First memecoin launched on Avalanche ends in $ 30 million scam," https://247newsbulletin.news/markets/53886.html, November 27, 2021, [Online; accessed 02-May-2022].

[8] J. Johnson, "U.S. internet users sharing passwords with friends and family 2016," https://www.statista.com/statistics/290525/ cyber-crime-biggest-online-data-breaches-worldwide/, 2021, [Online; accessed 02-April-2022].

[9] G. Lawton, "Web 2.0 creates security challenges," Computer, vol. 40, no. 10, pp. 13–16, 2007.

[10] T. O'reilly, What is web 2.0. " O'Reilly Media, Inc.", 2009.

[11] Reuters, "Coinbase removes cryptocurrency links after 'rug pull' warnings," https://www.deccanherald.com/business/businessnews/coinbase - removes- cryptocurrency-links-after-rugpull-warnings- 1080240.html, FEB 10 2022, [Online; accessed 02-May-2022].

[12] richardmacmanus, "Top Health 2.0 Web Apps," https:// readwrite.com/top health 20 web apps/, 21 Feb 2008, [Online; accessed 24-March-2022].

[13] W. Richardson, Blogs, wikis, podcasts, and other powerful web tools for classrooms. Corwin press, 2010.

[14] D. M. Scott, The new rules of marketing and PR: how to use social media, blogs, news releases, online video, and viral marketing to reach buyers directly. John Wiley & Sons, 2009.

[15] M. Sigalos, "There's a 'Squid Game' cryptocurrency – and it's up nearly 2,400% in the last 24 hours," https://www.cnbc.com/2021/10/28/squid-game-cryptocurrencyup-nearly-2400percent-in-the-last-24-hours.html, OCT 28 2021, [Online; accessed 02-May-2022].