World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:7, 2023

Data Security in a DApp Twitter Alike on Web 3.0 With Blockchain Based Technology

Vishal Awasthi, Tanya Soni, Vigya Awasthi, Swati Singh, Shivali Verma

Abstract—There is a growing demand for a network that grants a high level of data security and confidentiality. For this reason, the semantic web was introduced, which allows data to be shared and reused across applications while safeguarding users privacy and user's will grab back control of their data. The earlier Web 1.0 and Web 2.0 versions were built on client-server architecture, in which there was the risk of data theft and unconsented sale of user data. A decentralized version, Known as Web 3.0, that is mostly built on blockchain technology was interjected to resolve these issues. The recent research focuses on blockchain technology, deals with privacy, security, transparency, and innovation of decentralized applications (DApps), e.g. a Twitter Clone, Whatsapp clone. In this paper the Twitter Alike built on the Ethereum blockchain will replace traditional techniques with improved latency, throughput, and data ownership. The central principle of this DApp is smart contract implemented using Solidity which is an object- oriented and high-level language. Consequently, this will provide a better Quality Services, high data security, and integrity for both present and future internet technologies.

Keywords—Blockchain, DApps, Ethereum, Semantic Web, Smart Contract, Solidity.

I. Introduction

THE web has evolved considerably over time from Web 2.0 (dynamic) to Web 3.0 (decentralized web) [1]. The growing technical age has also increased the need for decentralized applications. Some of these applications are Sola (social media networking site), Decentraland (virtual world), Steemit, and Ethlance (job search and professional networking site), Secretum (a messaging app), the Brave browser and beyond that Dtube (a decentralized YouTube platform), which is exactly what we need now. In recent years, decentralization has been seen as a solution to privacy concerns, fake information, and censorship on social networking sites [2], [3]. Today, blockchain technology is the most prominent decentralized technology and was developed by Satoshi Nakamoto in 2008 and is now used in all walks of life, from hospitality to e-learning [2]-[4].

Twitter is a popular microblogging social media platform through which people converse with each other in short messages called "tweets". Twitter Alike DApp based on blockchain technology is more transparent, resilient, secure, cost-effective, and user-friendly [4]-[8] for users than the previous version of Twitter developed by Jack Dorsey in 2006. The basic implication of this clone version is decentralization and data security. This will provide confidentiality, knowing the fact that an unauthorized person can very easily access the relevant data to breach or misuse it [2]. It provides a platform for data transparency and immutability. Ownership of the data also passes directly into the hands of the public.

In Section II, the paper introduces web 3.0, its algorithm, key features, and applications, and in Section III, the paper discusses blockchains and their chronology while Section IV deals with working and types of blockchain along with their algorithm. Section V analyses the features, applications, pros and cons and challenges of blockchain. Section VI describes the proposed work by evolving a decentralized version of Twitter i.e. Twitter Alike in detail.

II. Web 3.0

Web 3.0 describes the next evolution of World Wide Web, the user interface that provides access to documents, applications, and multimedia on the internet unlike Web 1.0 and Web 2.0 as shown in Fig. 1. Web 3.0 is a decentralized semantic web. It is built on crypto networks such as Bitcoin [4], [5] and Ethereum. Due to the decentralized platform, data are distributed so the probability of a breach reduces. Web 3.0 focuses more on the innovation and convenience for the users. For example, if a user wants to create multiple data at the same time, this task can be easily implemented in Web 3.0.

Web 3.0 includes the emergence of blockchain, defi and crypto, as well as the incorporation of machine learning, artificial intelligence through cybernetic technologies, and AR/VR (Augmented reality/ Virtual reality). Some applications based entirely on Web 3.0 are IDEX, Storj, Audius, Axie infinity [15].

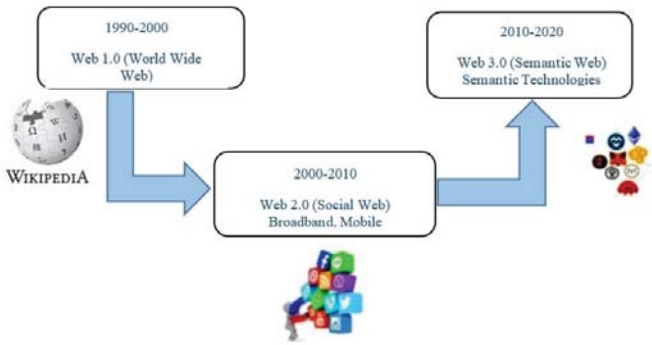

Fig. 1 Evolution in web

Vishal Awasthi, Tanya Soni, Swati Singh and Shivali Verma are with the Department of Electronics and Communication Engineering, U.I.E.T., C.S.J.M.University, Kanpur.

Vigya Awasthi is with the Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore, India (e-mail: awasthiv@rediffmail.com).

A. Algorithms in Web 3.0

1) The Consent Inspector Algorithm: The Consent Inspector Algorithm (CIA) gives a semi-automated method for capturing unique photos (i.e., website screenshots) of the website's biscuit banners. The CIA gains access to each website from an automated browser. This happens due to the default setting of our browser. Once the website is loaded in our browser, CIA accesses the main pages and takes screenshots. Then the second level of recognition is detected and the strings are matched with the string dictionary as well as if it matches, the second screenshot is created. This usually requires the user's consent [1].

2) Cookies Detection Algorithm: Cookies are small text files that websites send to your browser. This helps the website remember information about your visit and makes the website more useful to you. The CDA algorithm automatically categorizes cookies when you visit a website [1]. The cookies are categorized using the filters "simple privacy" and "fanboy-harassment". If a cookie does not ask for personal information and privacy is maintained, the CD algorithm automatically accepts the cookie without the user consent and if it threatens privacy, it is automatically blocked or rejected without the user's consent.

3) Web Beacon Detection Analysis: By using web beacons, the WEC can provide unobtrusive verification of an individual's access to certain content on a website or in an email. These web beacons are detected by the web beacon detector algorithm (BDA) [1]. BDA not only fetches the beacons detected by WEC but also points out the scripts and recognizes them accordingly.

4) Sample Categorization Algorithm: The SCA categorizes the websites according to the topics. The SCA downloads the HTML code of each website and categorizes the websites according to the strings defined in the dictionary SAC. This algorithm also increases the efficiency of the websites [1].

B. Characteristics of Web 3.0

1) Decentralisation: In Web 3.0, information or data are stored at multiple locations, unlike Web 2.0 where data were stored on a single server. This would eliminate the ownership of giants and give control to the users [1], [15].

2) Artificial Intelligence: Web 3.0 will use artificial intelligence and this will help computers understand information similar to humans through technologies and will provide better results.

3) 3D graphics: Web 3.0 will also use 3D designs in websites or games.

4) Semantic web: It allows users to create, share, and link materials and captures the meaning of words rather than keywords or numbers. Web 3.0 is one example of a semantic web.

C. Pros and Cons

1) Pros:

- Web 3.0 allows social media users to authorize and own their respective data.
- To achieve more efficient and better results, Web 3.0 provides decentralization and Decentralized Autonomous Organizations (DAOs) to its users [12], [15].
- Users get better graphics and experiences on Web 3.0.
- The combination of AI and Web 3.0 improves productivity ,economic, and social growth [15].

2) Cons:

- Users are not able to understand the conceptual functioning of Web 3.0, which leads to a lack of specific knowledge.
- Sometimes technological problems occur due to which it becomes stateless.
- Cryptocurrencies [4], [5], [7] and DeFi [7] protocols that work with Web 3.0 are already facilitating crime and money laundering. Meanwhile Crypto shows a lack of benefits in the real world.

Blockchain technology facilitates the decentralization that web 3.0 needs so in third section we will discuss blockchain.

III. Blockchain

In 1991, W.Scott Stornetta and Stuart Haber worked on the description of a chain of blocks secured by cryptography [16]. After that, several people began working on the development of digital currencies. In 2008, the first white paper on the blockchain is published by Satoshi Nakamoto which explains the model of blockchain and the hash method to timestamp the blocks [4]. After one year, he implanted the blockchain with the currency Bitcoin. At that time, experts began to realize the potential of blockchain for financial and organizational transactions.

The name of the blockchain is derived from its structure "block" and "chain". Blocks are connected in the form of a chain. It is a distributed ledger that records all transactions and related data in multiple locations simultaneously that have taken place in a chronological, secure, and immutable manner. Each node in a blockchain network keeps a carbon-copy of the ledger to avoid a single point of value, and all duplicates are reorganized and validated simultaneously. It is also as database but differs significantly because the management of blockchains is done by nodes present in peer-to-peer networks [4], [5] rather than by a server. Companies use blockchain to track products as they move through the supply chain. Blockchain based applications are more secure, reliable, cost-effective, and easier to manage [2], [3], [6], [8], [10].

A. Working Principle

The blockchain works through several processes and steps, which are as follows:

1) First, a trusted participant enters any transaction whose credibility is checked by the technology.
2) After the credibility check, a block representing that particular transaction is generated.
3) This block is distributed to every node in the network.
4) The verification of transactions and addition of blocks to the existing blockchain is done by verified nodes.
5) The changes are distributed to all networks and the transaction is completed.

B. Types of Blockchain

1) Public Blockchain:: A permission-less network where all nodes can freely access data without restriction (fully decentralized network), where no one has central authority, a fully open source platform that provides full transaction transparency. Most cryptocurrencies run on a public blockchain governed by rules or consensus algorithms. A Public blockchain is also secured with algorithms named proof of work and proof of stakes (Examples: Bitcoin [4], [8], Ethereum).

Ethereum Blockchain is a customer-developed blockchain platform that is considered an industry leading option for enterprise applications [10], [14].

2) Private Blockchain:: A permission-based network where only authorized nodes can access data. It provides a high transaction rate due to its small size and can also verify transactions in less time (examples: Hyperledger, Corda).

Financial and manufacturing industries use the Hyperledger Fabric which is a non-proprietary blockchain platform. It is used for decentralized hosting and storage of applications based on smart contracts [7], [10], [14].

3) Hybrid Blockchain:: A permission-based and permission-less network, where only a few networks are controlled by authority and remain visible to the public. The positive aspects of this type of blockchain are that it cannot be hacked, as 51 percent of users do not have access to the network (examples: Ripple network, XRP tokens).

4) Consortium Blockchain:: Also called the federated blockchain. This is a group of private blockchains, with each private blockchain owned by individual institutions. This leads to better information sharing and increases transparency and accountability [6].

IV. Algorithms of Blockchain

A. Proof of Work (PoW)

Blocks in the blockchain are generated using this algorithm to confirm transactions. The idea for Proof of Work (PoW) was first published in 1993 by Cynthia Dwork and Moni Naor [17] and later used by Satoshi Nakamoto in the 2008 Bitcoin release [4]. Cryptocurrencies such as Ethereum, Dogecoin, Monero and Bitcoin presently use PoW. This algorithm mainly focuses on:

- The algorithm checks the authorization of the transaction when it is entered.
- If the transaction is authentic, the block is incorporated into the chain that has the longest block height.
- Miners carry out some calculations to solve a complicated mathematical problem to include the block to the network as shown in Fig. 2, hence the name Proof-of-Work.

As the mathematical problem grows more complex, it becomes more challenging. Miners are special computers in the network.

POW algorithms help to verify the transaction with the help of mining, and it is more complex than the name shows, it consumes a lot of energy and time. And the most important thing is that miners also get some rewards e.g. bitcoin [11].

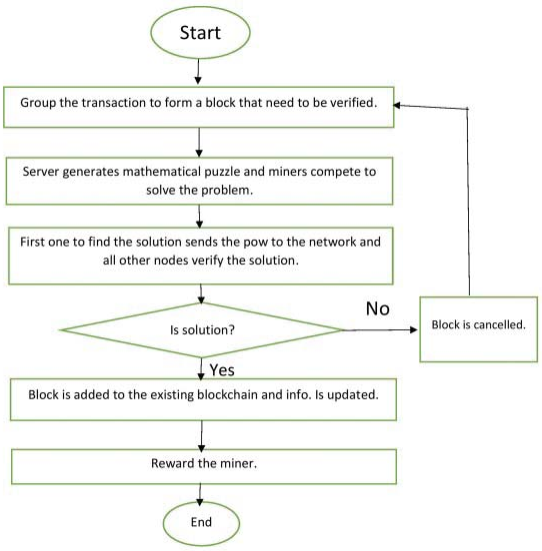

Fig. 2 Working of POW Algorithm

B. Proof of Capacity

A consensus mechanism algorithm of blockchains where nodes are allowed to operate as mining devices on the network to utilize their available disc storage space to elect mining rights and validate transactions is shown in Fig. 3.

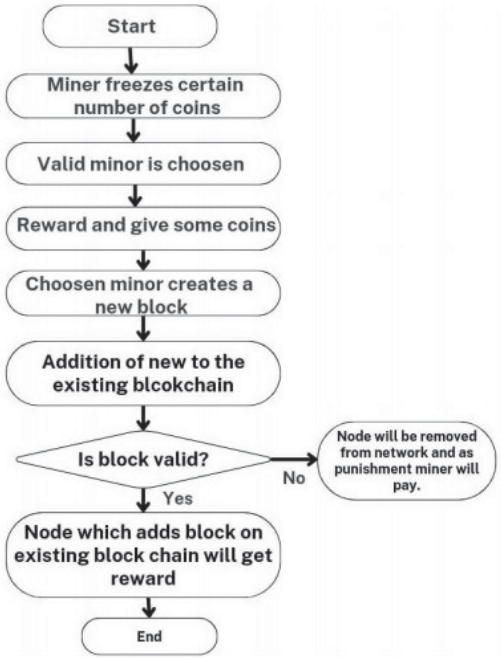

Fig. 3 Working of POC Algorithm

C. Proof of Deposit

PoD is a consensus algorithm in which a certain number of coins owned by miners are frozen during the mining process to ensure that no malicious activities are performed.

D. Proof of Elapsed Time

A consensus algorithm is designed by Intel Corporation that allows permissioned blockchain networks to determine who will create the next block. PoET works with a lottery system that distributes the odds equally for all network participants, giving each node in each network the same chance.

E. Proof of Stake

Proof-of-work is an energy-intensive algorithm (the electrical energy involved in mining a Bitcoin is quite intense). Therefore, a proof-of-stake was introduced, a consensus mechanism for the blockchain where the person with the highest stake confirms the transaction, and if more than one participant has the same stake as shown in Fig. 4, any participant is randomly selected so that it can completely replace the proof-of-work [11].

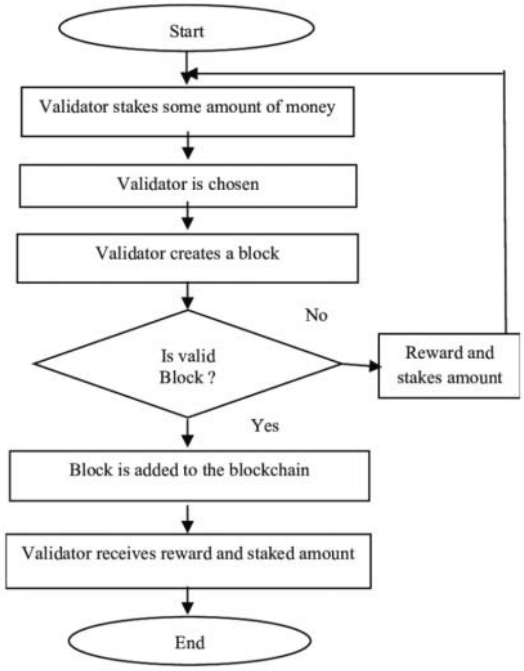

Fig. 4 Working of POS Algorithm

V. Characteristics of Blockchain

- Immutable: Immutable means anything that cannot be changed. In the blockchain, each transaction is distributed to all nodes and each node verifies the authenticity of the transaction before adding a new block. So, it is not possible to change data.
- Decentralized: There is no central authority but a group of nodes that will make all the decisions. So, there is less chance of errors.
- Transparency: Blockchain technology is transparent and everything happens in front of the user's eye, even a tiny change is quickly updated.
- Security: It is transparent, unaltered, and decentralized, which increases its security and makes it more reliable.
- No intermediaries: Users can now own their data and do not have to rely on third parties [10].

A. Recent Developments and Challenges

In 2016, Overstock.com, a retailer online, used Blockchain to distribute more shares [5]. In 2018, Ticket master, the entertainment ticketing software and services company, bought a blockchain provider to improve and advance the business [18]. In October 2020, PayPal, an online payment platform that uses blockchain, launched. In April 2021 the global entertainment company launched Tix To Me, which is based on Blockchain. The sale of non-fungible tokens, a unique digital identifier that cannot be copied, replaced or split and is recorded on a blockchain, also took off in 2001.

The challenges in blockchain are mentioned below.

1) Throughput: The throughput refers to the units of information a system can process in each amount of time. The throughput of visa is 2000tps (transaction per second) and Twitter throughput is 5000tps while the blockchain throughput is very less, it is only 7tps per second.
2) Latency: The blockchain takes nearly 10 mins to complete one transaction which is to reach its destination from the origin, which is a large amount of time.
3) Size and bandwidth: To increase the throughput of blockchain technology we need to increase the size and bandwidth which is not an easy task.
4) Security: It is still possible for Hackers to hack it when the network contains a small number of modes.
5) High power consumption: The blockchain needs a very high computational power and it leads to the wastage of resources.
6) Usability: Blockchain is a complex technology so it will be difficult for users to understand means there is a need to create a more user-friendly API.

B. Pros and Cons

1) Pros:

- Blockchain privacy and security: The blockchain is considered reliable and secure. Blocks are stored sequentially, and it is tough to change data in the block because data are distributed to each node before a change is made, which must be validated by each node.
- DLT-based transactions are more efficient than non-DLT systems, though public blockchains are sometimes inefficient.
- The failure of one node is not a problem as all other nodes have a copy of the ledger.
- It comes up with trust between participants in a network. Confirmed blocks are very difficult to change, which indicates that data cannot be removed or modified.
- By eliminating intermediaries and third parties, it reduces the costs associated with transactions.
- Increased efficiency and speed: Traditional paperwork was time-consuming, often require third-party intermediation, and also was prone to human error.

With the use of blockchain, we can overcome these shortcomings.

2) Cons:

- With the public blockchain, there is always a question mark about our ownership and we cannot question anybody if a problem arises.
- Once data are stored on a blockchain it cannot be altered and requires a lot of computing power.
- Money must be kept safe by keeping track of the private key.
- If the number of nodes eventually increases, it will be difficult for users to download the blockchain.
- It is still vulnerable to cyberattacks and crime.

VI. Proposed Work

A standard web app like Twitter runs on a system controlled by an organization which means servers have full control over the app and how it works. On a centralized site, there are multiple users, whose data are owned by a single organization. To interact with the app, you must download a copy and then send and receive data between your phone and the app's server [14]. To overcome this problem we developed a decentralized version of Twitter i.e., Twitter Alike.

A. Twitter Alike

It is a decentralized Twitter run on a blockchain or peer-to-peer network of computers where users send and respond to messages. The messages cannot be deleted once they have been posted, not even by the app creators. It allows users to transact directly with each other instead of depending on a central authority. The users of such type of applications pay an amount to the developer in form of cryptocurrency to download the program's source code. The code is termed as smart contract, which permits users to conduct transactions without revealing their personal information.

B. Smart Contract Operation

For the working of the smart contract we need to download the meta mask extension which is both a wallet and an Ethereum browser. It allows the interaction between smart contract and DApp without downloading the complete blockchain in the computer. For the deployment of smart contract on the network, users need to have some Ether in their wallet. After that user can write a smart contract on the remix browser IDE in solidity language. Then the smart contract is deployed at the Ethereum test network by pressing the deploy button at the remix window. Wait untill the transaction is completed.

Tools/libraries used in the deployment of smart contract are mentioned below:

1) Remix: Web browser-based combined development environment that permits developers to write, deploy, and execute smart contracts.
2) Solidity: An object-oriented programming (OOPs) language for writing and framing smart contracts on various blockchain networks.
3) Truffle Framework: An environment testing framework and structured pipeline for blockchains utilizing the Ethereum Virtual Machine (EVM) included in Contract Kit.

C. Features of Twitter Alike

- Since Twitter Alike uses a blockchain network with several nodes, it is more reliable and transparent than Twitter 2.0. Data loss and app crashes will therefore be less likely.
- The Twitter Alike can use tokens for transactions with centralized app, ensuring high scalability.
- In Twitter Alike, we authenticate the network through consensus algorithms.
- The character limitation can be increased on Twitter Alike as there is a character limit of 280 so it becomes difficult for users to tweet in limited characters.
- The probability of spam account is reduced due to identity authentication using NFTs.

VII. Conclusion

In this work a blockchain-based Twitter application has been developed which provides better security and integrity compare to traditional Twitter. This framework eliminates the need for central repository. Thus, in turn, improves the quality of services for the users and future technologies of the internet.

References

[1] Martinez DCalle EJove APerez-Sola C.Web-tracking compliance: websites"level of confidence in the use of information-gathering technologies: Web-tracking level of confidence. Computers and Security, (2022), 122.
[2] Zyskind GNathan OPentland A. Decentralizing privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, (2015), 180-184.
[3] Wright ADe Filippi P. Decentralized Blockchain Technology and the rise of lex Cryptographia(2015).
[4] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System.(2008)
[5] Crosby Nachiappan Pradan Pattanayak Sanjeev Verma MKalyanaraman V. BlockChain Technology: Beyond Bit-coin. (2016), Issue no.2 june 2016.
[6] Yli-Huumo JKo DChoi SPark SSmolander K.Where is current research on Blockchain technology? - A systematic review. PLoS ONE, (2016), 11(10). Doi:10.1371/journal.pone.0163477
[7] Pilkington M. Blockchain Technology: Principles and Applications. 30 September 2016, 225-253.
[8] Twesige, Richard Lee. Bitcoin A simple explanation of Bitcoin and Block Chain technology. 2015, january. Conference: Bitcoin Cryptocurrenct, Volume:1 . DOI:10.13140/2.1.1385.2486.
[9] Shubhani Aggarwal, Neeraj Kumar, Pethuru Raj. History of blockchain-Blockchain 1.0: Introduction to blockchain. Elsevier,(2021), 147-169.
[10] Huaqun Guo, Xingjie Yu. A survey on blockchain technology and its security, Blockchain: Research and Applications.(2022), Volume 3, Issue 2.
[11] Jorge Soria, Jorge Moya, Amin Mohazab. Optimal mining in proof-of-work blockchain protocols. 29 December 2022.
[12] Jake Frankenfield. Reviewed by Jefreda R. Brown. Updated January 09, 2023.
[13] Alexander A. Varfolomeev, Liwa H. Alfarhani, Zahraa Ch. Oleiw. Secure-reliable smart contract applications based blockchain technology in smart cities environment, Procedia Computer Science. 2021, Volume 186, 669-676.

[14] Yuxin Huang, Ben Wang, Yinggui Wang. Research and Application of Smart Contract Based on Ethereum Blockchain. Journal of Physics: Conference Series, 2021, january. Doi: 10.1088/1742-6596/1748/4/042016.
[15] Zarrin, Javad; Wen Phang, Hao; Babu Saheer, Lakshmi; Zarrin, Bahram (May 15, 2021). "Blockchain for decentralization of internet: prospects, trends, and challenges". Cluster Computing. 24 (4): 2841–2866. doi:10.1007/s10586-021-03301-8. Archived from the original on September 24, 2022.
[16] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
[17] Dwork, Cynthia; Naor, Moni (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". CRYPTO'92: Lecture Notes in Computer Science No. 740. Springer: 139–147
[18] Ellisngson, Annlee. "Ticketmaster buys marketing platform to help clubs engage with fans", 2018.

Dr. Vishal Awasthi received his B.E. and M. Tech. degree in the field of Electronics & Communication Engineering from Mumbai University and HBTI, Kanpur in 1999 and 2007 respectively. He has completed his Ph.D. in the field of VLSI-Digital Signal Processing. His area of interest is Digital Signal Processing & Control system. Presently he is working as Coordinator of The Department of Electronics & Communication Engineering, U.I.E.T., C.S.J.M. University, Kanpur (UP), India.

Miss Tanya Soni is Project scholar in the department of Electronics & communication Engineering, UIET Kanpur and currently Working on Decentralized Applications (Dapp). Her area of interest is Computer networking and nanorobotics.

Miss Vigya Awasthi is a driven computer science scholar who has developed a strong foundation in programming languages such as Python, Java, and C++, as well as web development technologies like HTML, CSS, and JavaScript. Her area of interest is Artificial Intelligence stream and data science.

Miss Swati Singh is Project scholar in the department of Electronics & communication Engineering, UIET Kanpur. Her area of interest is Data Science and Embedded System.

Miss Shivali Verma is Project scholar in the department of Electronics & communication Engineering, UIET Kanpur. Her area of interest is signal processing and IOT.