Peer-to-Peer Ride Sharing Services using Block chain

(G-49)

Ms. DeepShikha
Project mentor
Assistant Professor
Noida Institute of Engineering and Technology
Greater Noida, India

Karan Kanojia
1901330100132
B.Tech Ccomputer Sscience and Eengineering
Noida Institute of Engineering and Technology
Greater Noida, India

Kartik Anand
1901330100133
School of Computer Sscience and Eengineering
Noida Institute of Engineering and Technology
Greater Noida, India

Divyansh Jaiswal
19013301000105
School of Computer Sscience and Eengineering
Noida Institute of Engineering and Technology
Greater Noida, India

Abhishek Kumar
2001330109002
School of Computer Sscience and Eengineering
Noida Institute of Engineering and Technology
Greater Noida, India

***Abstract*—** Peer-to-peer ridesharing is a project that aims to build a ridesharing service by decentralizing the transactions that happen within the app and making sure that no single entity controls the transactions or the data involved in that transaction. In addition to that, the project aims to provide fair and accurate pricing by eliminating thirdparty services, by doing assuring customer privacy, and with the help of smart contracts, it is possible to automate most of the tasks and create an application-specific crypto token that can be used in the means of exchange for ridesharing service between the customer and driver.

***Keywords*— Block chain, Decentralization, Peer-To-Peer Ridesharing, Intermediaries.**

I. INTRODUCTION

Due to high demand, there is a rise in ride-sharing services, various companies are coming forward and providing ridesharing services, with their approach such as uber and OLA adopted auto-rickshaws in India along with cabs, similarly, Rapido provides ridesharing via two-wheeler, etc. But the one thing that is common between them is that they are using a centralized methodology to carry out their day-to-day operations which impose policies, rules, regulations, terms, and many conditions that are imposed on both customers and drivers.

Furthermore, to ease the user experience the ride-sharing service providers would involve mediators or third party businesses to carry out the many processes such as payment, verifications, data security, etc. With more parties involved, the more problematic with the creation of a lack of transparency, inaccurate pricing model, lack of privacy since the data will be shared with mediators, etc.

These disadvantages have led to an extensive study of blockchain technology and led to our motivation to propose a paper on solving the problems involved with centralized methodology. We tend to solve them using the decentralized methodology and by eliminating third-party involvement and automating processes using Ethereum smart contracts.

Blockchain is similar to a database that is decentralized, immutable, reliable, and distributed throughout the world. Ethereum smart contracts as the name suggest is a contract that has predefined rules, which once defines cannot be modified again, not even by admin..

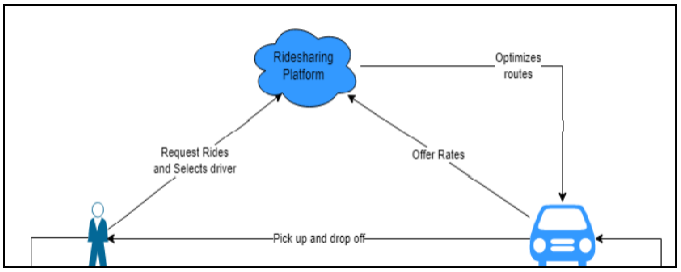


Fig 1 : peer to peer ride sharing service

II. LITERATURE REVIEW

This section is a study of seven of the most popular existent proposals of Peer-to-Peer Ride Sharing Architecture.
1. Block-V uses a built-in reputation system. In order to assure the fairness of the ride, everything regarding the ride will be permanently written into the ledger, ensuring access to all in the peer-to-peer network. With each account distinctly mapped, it prevents identity theft and when a complaint is lodged, the authorities can verify it by checking the ledger.

2. Block-VN is distributed vehicle network architecture. It examines how the network of vehicles evolves with paradigms. The department of vehicles transmits details to the revocation authority each time a vehicle registration is issued. The revocation authority then informs the distributed block chain of all information about ordinary and miner vehicle nodes.

3. B-Ride acquaints a reputation model which rates drivers built on prior behavior, allowing riders to select based on the collection of interactions of the drivers. The confirmation is done using zero-knowledge proof to protect rider/driver privacy. To ensure fair payment, a pay-as-you-drive philosophy is presented.

4. Green Ride promotes social commitments by implementing decentralization where it facilitates carbon emission reduction. It consists of two structures; centralized code that will dwell on Google Cloud App Engine and the decentralized GRTs. It leads to businesses, colleges, and government agencies reducing their annual carbon footprint.

5. PEBERS is a ride hailing service based on Ethereum. Each user is given a unique ID using which they search for a ride in the blockchain ledger using the fog mechanism. Data is stored based on Distributed Ledger Technology making it decentralized. Consensus Protocol ensures data consistency.

6. O-Ride, a privacy-preserving system optimizes SHE so that bandwidth requirements and processing overhead are lessened using ciphertext packing and transformed processing. It includes features such as credit-card payment, contacting drivers in the event of missing belongings, and traceability in the event of criminal activity.

7. Ride Matcher is an architecture where clients do not use a central database to find available rides but a peer-to-peer method i.e., forming ridesharing groups online. In this application, a node decides and executes an activity; it searches for a node whose routes match fully**.**

III. CURRENT SCENARIO OF PEER TO PEER RIDE SHARING SERVICE

Ridesharing is a facility that arranges one-way transportation on short notice through mobile apps and websites. To make the overall ride more affordable and environment friendly, the system groups users going in the same direction together and then splits the cab fare. The industry is booming, with clients ready to pay on-demand providers for convenience and a lower fee. However, there are challenges too.

The identification and subsequent addressal of these challenging factors are of utmost importance to cab service providers, before consumers lose interest.

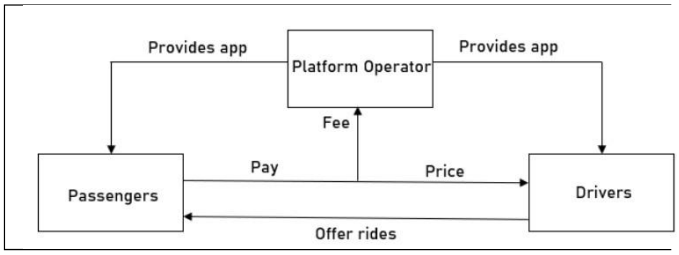


Fig: Peer-to-Peer Ride-Sharing Process

Challenges in the Ride-Sharing Industry :

1. **Cost Problems due to Intermediaries**: The booking of cabs requires third-party businesses to carry out the payment process, vehicle-tracking, etc. Each of these mediators will take a significant fee per transaction. This will not only increase the cost for the passengers but also present a cut in the drivers' salaries.

2. **Insufficient Transparency:** The existing, centralized system is managed by large companies with several levels of employees which remain unknown to both drivers and riders. Owing to the intervention of numerous unknown roles, both riders and drivers do not get any explanation behind abrupt price spikes and changes in company policy. Moreover, the database of all transactions and bookings is upheld by the company itself, making it unavailable to the public, thus unauthorizing any self-verification the riders or drivers might desire.

3. **Lack of Data Security and Privacy Mechanisms**: The company's database is home to a plethora of sensitive data including current location, phone number and home address of all the users. Even though organizations invest large amounts on user authentication and data protection, cases of false identities and data pirates hacking into the database are not uncommon.

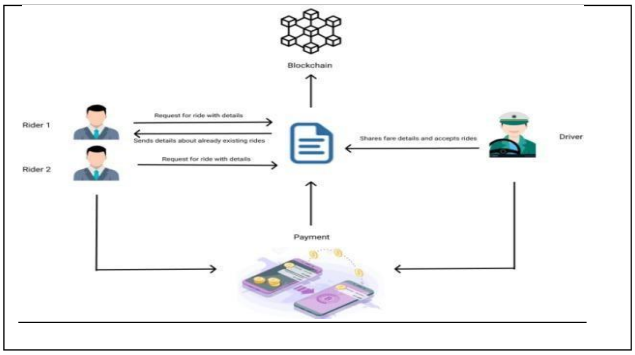
4. **Exploitation of Employees by Companies**: Ridesharing firms are currently facing a labour dilemma, arising from the fact that their relationship with employees is exploitative in nature. Firms are facing numerous lawsuits over their labour practices. Because the entire system is centralized, labour laws are framed solely by corporate executives with no consideration given to the actual employees.

5. **Trust-based Centralization:** As mentioned earlier, the company is the sole proprietor of a vast database of rider and driver information. Credibility and accountability arise from the trust vested by the users in the firm. This also means there is a single point of failure owing to the centralized nature of the organization. In other words, one dishonest employee or a single malicious attack can cause the entire system to collapse.

IV. METHODOLOGY

After reviewing the architecture of centralized ridesharing systems, our proposed system aims to tackle the various issues that riders and drivers face. It was observed how the presence of a centralized body controlling the ride-sharing application affects both riders and drivers. One of the primary reasons for this is the commission fee. In acentralized ride-sharing system, the middle man takes a commission fee from the rider leading to higher price values for riders and a lower amount (Payment done by riders - Commission) for drivers.
Centralized applications are also extremely vulnerable to hacking. If this application is somehow hacked millions of people's private information can be exposed. Decentralized cryptocurrencies and applications have a different approach. They allow users to carry their own data, as opposed to relying on centralized bodies and middlemen to secure that data in exchange for using their platforms.

Smart contracts are used to store the main details about the ride like the source, destination, price, and the public key of the user who is initiating the contract. By using this, the data is transparent, trackable and irreversible. At the same time this also ensures that the privacy of the user is not breached. The rider can share any rides from the available blockchain by paying for it via the cryptocurrencies. As soon as the transaction is complete, the changes are visible on the main blockchain and the ride can't be shared anymore.



V. IMPLEMENTATION

Our proposed system has been broadly divided into 3 modules:
User interface, Smart contracts, and backend client. The user interface is meant for the user to enter the ride details and easily share the ride. The user interface also shows the ride history which is stored on the blockchain.This ride history is visible to any user who tries to share a ride.

The smart contracts are intended to make sure that the data being entered is traceable, transparent and irreversible. The details of the rides to be shared are stored on the blockchain with the help of the smart contract and cannot be changed at any cost. This ensures that the network is safe and secured. The backend client is used to transfer the data entered by the user to the smart contract and vice versa.

The rider/driver who wants to share the ride can enter the required details and can post it on the blockchain. He then has to pay a small amount of gas fees to make sure that the transaction succeeds. The other rider can just view it from his account. If he wants to share the ride at the given cost, he can just share the ride by paying the price of the ride and the required gas fees.

VI. FEATURES

The main aim of this project is to provide a decentralized application that provides an ultimate ridesharing experience through one(peer) to one(peer) secure communication and pave way for a secure transaction between the two parties. The proposed system tries to implement the following approach through the following methods.

1. **Fair and accurate pricing model**: The main reason for variable prices depends on a number of factors such as weather, peak hours, type of vehicle, distance, number of passengers, etc. These are some of the valid parameters for the pricing algorithm to generate an accurate price for the ride. However, with the third-party involvement, there might be some additional parameters to the algorithm which in turn increases the price of the overall ride. To provide fair and accurate pricing, this project aims to eliminate third-party involvement as much as possible so that only valid parameters are considered for the pricing algorithm. Which benefits both customers and drivers.

2. **Privacy:** Since the main goal of this project is to reduce third-party involvement as much as possible, this will enable the application to securely process user data within the app and store it in the blockchain instead of funneling them through the third-party servers for further processing. By doing so, the project guarantees privacy for the user.

3. **Data integrity and security:** Since the application is decentralized where no single entity holds control over the transaction, everything is processed by smart contracts and, hence changing or modifying the data once the transaction is completed is impossible which guarantees the data integrity. In addition to that, since the data is stored in Blockchain, it is cryptographically secured, which guarantees data security.

4. **Token-based transactions:** In order to tackle the key management drawbacks of the Blockchain, the project would have a dedicated wallet within the application and uses a token called $PRI for transactions. The application wallet would securely maintain the set of key pairs that can be used for a further transaction, this would relieve the user from securing/remembering the keys every time. In addition to that, the application provides a few ways to restore the keys, if the user losses/forgets their pin. The token used here are Ethereum standards compatible, it is built using ERC20 standards, which is widely accepted by many decentralized exchanges throughout the world.

5. **Scalability:** The application tends to counter scalability issues of blockchain by sending minimal data through blockchain, meaning only textual data and object data such as images, audio, and video would be sent and maintained by IPFS storage since blockchain only handles textual data, the completion rate of the transaction would increase. This solution would be sufficient to scale the application for the first 10000 users.

VII. PROBLEM OF EXISTING SYSTEMS

1. Rideshare apps have a history of doing minimal background checks on drivers, but taxi drivers must go through more thorough security screenings that include fingerprinting and identification checks.
2. The blockage of fake requests burdens the organization and correspondence between the sender and the receiver and and can turn out to be very hard to maintain. The size of Blockchain data is quite large and therefore it can be a challenge to maintain consistent security and privacy.

3. A fraudulent driver can acquire down-payments without sticking to his/her proposition because the down-payment made by a rider goes directly to the driver once he/she confirms his/her arrival to the pick-up destination.

4. The user accounts are distinctly mapped with the reputation system. This prevents people from being anonymous, i.e., without changing their credibility score and wallet values, they cannot alter their identity.

VIII. FUTURE WORK

Although there are a few unknowns, block chain technology has the potential to revolutionize the way existent ride-sharing corporations function.
We believe that Ethereum-based crypto-equity can solve the labour dilemma that ride sharing firms are facing, where they have exploitative relationships with their employees and are facing several lawsuits over their labour practices.
With decentralization, labour laws could be framed taking into consideration the concerns and ideas of drivers. One of the most unsolvable challenges is transparency in payment.
The incorporation of the principles and ideas of bitcoin and crypto currency could revolutionize the entire industry with a foolproof layer of added credibility, accountability and reliability.

IX. APPLICATION OF BLOCKCHAIN CONCEPTS IN RIDE - SHARING

Blockchain based firmware update scheme: Autonomous vehicles manufacturers form a consortium blockchain

ensuring high availability and quick delivery of products and updates with low computational cost which is resistant to a DoS attack. Attribute-Based Encryption (ABE) generates an access policy that ensures that only approved autonomous vehicles may download and install new updates while also utilizing a smart contract to assure the validity and integrity of firmware updates. Due to the limited time required for cryptographic computations and the transfer time, the scheme can be implemented during the contact time of two moving autonomous vehicles.

Use of Zero Knowledge Proof Modules:

In a volatile environment a zero-knowledge proof protocol is utilized. In exchange for proofs of distribution from receiver AVs, each distributor can trade an encrypted version of the update. The smart contract guarantees the delivery of the decryption key, which will be revealed after the proofs are collected. Based on the received proof, the smart contract also increases the distributor's reputation.

Use of Incentives and Rewards:

A reward mechanism is designed to incentivize autonomous vehicles to distribute Firmware updates for consortium blockchain by maintaining a credit reputation for each distributor account in the blockchain.

Use of Smart Contract:

Consider a Blockchain-based service that provides smart contract templates for drivers and passengers. The two parties will choose a “basic” smart contract template initially. The parties will then agree on the transaction's specifics (For instance, the precise fee to be paid; the choice to carry more people or not;. Individuals will no longer require a third party to complete the transaction since the Smart Contract template will ensure that either both sides of the transaction are fulfilled, or none at all.

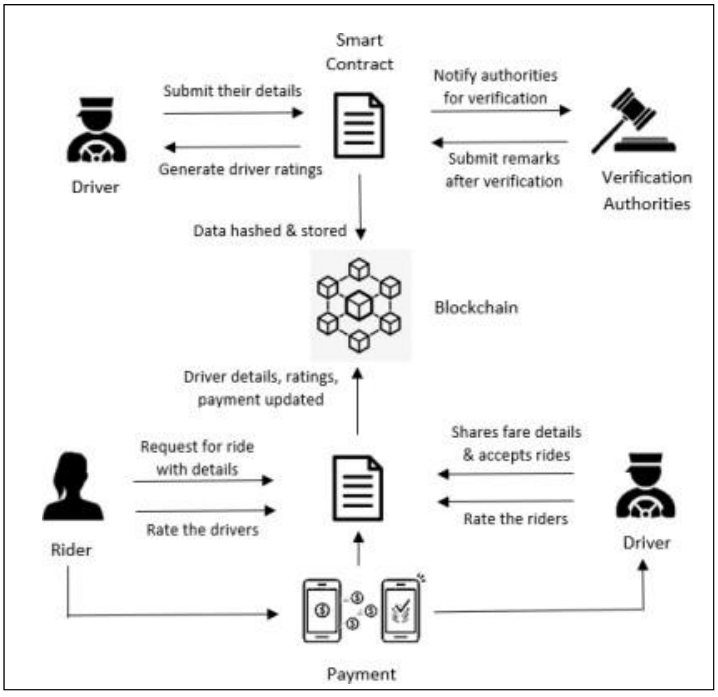


Fig:Peer-to-Peer Ride-Sharing Process

Use of Pseudonymity: Pseudonymity is defined as the usage of aliases (pseudonyms) for confidentiality for the purpose of either shielding one’s identity, achieving self-sovereignty, or for privacy and security concerns. Privacy in Blockchain refers to the preservation of anonymity and the unravelling of transactions. Transaction anonymity entails that it is impossible to connect each transaction to a unique user. Consequently, the user makes use of a unique address for every single new transaction. Unravelling makes the assumption that Blockchain addresses and transactions are not linked to the real user identities.

X. PROPOSED WORK

The application is developed using modern tools and frameworks such as NextJS, NodeJs, Redis, Metamask, Ethereum smart contracts, Web3, IPFS, AWS, Nginx, Vercel, etc. The system architecture is designed to support 100 to 500 concurrent active users at once with the support for vertical scaling in the near future.
The backend and frontend are decoupled to distribute traffic to appropriate servers to enable efficient performance on both sides, and database instances are running on managed clusters provided by MongoDB atlas, which would handle the auto-scaling, replications, and eventual consistency between the replicas, backup of the database out of the box.

We are using Amazon Web Services (AWS) as a cloud services provider to deploy and manage our application, with AWS EC2 virtual machine we deploy and manage our backend, and with Nginx as a reverse proxy, we are able to route incoming traffic from the internet to application backend running inside EC2 instance.
For the cache server, we're using Redis from AWS elasticache. The elasticache from AWS is a managed cache service where AWS would handle autoscaling, backups, optimizations, replicas, etc. The servers or the applications are accessed via a custom domain that is registered through AWS Route53. Route53 helps us with resolving DNS records when accessing the appropriate server. For example, peerride. tech would redirect to frontend, whereas api.peerride.tech would redirect to the backend server.

To implement the decentralized methodology, we're using the Mumbai Polygon testnet to build and deploy our smart contract and ERC20 token standard for our token. In addition to that, we're utilizing peer-to-peer storage such as IPFS to store objects such as images, videos, etc. In order to pin our data in IPFS, we're using web3.storage service, this acts as CDN and enables us to serve files faster.
To host for our frontend, we're using vercel which has the best support for applications built with NextJS, since vercel is the official founders and maintainers of the NextJS framework.
The main reason to choose vercel over other providers is their implementation edge functions, which would help us to serve our frontend app with very minimal latency at any place around the globe. And the edge functions run closer to the place where the user is requesting which would also help us to load appropriate components on the frontend without having the users wait.
The architecture is designed to provide efficient performance to users with low bandwidth or low network connections as well. And as mentioned earlier the application design can handle more than 100-500 concurrent users with very minimal latency and supports vertical scaling by default. In order to support horizontal scaling that can handle more than 10k to millions of users can be achieved through either replicating the same architecture with load balancers and orchestrating with Kubernetes or with the help of serverless.

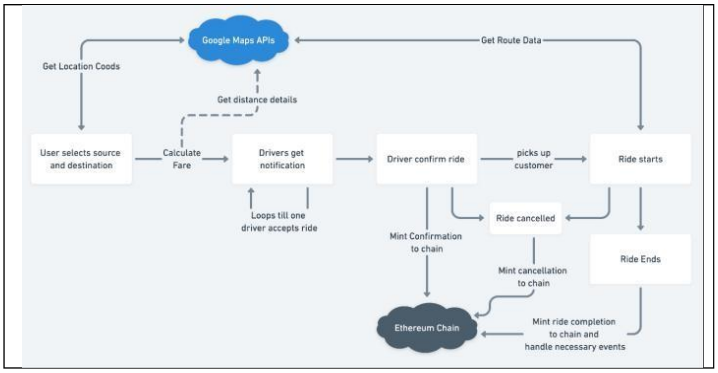
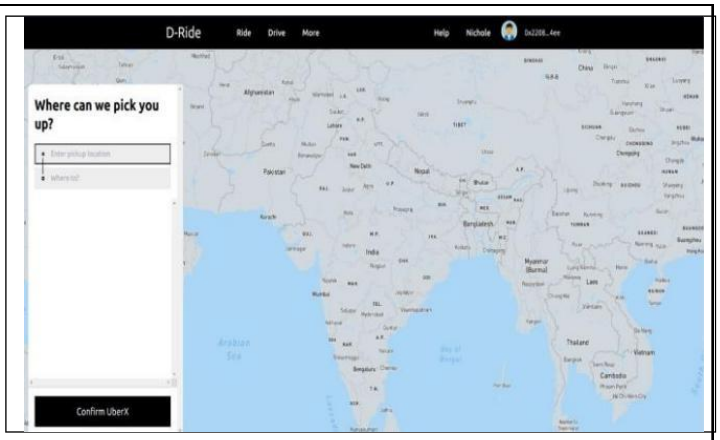


Fig: Data Flow Diagram



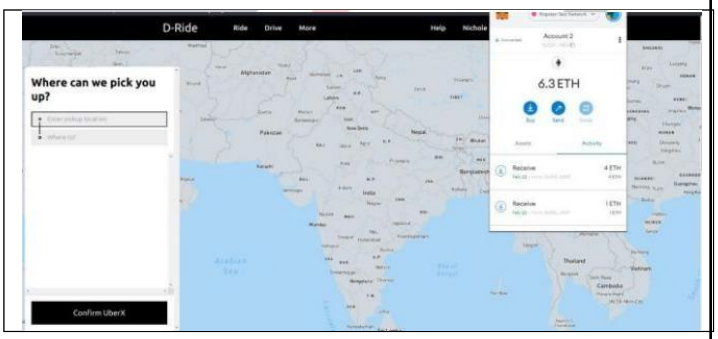


Fig: Sample Inages

XI. CONCLUSIONS

Existing ride-sharing platforms, though effective and popular, still have room for improvement in terms of pricing models, user safety, lack of transparency in transactions and data security. Blockchain enabled systems can help solve all of these issues and offer more innovative functionality with an increased ease of use and management.

Riders can connect directly with drivers via blockchain's decentralized network, thus reducing the additional costs. Because there are no intermediaries, folks with a smartphone and secure modern vehicles have more market prospects. Passengers can analyze how a ride-sharing service functions thanks to blockchain's capacity to establish accountability. Smart contracts encourage stakeholders to employ blockchain-enabled peer-to-peer leasing of automobiles for two parties directly involved based on the essential pre-decided specifications.

As a result, it provides appropriate pricing every time and the system gains credibility and transparency. The restrictions created ensure that drivers do not engage in any illegal conduct by generating an appropriate ranking for riders. For instance, blockchain technology can be developed to customize auto insurance based on particular data gathered about car usage.

Furthermore, statistical studies show that a car stays idle for a significant period of its lifetime. Blockchain offers a way of monetizing the ability of asset owners to use it at a much higher level and monetize transactions

XII. RESULTS AND DISCUSSION

1. The customers can book a ride by specifying pick up and drop location.
2. The customer will confirm the request by verifying the price and vehicle type.
3. Drivers get notified about the request and start sending acceptance requests.
4. The application will assign the driver based in First Come First Serve basis.
5. Later during the ride, updated route details will be fetched from google maps API.
6. After ride completion, the confirmation status is minted to the blockchain and ERC20 token transfers will be made automatically as payment.

XIII. ACKNOWLEDGEMENT

Our heartily thanks to the project mentor Mr Sanjay Nayak Sir, Assistant Professor, Department of CSE Noida Institute of Engineering and Technology for being a constant source of help throughout the completion of this project.

XIV. REFERENCES

- https://www.researchgate.net/publication/335241161_Blockchain_Based_Car-Sharing_Platform
- https://www.ijert.org/a-survey-of-peer-to-peer-ride-sharing-services-using-blockchain
- https://devpost.com/software/decentralized-uber
- https://www.ijsr.net/archive/v11i6/SR22608100338.pdf
- https://www.academia.edu/download/69306330/a_survey_of_peer_to_peer_ride_sharing_services_IJERTV10IS080172.pdf

plag report

ORIGINALITY REPORT

12%	10%	2%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	overcoder.net Internet Source	2%
2	ijret.org Internet Source	1%
3	global.oup.com Internet Source	1%
4	www.coursehero.com Internet Source	1%
5	isrjournals.org Internet Source	1%
6	technodocbox.com Internet Source	1%
7	journal.utem.edu.my Internet Source	1%
8	Panagiotis Leloudas. "Introduction to Software Testing", Springer Science and Business Media LLC, 2023 Publication	1%
	www.ijarcs.info	