International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

RESEARCH ON THE PRIVACY PROTECTION TECHNOLOGY OF BLOCKCHAIN SPATIOTEMPORAL BIG DATA

BIRU SHIVA [1], CHEPURI KAVYA [2], GOSIPETALA LAKSHMI NARASIMHA SWAMY [3], GUDIMALLA VIGNESH [4], POTHUGANTI DEEPAK KUMAR [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— At present, the rapid development of big data technology and the Internet of Things has led to the generation of spatiotemporal data streams on a substantial scale. In this context, data holders often opt for cloud storage of their data to mitigate the pressure of local storage and computing overhead. However, this centralized storage mode renders the data susceptible to risks of tampering and leakage due to the absence of physical control over spatiotemporal big data. Therefore, this paper devises a blockchain-based spatiotemporal big data privacy protection scheme. Initially, to ensure data privacy, the scheme adopts a storage mode where the public and side chains are coordinated. Subsequently, the irreversible SHA256 algorithm is utilized to authenticate the access nodes. Finally, AES and RSA hybrid encryption are applied to encrypt the collected spatiotemporal big data, further enhancing the security of private data. The security performance of the system was evaluated by comparing the success rate of attacks on the blockchain under various circumstances. Additionally, the system throughput of this scheme was analyzed through simulation, revealing that the service life of this system extends to a minimum of 13.79 years when 100 nodes are used. In this context, the system throughput achieves 1607 transactions/s, each node hosts 1.2107 blocks, and querying specific spatiotemporal data takes less than 2 seconds.

Index Terms – Blockchain, spatiotemporal big data, privacy protection, cloud storage, Internet of Things (IoT), AES encryption, RSA encryption, SHA-256, hybrid encryption, public blockchain, sidechain, secure data storage, data integrity, blockchain security, throughput analysis.

I. INTRODUCTION

With the increasing popularity of the Internet of Things and the Internet, a substantial volume of big data has been generated worldwide. Furthermore, the unit of data storage has shifted from the previous GB and TB to the current ZB level. According to statistics, the global big data reserves were 4.3ZB (1ZB=240GB) in 2013 and increased to 33.0ZB in 2018. This figure is estimated to reach 53.7ZB by 2021.Utilized to characterize the relative movement of participants in both space and time, spatiotemporal big data is intimately associated with personal privacy information. Common man if estations of spatiotemporal big data include shared bicycle usage records, subway card transactions, and WeChat travel data, among others. As the social economy expands and Internet technology advances, spatiotemporal big data has found extensive application across various aspects of life, significantly influencing people's basic necessities. At present, research focus on the management of spatiotemporal big data primarily centers on the storage, processing, and mining of spatiotemporal big data. With the advancement and widespread adoption of cloud computing, 5G, and Internet of Things (IoT) technology the speed of data transmission increases aiding in addressing challenges such as insufficient spatiotemporal big data storage and computing power. A pivotal solution to this challenge involves storing spatiotemporal big data in cloud storage, which offers significant computing capabilities. However, this gives rise to notable storage and computing security concerns. As an intermediary, cloud storage becomes ''transparent'' during attacks, furthermore, there is a heightened risk of privacy data leakage and tampering. Consequently, employing the traditional centralized model poses inherent risks. Spatiotemporal big data is related to the security of the country's geographical resources and has a high degree of confidentiality requirements. Spatiotemporal big data also has the characteristics of huge data volume, so it also has extremely high requirements for data throughput, and it is necessary to fully demonstrate the security performance, confidentiality performance and system throughput of the solution

Characterized by decentralization, traceability, and immutability, blockchain technology is capable of providing services such as confidentiality, integrity, and access control for spatiotemporal big data. To protect blockchain data privacy, various countries have heavily invested in conducting a series of in-depth research projects on protecting blockchain privacy. In 2000, introduced a searchable encryption scheme for the first time, attracting widespread attention. In 2019, proposed ensuring user privacy through the construction of a blockchain-enabled smart contract system. By summarizing existing blockchain data privacy protection schemes, Xu and Li highlighted their shortcomings and categorized the data based on privacy protection requirements in the blockchain. Furthermore, they proposed protecting the area using double encryption technology as part of a scheme for blockchain data privacy. In 2021, Song et al. integrated an ideal lattice-based homomorphic encryption scheme with blockchain technology, enhancing the privacy and security of user data. The growing need for enhanced private data security necessitates the development of a robust and reliable spatiotemporal big data privacy protection scheme, contributing to the security and reliability of large-capacity blockchain storage. The above solutions are not specifically analyzed in combination with the application scenarios of spatiotemporal big data. It is impossible to verify their performance in solving the security and privacy issues of spatiotemporal big data. Therefore, this paper fully verifies its security and privacy performance through simulation experiments in the spatiotemporal big data scenario. Traditional cloud services centrally store spatiotemporal big data, which poses the risk of data tampering and leakage. In order to solve this key problem, this paper proposes a spatiotemporal big data privacy protection scheme that combines public chain and side chain. The solution uses the SHA256 algorithm to authenticate visitors and uses the AES and RSA hybrid encryption mechanism to encrypt data. Through simulation verification, the reliability of the scheme is confirmed. This solution can effectively improve the security and privacy of data storage. Blockchain and spatiotemporal big data technology, and draws a blockchain-based spatiotemporal big data structure diagram.

II. RELATED WORK

A. TAB-SAPP: A trust-aware blockchain-based seamless authentication for

massive IoT enabled industrial applications

TAB-SAPP (Trust-Aware Blockchain-based Seamless Authentication for Massive IoT-enabled Industrial Applications) is an innovative framework designed to address the security and authentication challenges in the growing field of Industrial Internet of Things (IIoT). With the increasing integration of IoT devices in industrial environments, the need for a reliable, secure, and scalable authentication mechanism has become paramount. TAB-SAPP leverages blockchain technology to provide decentralized, tamper-resistant, and transparent authentication for IoT devices and users, ensuring the integrity and authenticity of communications. By incorporating trust-aware mechanisms, the system evaluates the trustworthiness of devices and participants based on their behavior and historical data, allowing for dynamic, context-aware authentication decisions. This approach enhances the security and reliability of IIoT networks, ensuring that only trusted devices and users gain access to sensitive industrial systems, while also facilitating seamless, automated authentication processes that do not hinder the efficiency of industrial operations. The use of blockchain further ensures that all authentication logs and transactions are securely recorded and immutably stored, providing a robust solution to combat the increasing number of cyber threats in industrial IoT applications.

B. Distributed timestamp mechanism based on verifiable delay functions

A Distributed Timestamp Mechanism based on Verifiable Delay Functions (VDFs) is a cryptographic approach designed to provide secure, verifiable, and efficient timestamps in distributed systems. VDFs are functions that require a specified amount of time to compute, ensuring that the output cannot be accelerated, making them ideal for applications where proof of time or sequential integrity is crucial. In this mechanism, VDFs are used to generate timestamps that are not only resistant to manipulation but can also be verified by anyone in the network without the need for centralized authorities. The distributed nature of the system ensures that no single entity can control or alter the timestamp, and the VDF's properties guarantee that each timestamp reflects a certain amount of real-time computation, providing trust and fairness in decentralized environments. This mechanism is particularly useful in applications like blockchain, distributed ledgers, and other systems that require immutable, verifiable

time records to establish the order of events or transactions. By leveraging VDFs, the system enhances security, guarantees fairness, and maintains the integrity of timestamping across multiple distributed nodes.

C. *EPPDA: An efficient privacy-preserving data aggregation federated learning scheme*

EPPDA (Efficient Privacy-Preserving Data Aggregation Federated Learning Scheme) is an advanced framework designed to enhance privacy and efficiency in federated learning, particularly in scenarios where sensitive data is distributed across multiple devices or nodes. Federated learning allows for decentralized machine learning, where data remains on the local devices, and only model updates are shared to train a global model. EPPDA further improves this approach by incorporating efficient privacy-preserving techniques to protect sensitive information during the data aggregation process. It ensures that individual data points are never directly exposed, while still enabling the model to learn from the aggregate knowledge. By leveraging encryption, secure multi-party computation, or differential privacy, EPPDA guarantees that participants' data remains confidential throughout the learning process. Additionally, the scheme is optimized for efficiency, reducing the computational and communication overhead typically associated with privacy preserving techniques, making it suitable for resource-constrained environments. This makes EPPDA ideal for applications such as healthcare, finance, and IoT, where privacy and security are paramount, and where large-scale collaborative learning is needed across multiple distributed entities.

D. *A lightweight blockchain-based remote mutual authentication for AI-empowered IoT sustainable computing systems*

A lightweight blockchain-based remote mutual authentication scheme for AI-empowered IoT sustainable computing systems offers a secure and efficient solution to authenticate devices and users in IoT networks that leverage artificial intelligence (AI) for sustainable computing. In IoT environments, where a large number of devices communicate and share data, ensuring secure authentication is critical to prevent unauthorized access and potential cyberattacks. This scheme utilizes blockchain technology to establish a decentralized, tamper-proof ledger that records and verifies authentication transactions, ensuring that only trusted devices and users can access the system. The

mutual authentication process, in which both the device and the user authenticate each other, is enhanced by AI, which can dynamically assess the risk and behavior of the devices to ensure trustworthy interactions. By leveraging blockchain's immutability and transparency, the system enables secure, scalable authentication without relying on a central authority. Additionally, the lightweight nature of the approach makes it suitable for resource-constrained IoT devices, optimizing both computational efficiency and energy consumption. This combination of blockchain, AI, and lightweight design ensures that IoT systems in sustainable computing applications remain secure, efficient, and resilient, facilitating trustworthy and seamless interactions across diverse devices and environments.

III. PROPOSED METHODOLOGY

Therefore, this paper devises a blockchain-based spatiotemporal big data privacy protection scheme. Initially, to ensure data privacy, the scheme adopts a storage mode where the public and side chains are coordinated. Subsequently, the irreversible SHA256 algorithm is utilized to authenticate the access nodes. Finally, AES and RSA hybrid encryption are applied to encrypt the collected spatiotemporal big data, further enhancing the security of private data. The security performance of the system was evaluated by comparing the success rate of attacks on the blockchain under various circumstances. Additionally, the system throughput of this scheme was analyzed through simulation, revealing that the service life of this system extends to a minimum of 13.79 years when 100 nodes are used. In this context, the system throughput achieves 1607 transactions/s, each node hosts 1.2107 blocks, and querying specific spatiotemporal data takes less than 2 seconds.

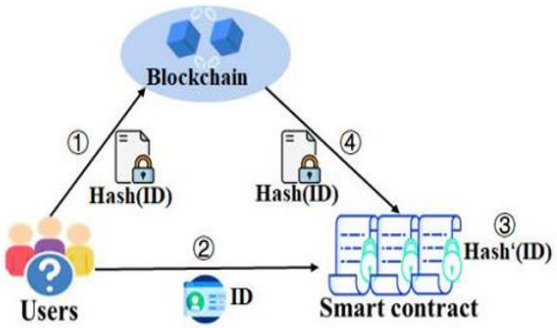
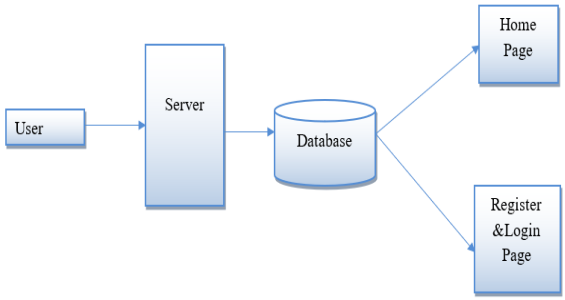


Fig. 1: System Overview

1. User Interface Design

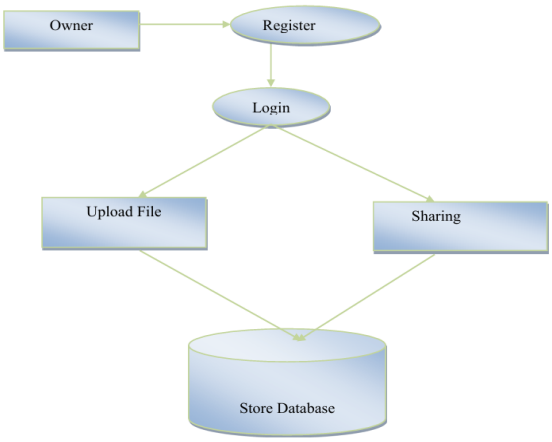
In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id,

into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.



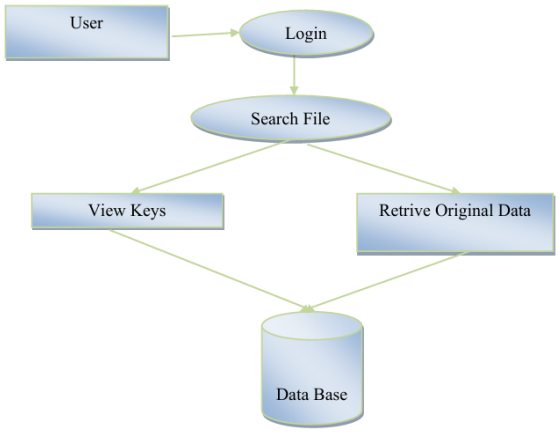
2. Owner

In this context, the owner plays a pivotal role in overseeing the development and implementation of the solution. The owner is responsible for ensuring that the project aligns with the goals of securing and preserving the privacy of sensitive spatiotemporal data, particularly given its high confidentiality requirements and extensive applications across various domains. The owner will also monitor the storage and sharing of data, ensuring that only authorized individuals have access to sensitive files, and that security measures remain intact throughout the lifecycle of the data. The owner will upload the text file and that file will be encrypted by using aes and rsa algorithms.



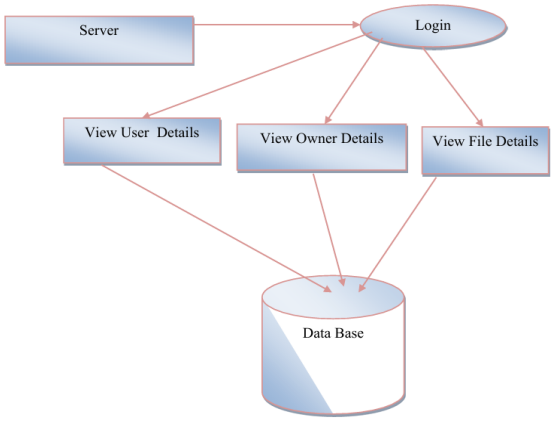
3. User

The user plays a critical role in interacting with the spatiotemporal big data privacy protection system, leveraging its enhanced security features for secure data storage and retrieval. Users are granted access based on the access control policies defined by the server, and they are provided with the necessary decryption keys to retrieve the query results. When a user submits a search query, they provide the relevant private key to search through the encrypted data stored in the database.



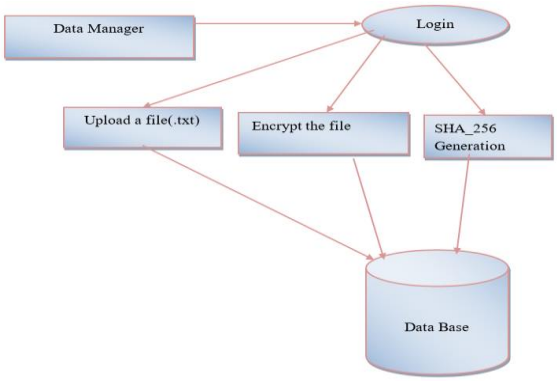
4. Server

The server acts as the administration in this project where he will have all the user details, all the owner details and all the file details and he can retrieve all the information present in user and owner database. He has the right to check whatever the files uploaded by the owner also. He can retrieve all the file details uploaded by owner also. Server is responsible for giving access to user and owner requests. Therefore, here server will have the all the information about users and owners and files uploaded by owners also.



5. Upload

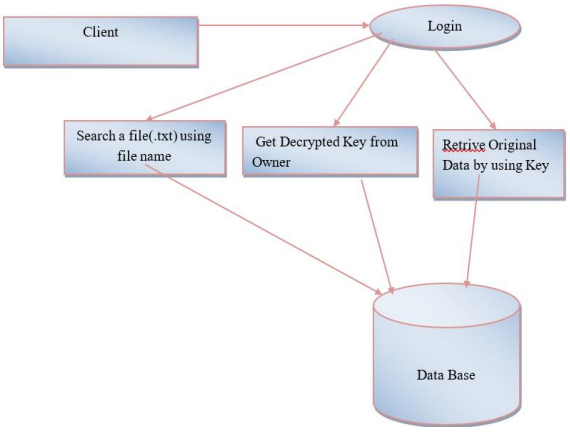
When a user uploads a file, the system first generates a dynamic AES key specifically for that file, ensuring that each file is encrypted with a unique and constantly changing encryption key. This dynamic key management mechanism strengthens file-level security by reducing the risk of decryption even if one key is compromised. Additionally, the encryption process is further enhanced by utilizing Elliptic Curve Cryptography (ECC) during the transmission of the file, ensuring that the file is securely encrypted during the upload process, protecting it from unauthorized interception.



6. Search

When a user initiates a search for a particular file, the system ensures that only authorized users can access the file by verifying their credentials and ensuring that the encryption keys necessary for decryption are securely retrieved. As the files are stored with unique dynamic AES keys, the search process

includes a mechanism that checks the file's associated metadata and verifies the correct key for decryption. The search process is, therefore, designed to be both secure and efficient, ensuring that users can retrieve their files while maintaining confidentiality and integrity.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed blockchain-based privacy protection framework effectively secures spatiotemporal big data using SHA-256 authentication and AES-RSA hybrid encryption.

The system achieved a throughput of 1607 transactions per second, with data query times below 2 seconds. Simulation results also indicate a minimum system service life of 13.79 years with 100 blockchain nodes. Overall, the framework provides secure, efficient, and scalable privacy protection for cloud-based spatiotemporal big data.



Fig. 2: Home Page

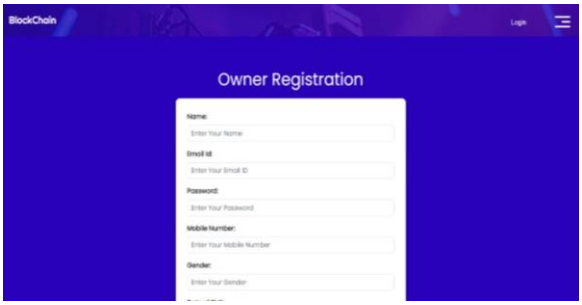


Fig. 3: Registration

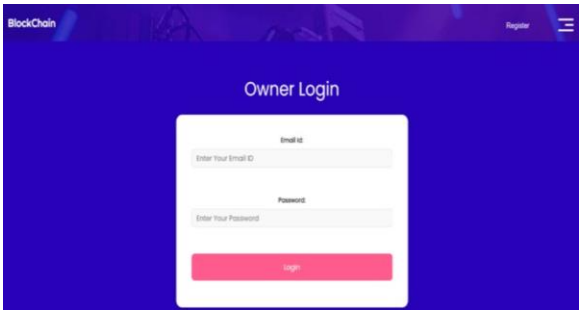


Fig. 4: Login

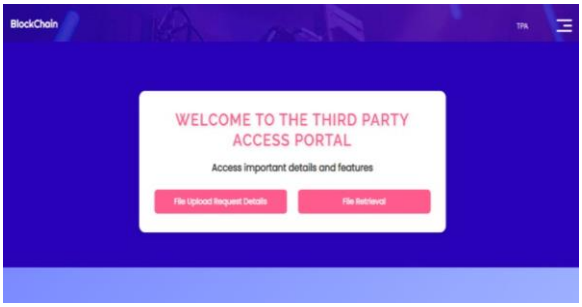


Fig. 5: Third Party Portal

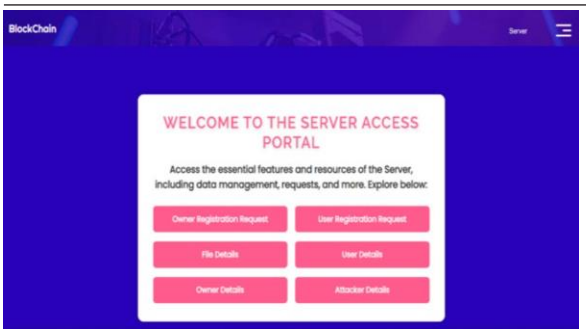


Fig. 6: Server Access Portal

V. CONCLUSION

This paper proposes a spatiotemporal big data privacy protection scheme based on blockchain technology. Unlike existing schemes, this approach partitions the blockchain to safeguard private data, acknowledging that no encryption scheme can guarantee absolute security. It implements classified protection. The inevitable leakage of some spatiotemporal data necessitates minimizing sensitive information exposure during transactions. The scheme presented herein is applicable to various spatiotemporal data scenarios. The rapid development of blockchain technology simplifies system implementation, significantly reducing development and operational costs. Furthermore, this enhances the scheme's promotability. Beyond enhancing data transmission capabilities, the hybrid AES and RSA encryption ensures the security of the system solution. Concurrently, an irreversible hash algorithm authenticates access nodes, thereby verifying node identities. The system's security performance is evaluated by comparing the success rate of attacks on the blockchain under various conditions. Simulation analysis of this scheme's system throughput reveals a minimum service life of 13.79 years with 100 nodes, and the time required to query specific spatiotemporal data is less than 2 seconds.

REFERENCES

[1] Y . Ren, F. Zhu, J. Wang, P. K. Sharma, and U. Ghosh, ''Novel vote scheme for decision making feedback based on blockchain in Internet of Vehicles,''IEEE Trans. Intell. Transp. Syst., vol. 23, no. 2, pp. 1639–1648, Feb. 2022.

[2] T. Wang, Q. Yang, X. Shen, T. R. Gadekallu, W. Wang, and K. Dev, ''A privacy-enhanced retrieval technology for the cloud-assisted Internet of Things,'' IEEE Trans. Ind. Informat., vol. 18, no. 7, pp. 4981–4989,Jul. 2022.

[3] B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, W. Wang, and N. M. F. Qureshi, ''TAB SAPP: A trust-aware blockchain-based seamless authentication for massive IoT-enabled industrial applications,'' IEEE Trans. Ind. Informat., vol. 19, no. 1, pp. 243–250, Jan. 2023.

[4] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, and C. Su, ‘‘Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps,’’ IEEE Trans. Ind. Appl., vol. 58, no. 5, pp. 5616–5623, Sep. 2022.

[5] C. Ge, Z. Liu, J. Xia, and L. Fang, ‘‘Revocable identity-based broadcast proxy re-encryption for data sharing in clouds,’’ IEEE Trans. Dependable Secure Comput., vol. 18, no. 3, pp. 1214 1226, May 2021.

[6] Q. Wu, Z. Han, G. Mohiuddin, and Y. Ren, ‘‘Distributed timestamp mechanism based on verifiable delay functions,’’ Comput. Syst. Sci. Eng., vol. 44, no. 2, pp. 1633–1646, 2023, doi: 10.32604/csse.2023.030646. [Online].Available: http://www.techscience.com/csse/v44n2/48294.

[7] Y. Ren, J. Qi, Y. Liu, J. Wang, and G.-J. Kim, ‘‘Integrity verification mechanism of sensor data based on bilinear map accumulator,’’ ACM Trans. Internet Technol., vol. 21, no. 1, pp. 1–19, Feb. 2021, doi:10.1145/3380749.

[8] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, ‘‘Revocable attribute-based encryption with data integrity in clouds,’’ IEEE Trans. Dependable Secure Comput., vol. 19, no. 5, pp. 2864 2872, Sep. 2022,doi: 10.1109/TDSC.2021.3065999.

[9] J. Song, W. Wang, T. R. Gadekallu, J. Cao, and Y. Liu, ‘‘EPPDA: An efficient privacy preserving data aggregation federated learning scheme,’’ IEEE Trans. Netw. Sci. Eng.

[10] L. Fang, M. Li, Z. Liu, C. Lin, S. Ji, A. Zhou, W. Susilo, and C. Ge, ‘‘A secure and authenticated mobile payment protocol against off-site attack strategy,’’ IEEE Trans. Dependable Secure Comput., vol. 19, no. 5, pp. 3564–3578, Sep. 2022, doi: 10.1109/TDSC.2021.3102099.

AUTHORS Profile



Mr. BIRU SHIVA has received his B. Tech CSE from JNTUH, Hyderabad in 2013, M. Tech in Computer science and engineering from JNTUH, Hyderabad in 2016 and He has been dedicated to the teaching field for the last 6 years. present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. CHEPURI KAVYA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GOSIPETALA LAKSHMI NARASIMHA SWAMY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GUDIMALLA VIGNESH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. POTHUGANTI DEEPAK KUMAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.