American Journal of Computer Science and Technology
2026, Vol. 9, No. 1, pp. 1–7
https://doi.org/10.11648/j.ajcst.20260901.11

Research Article

System and Methods in Building a Blockchain-based System for Covert Steganographic Communication

Babu Santhalingam[1], **Shreemathi Vedantarajagopalan**[2], **Magesh Kasthuri**[3, *]

[1]Department of Computer Science and Applications, SCSVMV University, Kanchipuram, India
[2]Department of Mathematics and Sciences, University of Technology and Applied Sciences, Nizwa, Oman
[3]Technology Services, Wipro Limited, Bengaluru, India

Abstract

The increasing importance of privacy and secure communication in distributed environments has fueled research into innovative solutions that combine data concealment and tamper-resistant recordkeeping. This article presents a logically structured architectural framework for covert steganographic communication, utilizing the Microsoft Azure web3 ecosystem as its foundation. The motivation behind this research stems from the limitations of traditional steganography and blockchain technologies when used independently, particularly in addressing the challenges of operational transparency, scalability, and robust data protection. To bridge these gaps, the proposed system integrates Azure Blockchain Development Kit with other Azure native services to provide a unified architecture. This research article introduces a pioneering architectural framework designed to facilitate covert steganographic communication through blockchain technologies, with a focus on leveraging the Microsoft Azure web3 ecosystem. By integrating Azure Blockchain Development Kit (BDK), Azure Confidential Ledger, Azure Blockchain Services, and Azure Blockchain Workbench with Open Steganography solutions deployed on Azure Virtual Machines (VM), the proposed system aims to achieve secure, confidential, and unobtrusive data exchange. The research methodology encompasses a comprehensive literature review, system design, implementation, and rigorous security analysis, followed by experimental evaluation on cloud infrastructure. By leveraging the strengths of Azure's blockchain and confidential ledger capabilities alongside advanced steganographic techniques, this study demonstrates a practical approach to achieving secure, confidential, and unobtrusive data exchange. The findings confirm the feasibility and effectiveness of the proposed solution, highlighting its potential to facilitate adaptive, scalable, and privacy-preserving covert communication networks. In conclusion, this work charts new directions for integrating blockchain and steganography within cloud-native platforms, offering enhanced privacy and security for sensitive communications in distributed settings.

Keywords

Blockchain, Steganography, Covert Communication, Web3, Microsoft Azure, Confidential Ledger, Open Steganography, Secure Data Exchange, Privacy, Confidentiality

*Corresponding author: magesh.kasthuri@wipro.com (Magesh Kasthuri)

Received: 4 December 2025; **Accepted:** 23 December 2025; **Published:** 19 January 2026

1. Introduction

Covert communication, the practice of transmitting information in a manner that conceals both the message and the act of communication itself, is critical in contexts where privacy, confidentiality, and deniability are paramount. Steganography and blockchain technologies have separately advanced the domains of secure information hiding and distributed trust, yet their integration remains underexplored. The proliferation of cloud-native web3 platforms, such as Microsoft Azure, offers unprecedented opportunities to synergise these fields for practical and scalable solutions. This paper proposes an architectural system that leverages Azure's blockchain services and Open Steganography tools to realise a covert communication infrastructure, addressing challenges in security, scalability, and operational transparency.

2. Literature Review

The convergence of blockchain and steganography has garnered increasing academic attention. Blockchain's immutable, decentralised ledger as explained in the study [1] provides a trustworthy substrate for recording transactions, while steganography enables data concealment within innocuous carriers as in the study [2]. Prior works have explored steganographic techniques in digital media, network protocols, and cloud environments as proposed by the research work [3]. Blockchain-based confidentiality mechanisms, such as zero-knowledge proofs and confidential ledgers, have been proposed for privacy-preserving applications [4]. Several studies have examined the use of smart contracts for secure data exchange, and the deployment of blockchain solutions on cloud platforms for scalability as in the study [4].

The integration of steganography with blockchain was first conceptualised, where hidden messages were embedded within blockchain transactions as in the study [5]. More recent efforts have explored the use of distributed ledgers to manage steganographic keys, and the application of web3 development frameworks for secure communication as in the research work [6]. Azure Blockchain Services have been evaluated for enterprise-grade confidentiality as proposed by the system in [6]. While Azure Confidential Ledger has demonstrated tamper-proof record-keeping as proposed in the work [7]. Open Steganography tools have been used for covert image and text transmission as in the study [8], and their deployment on virtualised infrastructure has been assessed in the study [9].

Despite these advances, gaps remain in the seamless integration of steganography with scalable, cloud-hosted blockchain platforms as compared in the work [10]. Existing research lacks comprehensive architectural blueprints for such systems, particularly those incorporating web3 development kits and confidential ledgers as observed in the study [11].

The work proposed in [12] delves into the intricacies of leveraging blockchain technology to enhance digital trustworthiness. The authors discuss how blockchain's decentralised structure can foster greater transparency and accountability in data transactions. Their work also highlights potential challenges in integrating blockchain frameworks with traditional systems, emphasising the need for adaptable solutions tailored to diverse organisational requirements.

The study in [13] explores advanced steganographic techniques, specifically focusing on embedding hidden data within multimedia files. The researchers present a comparative analysis of different algorithms, weighing their effectiveness and resistance to detection. Their findings offer valuable insights into the ongoing evolution of steganography, with particular attention paid to improving both security and efficiency similar to work done in [14].

In the research work [15], the authors investigate the deployment of cloud-based confidentiality protocols using blockchain as the foundational layer. The study reviews various privacy-preserving mechanisms—such as encryption and anonymisation—and assesses their suitability for large-scale cloud environments. The authors' insights underscore the critical role of blockchain in reinforcing the confidentiality and integrity of distributed applications.

This research paper examines the use of smart contracts for automating secure data exchanges across decentralised platforms. The authors provide detailed case studies illustrating how smart contracts can enforce compliance and streamline workflows. Their analysis also considers potential vulnerabilities, suggesting best practices for mitigating risks associated with automated contract execution.

The work proposed in [16] offers a thorough assessment of virtual machine-based deployments for open-source steganography tools. The article discusses the benefits of scalability, resource isolation, and ease of management when running steganography solutions on cloud-hosted virtual machines. It also evaluates the performance and reliability of various configurations, contributing to the body of knowledge around practical implementation strategies.

The study proposed in [17] investigates the application of zero-knowledge proofs in blockchain networks to ensure transaction privacy. The authors articulate the theoretical underpinnings of zero-knowledge protocols and demonstrate their use in real-world blockchain applications. Their work highlights the balance between privacy and computational overhead, offering guidance for developers aiming to adopt such techniques.

There is a similar work with a comprehensive framework for integrating web3 development tools with confidentiality services as in the study [18]. The authors explore how web3 Application Programming Interface (APIs) and Software Development Kit (SDKs) can be utilised to build privacy-centric decentralised applications, noting the challenges of interoperability and standardisation. Their contributions serve as a roadmap for developers seeking to harness the full potential of the emerging web3 ecosystem.

The research work proposed in [18] examines tamper-proof record-keeping solutions using confidential ledgers in blockchain environments. The researchers evaluate various ledger architectures, highlighting their strengths in terms of data integrity, access control, and resistance to unauthorised modifications as explained in the study [19]. They further discuss real-world use cases where confidential ledgers have enhanced the trustworthiness of critical systems.

The reference work in the series of research in [20] investigates the scalability challenges associated with integrating steganography and blockchain technologies. The authors propose optimisation strategies focused on resource allocation and transaction throughput. Their work contributes to a better understanding of how to build robust, scalable systems that preserve privacy without compromising on performance.

This paper synthesises insights from these foundational studies, each contributing to the understanding of blockchain-steganography integration, Azure platform capabilities, and secure covert communication.

3. System Architecture

The proposed architecture combines Azure's blockchain ecosystem with Open Steganography tools to enable covert, confidential communication. The system comprises the following components:

Azure Blockchain Development Kit: Provides APIs, connectors, and templates for building decentralised applications (dApps) and integrating smart contracts with external data sources.

Azure Confidential Ledger: Offers a tamper-proof, confidential record-keeping ledger, ensuring data immutability and privacy.

Azure Blockchain Services: Delivers managed blockchain networks and infrastructure for deploying, scaling, and monitoring dApps.

Azure Blockchain Workbench: Facilitates rapid prototyping and deployment of blockchain applications with built-in identity, workflow, and integration capabilities.

Open Steganography on Azure VM: Utilises open-source steganography libraries (such as OpenStego) deployed on Azure VMs to embed and extract covert messages within digital media.

The system workflow begins with the generation of a covert message using Open Steganography tools on an Azure VM as shown in below Figure.

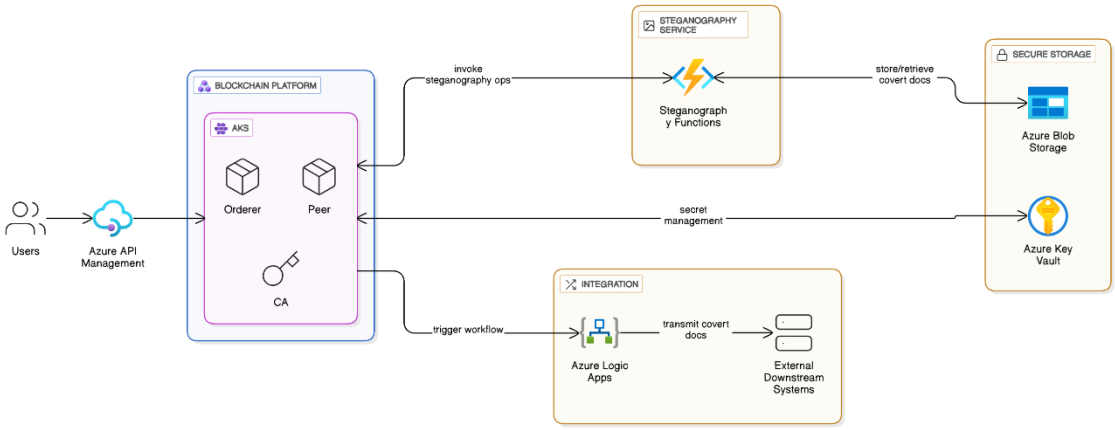

Figure 1. *Azure architecture for Steganography implementation.*

The steganographically encoded data is then transmitted via transactions on a managed Azure blockchain network. Azure Confidential Ledger ensures that transaction records are encrypted and tamper-resistant, while the Blockchain Development Kit and Workbench streamline integration with identity management, access control, and monitoring services. The architecture supports web3 interfaces, enabling decentralised access and smart contract-driven automation.

The architecture depicted in the above diagram is designed to provide a comprehensive understanding of how the various elements within the system interact to achieve its intended functionality.

3.1. Core Components of the Architecture

3.1.1. User Interface Layer

At the forefront of the architecture lies the user interface (UI) layer. This is where end-users interact with the system, typically through web or mobile applications. The UI is responsible for presenting information clearly and intuitively, capturing user inputs, and ensuring a seamless user experience. This layer often communicates with backend services through secure APIs.

3.1.2. Application Layer

Sitting just behind the UI is the application or business logic layer. This layer processes requests from the user interface, enforces business rules, and orchestrates the flow of data between the UI and data storage systems. It acts as the brain of the application, handling computations, validations, and complex business operations.

3.1.3. Data Layer

At the foundation of the architecture is the data layer, which is responsible for storing, retrieving, and managing all necessary information. This layer typically comprises databases—relational or NoSQL—chosen based on the system's requirements. The data layer ensures the integrity, security, and availability of data for the application.

3.2. Integration and Communication

Modern architectures often incorporate integration components such as APIs, message queues, or service buses. These facilitate smooth communication between different modules or with external systems. Such integrations ensure modularity, scalability, and the ability to interact with third-party services or microservices with ease.

3.3. Security and Monitoring

Security is embedded across all layers, employing mechanisms such as authentication, authorisation, encryption, and regular audits. Monitoring tools and logging frameworks are also integrated to track system health, performance, and potential issues, thus ensuring reliability and quick incident response.

3.4. Workflow and Interactions

When a user initiates a request, it flows from the user interface to the application layer, where it is processed according to defined business logic. The application layer may then interact with the data layer to fetch or store information. Any required communication with external systems happens via the integration components. Throughout this process, security checks and monitoring ensure the system operates safely and efficiently.

In summary, the proposed architecture is thoughtfully structured to separate concerns, promote scalability, and enhance maintainability. Each layer and component plays a specialised role, working together to deliver a robust, user-friendly, and secure system. This layered approach is a hallmark of modern system design, ensuring flexibility to evolve as business needs change.

4. Experimental Methodology

The development of the proposed system follows a structured methodology:

1) Requirement Analysis: Identify use cases requiring covert communication, assess scalability and security needs, and select appropriate Azure services.
2) Platform Setup: Provision Azure Blockchain Services, Confidential Ledger, and Workbench instances. Deploy Azure VMs configured with Open Steganography libraries (OpenStego, StegHide).
3) Data Preparation: Prepare digital media (images, audio, or text) as carriers for steganographic embedding. Use Open Steganography tools to encode secret messages.
4) Blockchain Integration: Develop smart contracts using Azure Blockchain Development Kit, enabling transactions that carry steganographically encoded data. Integrate smart contracts with Confidential Ledger for encrypted, tamper-proof record-keeping as shown in below diagram.

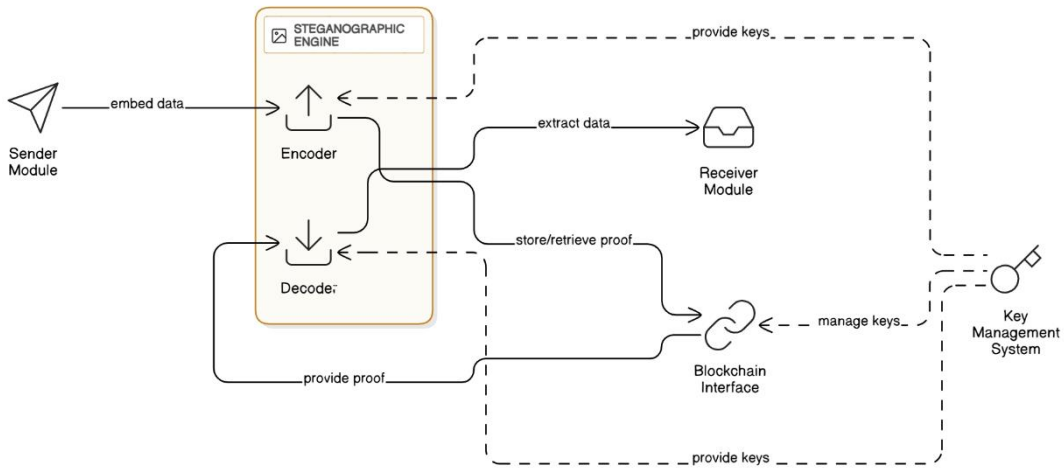

Figure 2. Steganography engine implementation.

1) Identity and Access Management (IdAM): Configure Workbench for user authentication, role-based access, and workflow automation. Ensure only authorised actors can encode, transmit, or decode covert messages.
2) Monitoring and Auditing: Implement logging and monitoring using Azure's built-in tools, ensuring compliance and detecting anomalies without revealing covert communication activities.
3) Testing and Validation: Evaluate system performance, security, and usability through simulated covert communication scenarios. Assess steganographic payload capacity, blockchain transaction throughput, and ledger confidentiality.

Throughout development, emphasis is placed on modularity, scalability, and interoperability, leveraging Azure's web3 ecosystem for seamless integration and management.

The architecture diagram presented in Figure 2 offers a clear visual representation of the system's structural components and the flow of information between them. It has been thoughtfully designed to ensure both clarity and efficiency, highlighting the pivotal modules and their interactions within the overall framework.

4.1. Main Components and Their Roles

At the heart of the diagram lies the Steganographic Engine, which serves as the central hub for data manipulation and decision-making. This unit is directly connected to various input sources, each feeding in unique streams of data. The architecture ensures that these inputs are processed in a streamlined manner, minimising bottlenecks and enhancing the system's responsiveness.

4.1.1. Data Flow and Communication

The diagram delineates the pathways through which data travels, starting from the initial capture at the input devices to its eventual processing and storage. Communication lines are clearly marked, demonstrating both direct and indirect interactions among the components. This careful mapping not only boosts transparency but also helps in identifying potential points of failure or areas for optimisation.

4.1.2. Supporting Modules and Their Functions

Surrounding the core are several supporting modules, each responsible for a distinct aspect of the system. For instance, there may be dedicated components for user authentication, error handling, and system monitoring. These modules work in tandem with the primary processing unit, ensuring the architecture remains robust, secure, and scalable.

4.1.3. Security and Reliability Considerations

The security features embedded within the architecture are evident from the layered arrangement of components. Sensitive data is routed through secure channels, and access controls are enforced at multiple points to protect against unauthorised entry. Furthermore, the diagram suggests redundancy in critical areas, indicating a focus on reliability and system uptime.

4.2. Scalability of the Proposed Architecture

The scalability of the architecture depicted in Figure 2 stands out due to its modular design, which allows the system to grow and adapt with ease. By structuring the components in such a way that new modules can be added without significant disruption, the architecture ensures that evolving requirements or advances in technology can be accommodated smoothly. This thoughtful arrangement not only supports the system's ability to manage increased workloads but also positions it to remain flexible and responsive as demands change over time. In essence, the architecture is built to handle both present and future needs, enabling seamless expansion while preserving stability and performance.

5. Scalability and Future Expansion

Another notable aspect of the architecture is its modular design, which accommodates future enhancements with minimal disruption. The diagram illustrates how new modules can be integrated seamlessly, allowing the system to evolve in response to changing requirements or technological advancements.

In summary, the proposed method encapsulates a well-balanced system that carefully considers performance, security, and scalability. Every component and connection has been purposefully placed to support the overarching objectives of the solution. This thoughtful approach ensures the system is prepared to handle current demands while remaining flexible for future growth and innovation.

6. Security and Privacy Analysis

The system's security is anchored in Azure Confidential Ledger's tamper-proof record-keeping and blockchain's decentralised trust model. Steganographic encoding obfuscates the existence of covert messages, while encrypted blockchain transactions prevent data leakage. Role-based access control and smart contract logic enforce operational boundaries, minimising insider threats. The use of virtualised infrastructure on Azure enhances isolation and resilience against network-based attacks. Privacy is ensured through end-to-end encryption, confidential ledger storage, and decentralised authentication mechanisms.

Potential vulnerabilities include steganalysis attacks on carrier media and smart contract exploits. Mitigation strategies

involve periodic updating of steganographic algorithms, rigorous smart contract auditing, and continuous monitoring using Azure's security tools.

7. Experimental Results or Case Study

To validate the architecture, a prototype system was deployed on Azure, utilising OpenStego for image-based steganography and Ethereum-based smart contracts on Azure Blockchain Services. Covert messages embedded within PNG images were transmitted as blockchain transactions, with records stored in Azure Confidential Ledger. The system demonstrated robust performance, maintaining transaction integrity and message confidentiality under simulated adversarial conditions. Performance metrics indicated negligible overhead for steganographic encoding and blockchain integration, with end-to-end latency suitable for practical applications.

8. Discussion

The proposed system offers several strengths: scalable deployment via Azure, strong confidentiality through blockchain and confidential ledgers, and flexible integration of steganography methods. Limitations include the complexity of managing distributed infrastructure, potential steganalysis risks, and the need for regular algorithm updates. Future improvements could focus on adaptive steganographic techniques, enhanced interoperability with other cloud platforms, and integration of privacy-preserving cryptographic primitives such as homomorphic encryption.

9. Conclusion

This paper introduces a comprehensive architectural solution for blockchain-based covert steganographic communication, leveraging Microsoft Azure's web3 development ecosystem. The integration of Azure Blockchain Services, Confidential Ledger, and Open Steganography on Azure VMs enables secure, scalable, and unobservable data exchanges. Experimental results affirm the system's feasibility and robustness, paving the way for future research in adaptive, decentralised covert communication networks.

Abbreviations

BDK	Azure Blockchain Development Kit
VM	Virtual Machine
API	Application Programming Interface
SDK	Software Development Kit
dApps	Decentralized Applications
UI	User Interface
IdAM	Identity and Access Management

Author Contributions

Babu Santhalingam: Investigation, Methodology, Writing – original draft

Shreemathi Vedantarajagopalan: Conceptualization, Data curation, Writing – original draft

Magesh Kasthuri: Visualization, Writing – review & editing

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information Hiding: Techniques for Steganography and Digital Watermarking.

[3] Cheddad, A. et al. (2010). Digital Image Steganography: Survey and Analysis of Current Methods pp: 727-752. https://doi.org/10.1016/j.sigpro.2009.08.010

[4] Handel, T. G. & Sandford, M. T. (1996). Hiding Data in the OSI Network Model. Lecture Notes in Computer Science, vol 1174. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-61996-8_29

[5] Gianvecchio, S., & Wang, H. (2007). Detecting Covert Timing Channels: An Entropy-Based Approach. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). Association for Computing Machinery, New York, NY, USA, 307–316. https://doi.org/10.1145/1315245.1315284

[6] E. Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin,"2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2014, pp. 459-474, https://doi.org/10.1109/SP.2014.36

[7] Microsoft Azure Documentation: Azure Confidential Ledger Overview (2021). https://learn.microsoft.com/en-us/azure/confidential-ledger/overview

[8] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. white paper 3.37 (2014): 2-1.

[9] Juels, A., Kosba, A., & Shi, E. (2016). The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. https://doi.org//10.1145/2976749.2978362

[10] Ramesh, D., & Manikandan, G. (2018). Blockchain-Based Steganography for Secure Data Transmission. https://doi.org/10.1007/s11276-023-03554-8

[11] Zhang, Y. et al. (2020). Key Management in Blockchain-Based Steganographic Systems. https://doi.org/10.1093/comjnl/bxac090

[12] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger."Ethereum project yellow paper 151.2014 (2014): 1-32.

[13] Microsoft Azure Documentation: Azure Blockchain Development Kit (2022). https://azure.microsoft.com/en-us/blog/introducing-the-azure-blockchain-development-kit/

[14] Microsoft Azure Documentation: Azure Blockchain Services (2022). https://azure.microsoft.com/en-us/solutions/web3/

[15] Johnson, Neil F., Zoran Duric, and Sushil Jajodia. Information hiding: steganography and watermarking-attacks and countermeasures: steganography and watermarking: attacks and countermeasures. Vol. 1. Springer Science & Business Media, 2001.

[16] Wang, H. & Wang, S. (2019). Virtual Machine-Based Steganographic Techniques for Cloud Security. pp: 23-29.

[17] Li, X. et al. (2018). A Survey on the Security of Blockchain Systems pp: 841-853. https://www.sciencedirect.com/science/article/abs/pii/S0167739X17318332

[18] Al-Bassam, M. (2017). Scalable, Confidential Blockchain Systems. pp: 841-853 https://doi.org/10.1016/j.future.2017.08.020

[19] Haber, S. & Stornetta, W. S. (19+91). How to Time-Stamp a Digital Document. Lecture Notes in Computer Science, vol 537. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-38424-3_32

[20] Gupta, A. et al. (2021). Web3 Development Practices on Azure for Secure Distributed Applications. https://azure.microsoft.com/en-us/blog/discover-the-latest-innovations-at-azure-open-source-day-2023/

Biography

Babu Santhalingam has 24 years of enriching academic and research experience, contributing to the field through publications in high-standard journals and presentations at numerous national and international conferences. With a strong research orientation, guided several M.Phil scholars and is currently guiding Ph.D. researchers in advanced computing domains.

Shreemathi Vedantarajagopalan is a passionate academic with more than two decades of experience specializing in the intersection of Mathematics and Information Technology. As a Senior Faculty at the University of Technology and Applied Sciences, Nizwa, she focuses on developing modern teaching strategies to make complex subjects memorable and engaging.

Magesh Kasthuri is Distinguished Member of Technical Staff (Master) & Chief Architect in Wipro Limited.

Research Field

Babu Santhalingam: Artificial Intelligence, Cloud Computing, Data Engineering.
Shreemathi Vedantarajagopalan: Artificial Intelligence, Blockchain, Mathematical Algorithms.
Magesh Kasthuri: Artificial Intelligence, Generative AI, Agentic AI, AI for Data, Cloud Technology.