International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 4, July-Aug 2025
Available at www.ijsred.com
RESEARCH ARTICLE OPEN ACCESS

BLOCKCHAIN AND IOT INTEGRATION IN HEALTHCARE: A HOLISTIC REVIEW OF APPLICATIONS, BARRIERS, AND EMERGING DIRECTIONS

Asha N S*, Dr. Mohamed Rafi**
*(Department of Computer Science, UBDT College of Engineering, and Davanagere
Email: ashans2819@gmail.com)
** ((Department of Computer Science, UBDT College of Engineering, and Davanagere
Email: mdrafi2km@ubdtce.org)

ABSTRACT:
The integration of Internet of Things (IoT) technologies into modern healthcare systems has led to significant improvements in patient monitoring, data sharing, and remote diagnostics. Despite these benefits, the handling of sensitive medical data through connected devices presents serious concerns related to privacy, data integrity, and system security. Blockchain technology, with its decentralized and tamper-proof characteristics, offers a promising framework to address these issues. This paper investigates how blockchain can enhance the safety, transparency, and efficiency of IoT-based healthcare systems. Key focus areas include secure management of electronic health records, reliable remote monitoring, and streamlined medical supply chains. The review also examines current limitations, such as scalability challenges and regulatory hurdles, while identifying future directions for research aimed at building more secure and trustworthy healthcare networks.

Keywords-**Blockchain, Internet of Things (IoT), Healthcare, Data Security, Electronic Health Records (EHR), Remote Patient Monitoring, Decentralized Systems, Privacy, Interoperability, Smart Healthcare, Medical Data Management**

I. INTRODUCTION

The rapid advancement of IoT technologies is driving a fundamental shift in the healthcare landscape, enabling more intelligent and connected systems. Wearables, smart diagnostic tools, and interconnected medical devices now allow continuous monitoring of patients, quicker identification of health issues, and streamlined data transmission between care providers.

These improvements offer the promise of enhanced medical outcomes, operational efficiency, and increased access to healthcare services, particularly in remote or under-resourced areas. However, the integration of IoT into healthcare infrastructures also introduces substantial risks—chiefly, the protection of sensitive medical data and the trustworthiness of data exchange.

The personal nature of health-related information makes it a prime target for breaches and tampering. Centralized healthcare databases often struggle to manage the massive and diverse data generated by IoT systems, exposing them to vulnerabilities. Therefore, a more secure and transparent approach is needed to manage these complex data flows and preserve patient confidentiality.

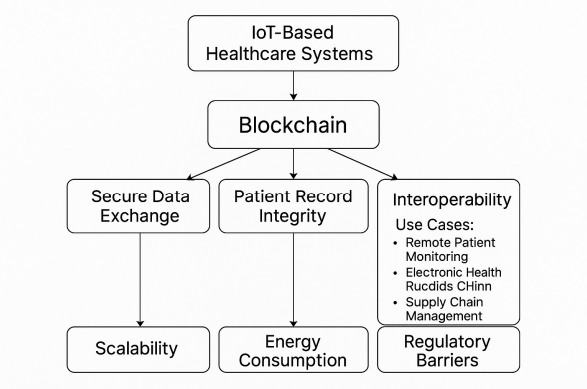

Fig.1 Architecture of Blockchain integration in IoT-based healthcare systems

Blockchain technology has emerged as promising solution to address the challenges. By providing decentralized, immutable, and transparent ledger, blockchain can enhance the security, traceability, and integrity of medical data. Features such as a smart contracts, consensus mechanisms, and cryptographic techniques make it suitable for building trust across distributed IoT networks without relying on centralized intermediaries.

II. BACKGROUND AND FUNDAMENTALS

A. Evolution of IoT in Healthcare

The Internet of Things (IoT) has transformed modern healthcare by enabling a network of connected devices that collect and exchange health-related data. This network—referred to as the **Internet of Medical Things (IoMT)**—includes wearables, implantable sensors, smart diagnostic tools, and connected medical infrastructure. These technologies facilitate real-time patient monitoring, remote diagnostics, and data-driven decision-making, contributing to improved patient outcomes and optimized hospital workflows.

Despite its benefits, IoMT systems face significant challenges:

- **Security vulnerabilities** due to open wireless communication.
- **Lack of standardization** across device platforms.
- **Centralized data storage** risks involving single points of failure or tampering.
- **Privacy issues** in storing sensitive patient records.

B. Blockchain Technology: Core Principles

Blockchain is a decentralized and distributed ledger technology that records data in a chain of immutable blocks, each linked via cryptographic hashes. Originally designed for cryptocurrency transactions, blockchain's inherent properties make it valuable in domains requiring secure, verifiable, and tamper-resistant data sharing.

Key features include:

- **Decentralization**: Removes reliance on centralized entities, increasing trust and fault tolerance.
- **Immutability**: Ensures data, once recorded, cannot be altered.
- **Transparency and auditability**: All transactions are chronologically ordered and verifiable.
- **Smart contracts**: Allow predefined logic to automate access and transactions among participants .

Blockchain is particularly well-suited for securing medical data, enabling privacy-preserving access to health records, and managing trust among multiple stakeholders.

C. Integrating Blockchain with IoT in Healthcare

The convergence of blockchain with IoT (often termed **Blockchain-IoT** or **B-IoT**) offers a powerful framework for secure and decentralized medical data exchange. In healthcare, this integration can:

- **Secure data streams** from IoMT devices through tamper-evident logging.
- **Enable decentralized identity management** for patient and device authentication.
- **Provide automated access control** through smart contracts for electronic health records (EHRs).
- **Enhance supply chain integrity** in pharmaceuticals and medical equipment .

This synergy ensures data integrity, boosts transparency, and facilitates collaboration among hospitals, insurance providers, and patients.

D. Layered Architecture of B-IoT Systems

Blockchain-IoT solutions in healthcare typically follow a **three-layer architecture**:

1. **Physical Layer (Perception Layer)**
   - Includes IoMT devices: sensors, wearables, diagnostic machines.
   - Captures patient metrics like glucose levels, heart rate, and body temperature.
2. **Blockchain/Network Layer**

Provides consensus mechanisms, encrypted storage, and decentralized data validation.
Enables secure data propagation across distributed nodes.

3. **Application Layer**

Interfaces for patients, healthcare providers, regulators.
Supports clinical analytics, data access requests, insurance processing, etc..
Such structured deployment supports scalability and facilitates compliance with health data regulations.

E. Research Challenges and Motivations

Although Blockchain-IoT integration shows promise, key challenges persist:

- **Resource constraints** of IoT devices (limited processing and energy).
- **Scalability** concerns in handling high-frequency medical data.
- **Latency** in real-time applications due to blockchain's transaction time.
- **Regulatory and legal hurdles**, including cross-border data sharing and compliance 40†Blockchain_for_IoT-ening **lightweight consensus protocols**, **off-chain storage techniques**, and **hybrid blockchain models** tailored for the healthcare IoT ecosystem.

This review paper investigates the function of blockchain in fortifying IoT-based healthcare systems. It examines how blockchain can ensure secure and interoperable data exchange, maintain patient record integrity, and support critical healthcare use cases such as remote patient monitoring, electronic health record (EHRs), and supply chain tracking for medical resources. In addition, this paper brings attention to present limitations, including scalability issues, energy consumption concerns, and legal or regulatory constraints. By analyzing recent research trends and recognizing existing limitations, this study targets to provide a comprehensive perspective on the integration of blockchain with healthcare IoT systems and its potential to revolutionize the future of medical data management.

III. INTEGRATION OF BLOCKCHAIN AND IOT

Embedding blockchain functionalities in IoT architectures creates a robust ecosystem capable of addressing critical challenges in healthcare such as data breaches, unauthorized access, and lack of interoperability. In this convergence, IoT devices act as data generators, while Blockchain serves as the secure infrastructure for recording, verifying, and managing that data.

This section explores how Blockchain enhances IoT functionality across key dimensions relevant to healthcare systems.

A. Security Enhancement

A major challenge in IoT-enabled healthcare is protecting confidential patient information. Conventional centralized infrastructures often serve as attractive targets for cyberattacks and are vulnerable to data manipulation and unauthorized intrusions.

Blockchain introduces a **tamper-proof distributed ledger**, where every transaction is cryptographically secured and validated through consensus mechanisms. This approach prevents alteration of medical records and ensures traceability of all data flows. Even if a node is compromised, the blockchain's distributed architecture ensures that the system remains secure and tamper-resistant.

Additionally, digital signatures and cryptographic keys provide **device-level authentication**, reducing risks from rogue or counterfeit IoT devices.

B. Privacy Preservation

Patient confidentiality is a legal and ethical cornerstone in healthcare. Traditional data exchange methods often involve third parties, increasing the risk of exposure.

Blockchain enables **pseudonymous identities** and **permissioned access**, where only authorized stakeholders can view or modify specific patient records. Moreover, **smart contracts** can be programmed to enforce data-sharing policies based on patient consent, guaranteeing that data handling practices conform to global privacy rules like HIPAA and GDPR.Decentralized access control also removes dependency on centralized servers, reducing the likelihood of mass data leaks.

C. Building Trust Among Stakeholders

In complex healthcare ecosystems, trust among hospitals, insurance providers, labs, and patients is often fragile.

Blockchain promotes **trustless collaboration**—a model where participants do not need to trust each other directly, but instead rely on the **transparency and verifiability** of the Blockchain ledger. Every data transaction is time-stamped and immutable, which means participants can validate information without manual reconciliation or third-party verification.

This trust framework is particularly useful for clinical trials, patient referrals, and insurance claims.

D. Automation with Smart Contracts

Smart contracts are self-executing scripts stored on the Blockchain that automatically trigger predefined actions when certain conditions are met.

In IoT-enabled healthcare, smart contracts can:

- Automate the **release of patient data** to authorized parties.
- Trigger **alerts** based on abnormal sensor readings.
- Facilitate **automated billing and insurance processing**.
- Enforce **data-sharing agreements** across platforms.

This reduces manual intervention, increases operational efficiency, and minimizes administrative errors.

E. Architecture and Framework Examples

Numerous architectures have been proposed to integrate Blockchain and IoT in healthcare. A generalized framework typically consists of:

a. IoT Layer

- Medical sensors, wearables, and diagnostic equipment capture patient health data.

b. Blockchain Layer

- Includes consensus protocols (e.g., PBFT, PoA), cryptographic validation, and decentralized storage.

c. Smart Contract Layer

- Automates policies for access, authentication, and data sharing.

d. Application Layer

- Interfaces for hospitals, insurers, and patients to interact with the system securely.

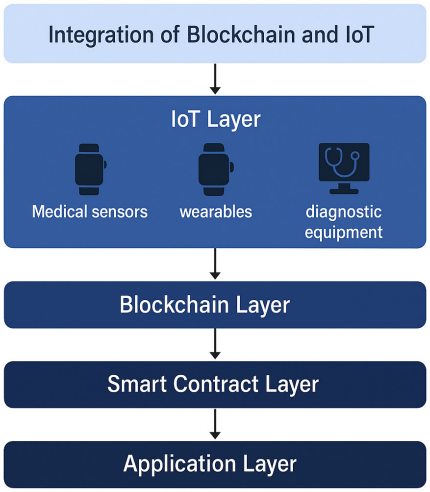

Fig 2: Block diagram of Blockchain-IoT integration in healthcare showing secure data flow across IoT, Blockchain, Smart Contract, and Application layers.

Some notable frameworks from literature:

- **IoTChain**: A Blockchain-based lightweight security architecture designed specifically for IoT networks.
- **IOTA**: A Blockchain-like structure (Tangle) optimized for IoT devices with low computing power.
- **FHIRChain**: Integrates Blockchain with the FHIR standard to enable secure clinical data exchange

IV. CURRENT RESEARCH AND APPLICATIONS

The integration of Blockchain and IoT in healthcare has attracted substantial academic and industrial interest, resulting in a growing body of research and practical implementations. This section outlines notable application areas and summarizes key research efforts that demonstrate how this convergence is shaping the future of healthcare.

A. Remote Patient Monitoring (RPM)

Blockchain-IoT platforms enable continuous monitoring of patients outside clinical settings using wearable sensors and connected devices. Data such as heart rate, glucose levels, and oxygen saturation are securely transmitted and stored in tamper-proof ledgers, ensuring **real-time visibility** and **trustworthy alerts** for healthcare providers.
For ex, some of the studies propose smart contract-based systems that automatically notify caregivers when predefined thresholds are crossed, reducing delays in emergency response.

C. Electronic Health Records (EHR) Management

Traditional EHR systems face issues related to interoperability, unauthorized access, and single points of failure. Blockchain allows decentralized EHR management, where patients retain control over who accesses their medical data.
Projects such as **FHIRChain** and **MedRec** demonstrate how Blockchain can enable **secure, auditable, and patient-centric** health data exchange across multiple healthcare institutions .

C. Pharmaceutical Supply Chain Management

Counterfeit drugs remain a major concern globally. Blockchain-IoT solutions are being used to **track medical products** from manufacturers to end-users. RFID tags and sensors integrated with blockchain record every transaction along the supply chain, ensuring **transparency**, **traceability**, and **compliance verification**.
Several frameworks leverage smart contracts to automate logistics, verify shipment conditions, and manage inventory in real time .

D. Clinical Trials and Research Integrity

Blockchain provides an transparent and immutable system for managing clinical trial data, reducing the risk of data manipulation or protocol violations. Smart contracts can automate participant consent, timestamp trial data, and validate results, fostering **data integrity** and **regulatory compliance**.
Recent proposals involve integrating IoT wearables to collect trial data and record it securely on-chain, ensuring verifiability without compromising patient privacy.

E. Insurance and Claims Processing

Insurance fraud and delayed reimbursements are significant challenges in healthcare. Blockchain

automates **insurance claim verification** by linking IoT-generated health records to smart contracts. This ensures that claims are **processed fairly and automatically**, based on verified data captured during treatment.
Recent projects are developing frameworks where wearable-generated health data serves as tamper-proof evidence for insurance approvals.

V. CHALLENGES AND LIMITATIONS

While the unification of Blockchain and IoT in healthcare presents significant advantages in terms of data security, trust, and automation, several technical and practical limitations hinder its large-scale adoption. These challenges must be critically analyzed to guide future research and real-world deployment.

A. Scalability Issues

Blockchain networks, especially those using traditional consensus mechanisms like Proof of Work (PoW), struggle with **limited throughput and high latency**. In healthcare, where IoT devices generate vast amounts of real-time data, this becomes a major bottleneck. The time and resources needed to validate each transaction make it impractical to use conventional Blockchain models for high-frequency medical data streams.

D. Energy Consumption

IoT devices typically operate with limited battery and processing power. However, many Blockchain operations are **energy-intensive**, especially when devices participate in consensus or cryptographic processes. This energy burden is incompatible with lightweight and wearable IoMT devices, thus demanding the development of **energy-efficient Blockchain protocols**.

C. Latency and Real-Time Responsiveness

Applications such as remote patient monitoring or emergency alerts require real-time responsiveness. Unfortunately, Blockchain transactions can involve delays due to network validation and block creation times. This **latency** is unacceptable for time-sensitive healthcare use cases and limits Blockchain's applicability in **critical care settings**.

D. Storage Overhead

Healthcare data, especially diagnostic images and continuous monitoring records, is **high in volume and unstructured**. Storing this data on-chain is neither scalable nor efficient. Although hybrid architectures with **off-chain storage (e.g., IPFS)** are being explored, managing and indexing such distributed data remains a challenge.

E.Interoperability and Standards

A major barrier in Blockchain-IoT systems is the **lack of standard protocols** for device communication, data formats, and system integration. Without unified frameworks, interoperability across different Blockchain platforms, IoT devices, and healthcare information systems remains difficult, resulting in **fragmented deployments**.

F.Legal and Regulatory Compliance

Storing and processing patient data on decentralized ledgers raises **regulatory concerns**, particularly under laws such as the **General Data Protection Regulation (GDPR)** and **HIPAA**. Blockchain's immutability conflicts with the "right to be forgotten," and cross-border data sharing can introduce **jurisdictional challenges**. Legal frameworks have not yet evolved to fully accommodate decentralized healthcare ecosystems.

G. Adoption Barriers

- **Lack of technical expertise** among healthcare institutions.
- **High implementation costs**.
- **Resistance to change** from legacy system vendors and stakeholders.

Successful implementation requires **multidisciplinary collaboration** between technologists, healthcare providers, legal experts, and policy-makers.

VI. Future Research Directions

Despite promising advancements, the integration of Blockchain with IoT in healthcare remains an emerging area with numerous unresolved challenges. To fully unlock its potential, future research should focus on addressing technical limitations, enhancing scalability, and ensuring ethical and regulatory compliance. This section outlines key directions for future exploration.

A.Lightweight and Scalable Blockchain Protocols

Conventional Blockchain protocols are computationally intensive and unsuitable for resource-constrained IoT devices. Future research should focus on:

- **Designing lightweight consensus mechanisms** such as Proof of Authority (PoA), Delegated Proof of Stake (DPoS), or Practical Byzantine Fault Tolerance (PBFT).
- **Developing IoT-friendly Blockchain platforms** (e.g., IOTA, Nano, or tailored sidechains) that reduce energy and storage overhead.

These innovations would make Blockchain more accessible for continuous health monitoring and wearable devices.

B. Off-Chain and Hybrid Storage Models

Storing all health data on-chain is impractical. Future systems should explore:

- **Hybrid storage architectures** combining Blockchain with decentralized off-chain solutions (e.g., IPFS, BigchainDB).
- Efficient **indexing and retrieval mechanisms** for high-volume medical data while preserving integrity and accessibility.

Such models would enable real-time access to large diagnostic files without bloating the Blockchain network.

C. Interoperability Standards and APIs

Lack of interoperability remains a key barrier. There is a need for:

- **Standardized data models and APIs** that ensure compatibility between Blockchain platforms, IoMT devices, and EHR systems.
- Integration with existing healthcare standards such as **HL7 FHIR** to support seamless data sharing across providers.

This would enable unified care and collaboration between multiple institutions.

D.Privacy-Preserving Mechanisms

While Blockchain is transparent, healthcare demands confidentiality. Future research should investigate:

- **Zero-knowledge proofs (ZKPs)**, **homomorphic encryption**, and **multi-party computation (MPC)** to enable privacy-preserving transactions.
- **Granular access control frameworks** that dynamically adapt to patient consent models and data types.

Balancing **data transparency** with **user privacy** is critical for patient trust and compliance.

E. Integration with AI and Edge Computing

Combining Blockchain with **Artificial Intelligence (AI)** and **Edge Computing** presents a novel opportunity:

- AI models can analyze health data on edge devices while Blockchain ensures result verifiability and model auditability.
- Edge-Blockchain fusion reduces latency, enhances privacy, and minimizes network load.

Research in **AI-on-Blockchain** can power predictive healthcare while maintaining trust and traceability.

F.Regulatory Frameworks and Ethical AI

To ensure adoption, future work must align with:

- **Global and local regulations** like GDPR, HIPAA, and data localization laws.
- Ethical frameworks that address **data sovereignty**, **patient consent**, and **algorithmic fairness** in AI-blockchain integration.

Close collaboration between **technologists, policymakers, and ethicists** will be key in shaping responsible deployments.

VII. Conclusion

The integration of Blockchain and IoT in healthcare presents a transformative opportunity to enhance data security, patient privacy, system interoperability, and operational efficiency. By leveraging Blockchain's decentralized architecture and IoT's real-time data collection capabilities, healthcare systems can evolve into more trustworthy, automated, and patient-centric ecosystems. Despite current challenges—such as scalability, regulatory compliance, and energy constraints—ongoing research continues to explore innovative solutions, including lightweight consensus protocols, hybrid storage models, and AI integration. This review highlights the growing potential of Blockchain-IoT synergy and underscores the importance of interdisciplinary collaboration in advancing secure and scalable smart healthcare solutions.

REFERENCES

[1] R. AlGhamdi, F. Alsolami, F. Alsharif, and N. Alzahrani, "Developing Trusted IoT Healthcare Information-Based AI and Blockchain," Processes, vol. 11, no. 1, p. 34, 2023. [Online]. Available: https://doi.org/10.3390/pr11010034

[2] Y. Y. Ghadi, M. H. Dawaymeh, and A. S. Alhmouz, "The role of blockchain to secure internet of medical things," Scientific Reports, vol. 14, no. 1, 2024. [Online]. Available: https://doi.org/10.1038/s41598-024-68529-x

[3] A. Haleem, M. Javaid, and R. P. Singh, "Blockchain technology applications in healthcare: An overview," Int. J. Intell. Netw., vol. 2, pp. 130–139, 2021. [Online]. Available: https://doi.org/10.1016/j.ijin.2021.09.005

[4] S. R. Mallick, M. H. Alshammari, and A. B. Mabrouk, "Blockchain-enhanced IoT ecosystem for healthcare: Potentials, challenges and solutions," Comput. Ind. Eng., vol. 197, p. 110538, 2024. [Online]. Available: https://doi.org/10.1016/j.cie.2024.110538

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE PerCom Workshops, Kona, HI, USA, 2017, pp. 618–623. [Online]. Available: https://doi.org/10.1109/percomw.2017.7917634

[6] A. Asif, A. Qayyum, M. Imran, and M. A. Jan, "Blockchain-Enabled Internet of Things (IoT) Applications in Healthcare: A Systematic Review of Current Trends and Future Opportunities," IEEE Access, 2023. [Online]. Available: [PDF uploaded file]

[7] R. Ramesh and P. B. Reddy, "Blockchain-IoT in Healthcare Applications," in IOP Conf. Ser.: Mater. Sci. Eng., vol. 1055, 2021. [Online]. Available: https://doi.org/10.1088/1757-899X/1055/1/012106

[8] S. B. Sivasankari and P. Varalakshmi, "Blockchain and IoT Technology in Healthcare: A Review," in Blockchain and AI in Healthcare, Springer, 2022. [Online]. Available: [PDF uploaded file]

[9] J. P. Sahoo, S. K. Mohapatra, and R. K. Sahoo, "Blockchain for IoT-enabled Healthcare," Materials Today: Proceedings, 2020. [Online]. Available: [PDF uploaded file]

[10] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," IJSRCSEIT, vol. 5, no. 1, pp. 121–127, 2019. [Online]. Available: https://doi.org/10.32628/CSEIT195137

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[12] World Health Organization (WHO), "Digital health," 2023. [Online]. Available: https://www.who.int/health-topics/digital-health

[13] S. Chaudhary, A. Malhotra, and P. Kumar, "A comprehensive review of blockchain-based smart healthcare," Multimedia Tools and Applications, vol. 82, no. 4, pp. 4963–4991, 2023. [Online]. Available: https://doi.org/10.1007/s11042-022-13021-x

[14] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Berkeley Engineering, 2016. [Online]. Available: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

[15] IBM Blockchain, "Blockchain in Healthcare: A New Model for Health Information Exchanges," IBM Whitepaper, 2020. [Online]. Available: https://www.ibm.com/downloads/cas/EXK4XKX8

[16] C. Esposito, A. Castiglione, K. K. R. Choo, and M. Ficco, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018. [Online]. Available: https://doi.org/10.1109/MCC.2018.011791712

[17] D. Tapscott and A. Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World," Portfolio, 2016.

[18] M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," in Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Serv. (Healthcom), 2016, pp. 1–3. [Online]. Available: https://doi.org/10.1109/HealthCom.2016.7749510

[19] A. Bhattacharya et al., "Secure and Privacy-Preserving Framework Using Blockchain in Healthcare," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 985–998, 2021. [Online]. Available: https://doi.org/10.1007/s12652-020-02239-5

[20] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.05.046

