

INTEGRATING ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGY INTO SMART MOBILE APPLICATIONS

Avni RUSTEMI¹

¹*Department of Informatics, Faculty of Natural Sciences and Mathematics, University of Tetovo, North Macedonia*

^{*}*Corresponding author e-mail: avni.rustemi@unite.edu.mk*

Abstract

The rapid development of contemporary technologies tends to digitalize all services across various public and private institutions, where most services are also provided on mobile devices due to their great practical usability by people in everyday life. The integration of Blockchain Technology (BT) and Artificial Intelligence (AI) into mobile devices and mobile programming enables, among other things, the creation of intelligent, autonomous, independent systems that, in automated form, are able to not only process data in real time, but also predict and make decisions in an intelligent way while preserving privacy and offering complete security and transparency. Through this paper, we attempt to explain the importance of the practical integration of these two technologies, with particular emphasis on the role of Edge AI in mobile devices and programming, security and privacy, and practical code frameworks and sequences used to create decentralized mobile applications. Through BT and AI, and the creation of hybrid architectures, the trust, transparency and integrity of mobile applications are increased, and validation is automated by creating intelligent autonomous mobile ecosystems. Even though technological developments tend to focus on improving privacy and security issues, there are many weaknesses and challenges directly related to practical implementations. However, the combination of BT, Edge AI and federated learning is seen as a mechanism for improving security and privacy, reducing dependence on cloud servers and focusing data processing locally. The findings show that despite challenges related to scalability, resource constraints, and costs, continuous developments in these contemporary technologies and hybrid infrastructures accelerate the creation of secure and intelligent systems on mobile devices.

Keywords: Blockchain Technology, Artificial Intelligence, Edge AI, mobile applications, hybrid architectures, privacy and security.

Introduction

The integration of Artificial Intelligence (AI) and Blockchain Technology (BT) are key components in the development of modern intelligent systems, including mobile applications, transforming the way people interact with technologies while providing more secure, transparent and intelligent services in the implementation of certain processes. Most mobile applications, in addition to the static and traditional functions they implement, today, thanks to Machine Learning (ML) techniques, are able to learn from user data, and thus analyze their behavior and make intelligent decisions in real time, or even provide suggestions and recommendations for future actions. Mobile Artificial Intelligence (Mobile AI) is a term that refers to the integration of artificial intelligence algorithms into mobile devices for the purpose of local data processing on mobile devices, with the aim of increasing security, privacy, reducing latency and various cyberattacks. Mobile AI is increasingly becoming a key component of mobile computing, integrating contemporary technologies such as ML, edge intelligence, and mobile computing with the aim of automating processes and increasing the performance of mobile applications, but above all, the main focus is on user privacy (Slyusar et al., 2024). Facial recognition, the implementation of intelligent chatbots, the personalization of activities in mobile applications, increased performance and efficiency in resource management, and above all, process automation and intelligent decision-making are just some of the modern technological evolutions (Li et al., 2025). The integration of Neural Processing Units (NPU) has enabled the development of the on-device AI concept, where ML algorithms are executed on the mobile device itself, without the need for cloud computing, although with certain limitations in terms of memory and other resources, yet with numerous advantages in terms of privacy, data security, process execution latency and increased performance in general

(Kwon & Kang, 2024). The main goal of modern mobile applications is to provide real-time services in line with dynamic changes, content personalization, assistance for easier process implementation, detection of various security threats, and even prediction of user behavior and automatic recommendations for future actions, in order to meet the needs and preferences of different users (Usman et al., 2025).

The latest implementations in mobile applications are towards the use of Large Language Models (LLM), and Generative AI, with the aim of natural language understanding, real-time responses, AI assistance for support and process automation, with the aim of maintaining performance and optimizing resources, but above all, facilitating many user processes (Dubiel et al., 2024). Facial recognition technology, intelligent document scanning, Augmented reality (AR) and Virtual Reality (VR) filters in mobile device cameras, medical diagnostic applications, various virtual games, use Convolutional Neural Networks (CNNs) models. Supervised learning is among the ML techniques used in mobile applications for the purpose of data classification and prediction, and experience personalization, where it practically finds implementations in facial recognition, voice, spam, and predictive keyboard (Ashok & Katarya, 2025). Deep Learning, on the other hand, is an advanced technique that is finding wide application in many fields, including mobile devices, which is mainly based on the combination of Computer Vision and Natural Language Processing techniques for the purpose of biometric authentication, image recognition, and virtual and augmented implementation in mobile programming (Kwon & Kang, 2024). Reinforcement learning, where applications learn through user interaction and optimize behavior based on the feedback they receive, is also widely implemented in some mobile applications. It is mainly used in battery optimization, creating adaptive user interfaces, gaming, and efficient resource management (Pan et al., 2020). And finally, Blockchain technology through smart contracts offers automation of processes on mobile devices, enabling the elimination of third parties, and in this way increasing security, reliability and the risk of possible data misuse (Rustemi et al., 2024). Blockchain technology through decentralization, transparency, immutability, offers higher security and reliability among users, but at the same time is seen as the only hope that guarantees self-sovereign identity, high security mechanisms through advanced cryptographic algorithms and decentralized storage (Rustemi et al., 2025). Through Figure 1, we have presented a taxonomy, where we summarize the main concepts of implementing blockchain technology and artificial intelligence in mobile applications.

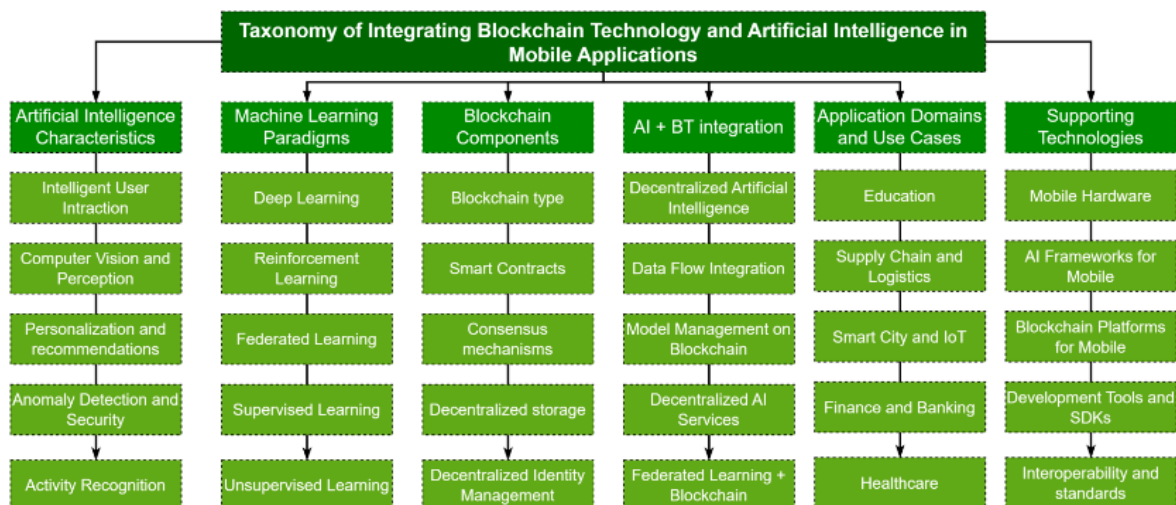


Figure 1. Taxonomy of Blockchain and AI implementation in mobile applications

Edge Computing in Mobile AI

Edge Computing is a new paradigm that aims to process data on mobile devices or edge servers, instead of sending data to cloud servers. This offers the possibility for ML algorithms, among others, to be executed directly on smartphones, wearable devices, reducing latency, traffic and dependence on the internet. The Edge AI architecture in mobile applications consists of three main layers, the mobile device layer, which includes mobile devices that collect data in real time, the edge layer, which includes servers or gateways that perform more complex processes, and the cloud layer for handling larger models and longer data storage (Ale et al., 2024). Edge AI plays an important role because, without relying on cloud services, it enables immediate response to many features of mobile devices such as face recognition, AI assistants, healthcare monitoring, and more. Above all, the use of edge AI enables energy and performance optimization compared to cloud architectures (Na & Lee, 2024). Many coherent techniques are used for maximum resource optimization, due to memory, processor and energy limitations, therefore quantization, pruning, knowledge distillation, and lightweight neural networks are some techniques that offer optimization of these resources. Among the modern frameworks used for efficient execution of ML models on smartphones and edge devices are TensorFlow Lite, Core ML, and ONNX Runtime Mobile, which, among other things, enable optimization of hardware resources and faster inference (Grzesik & Mrozek, 2024). Edge AI today finds application in many areas, including real-time patient monitoring in medicine, intelligent diagnostics, biometric signal analysis, local traffic analysis, object detection in autonomous vehicles, and many others (Ale et al., 2024). Also in mobile financial applications, it is used for detecting various attacks, as well as for predictive analytics and recommendations in various intelligent systems (Grzesik & Mrozek, 2024). Despite the great importance of Edge AI in mobile applications, many important technical challenges remain, such as battery and other hardware resource limitations, which are critical factors in the execution of deep learning algorithms. Also, the security of AI nodes and models from various attacks, as well as the heterogeneity of mobile devices create difficulties in standardizing practical implementations, where, among other things, work is being done on the integration of blockchain technology with Edge AI with the sole purpose of increasing security and reliability, but on the other hand, blockchain is facing practical challenges, which complicates the practical integration of these two technologies (Shaheen et al., 2024).

Privacy and security analysis from the integration of blockchain and AI in mobile applications

The integration of BT and AI in the creation of mobile applications, in addition to bringing new opportunities towards the creation of autonomous, secure and reliable systems, also brings complex challenges in terms of security and privacy. AI is primarily used for intelligent analysis and decision-making, and BT for immutable storage, smart contract execution and integrity verification. This integration enables the development of mobile applications that ensure transparency, trustworthiness and auditability of AI processes (Deval et al., 2024).

Mobile systems are exposed to various security threats due to the nature of transparency and the use of ML models, with one of the main problems being the manipulation of AI models through adversarial attacks, where attackers attempt to trick ML algorithms into entering incorrect inputs, which will result in incorrect results. There are also opportunities when attackers attempt to extract parameters or inference logic, where through abstraction attacks they attempt to compromise intellectual property and system security (Gill et al., 2025). One of the vulnerabilities in mobile applications is data poisoning attacks, where manipulated data is injected with the aim of degrading performance, which is particularly problematic in

federated learning (Rudin; 2019). One of the other important challenges in Mobile AI is privacy, as intelligent mobile applications process personal data, and in most cases, we as users, without carefully reading the terms and conditions of various applications, give confirmation for the use of personal data, which can also be misused by malicious people.

Although on-device AI and edge AI have been developed to overcome the problems of transferring data to cloud servers, where there is a risk of unauthorized access and data leakage, they are still facing limitations in hardware resources for processing ML algorithms and storing data in larger capacity (Kwon & Kang, 2024). On the other hand, on-device AI also faces various privacy risks, due to various attacks that attempt to alter data from the outputs of ML models, which is especially critical in fields where personal information is exposed, such as medicine, finance, etc. (Gill et al., 2025). BT is seen as a hope for improving security and privacy in Mobile AI applications, especially in terms of verifying information without the need for a central authority, but through smart contracts. So BT finds use for secure AI model verification, where the hash values of AI models or even the results are stored on the blockchain to guarantee the integrity and authenticity of the same. Through Figure 2, we have presented an example of a smart contract that implements immutable AI verification, trusted timestamping, decentralized storage, and auditability of results.

```

1  pragma solidity ^0.8.0;
2  contract AIIntegrity {
3      struct Prediction {
4          string hashValue;
5          uint256 timestamp;
6      }
7      Prediction[] public records;
8      function storeResult(
9          string memory _hash
10     ) public {
11         records.push(
12             Prediction(
13                 _hash,
14                 block.timestamp
15             )
16         );
17     }
18     function verifyResult(
19         uint index
20     ) public
21     view
22     returns(
23         string memory,
24         uint256
25     ) {
26         return (
27             records[index].hashValue,
28             records[index].timestamp
29         );
30     }
31 }

```

Figure 2. Blockchain Smart Contract for AI Verification

AI-blockchain integration, although improving security and privacy, creates trade-offs that directly impact various technical issues, such as energy consumption, latency, computational overhead, and others. Blockchain technology, although it is known for increasing the reliability and immutability of data, in practice it has problems with scalability and management of mutable data, or in other words, updating data, because each action represents a transaction in itself, which generates a unique hash value. Edge AI, on the other hand, although it has benefits in terms of local inference by increasing security, has challenges in terms of various attacks on the models used. Smart contracts, although they offer automatic validation and access control by increasing privacy, still have challenges in various vulnerabilities, and each execution of a smart contract has its own cost, and the same cannot be changed during execution (Valdez-Solis et al., 2026).

Practical implementations of Blockchain and AI on mobile devices

The practical integration of blockchain technology and artificial intelligence is in the early stages, namely in the conceptual modeling stages, due to the many practical challenges that these two technologies are facing separately. However, the efforts and implementations of some features in current systems are only practically implemented, making users familiar with these technologies and gaining trust above all (Rustemi & Dalipi, 2026). Recently, there has

been an increasing trend towards hybrid architectures, taking the best elements of each technology and adapting them into an architecture that is appropriate for the environment in which they are implemented. Similarly, in mobile applications, edge-cloud-blockchain architectures are being implemented, with the aim of analyzing as much data as possible locally and storing hash values and metadata on the blockchain (Ale et al., 2024). Through Figure 3 we have presented a code sequence of the practical implementation of EdgeAI through TensorFlow Lite, which enables, among other things, efficient execution of ML models, directly on mobile devices with the aim of optimizing battery usage and minimal latency, respectively, local inference of the AI model on the mobile device. Through the variable *input_data*, input data such as biometric information, image tensors, and others are received, while *prediction* represents the predicted result after analyzing the ML model.

```

1  import tensorflow as tf
2
3  interpreter = tf.lite.Interpreter(
4      model_path="avni_model.tflite"
5  )
6
7  interpreter.allocate_tensors()
8
9  input_details = interpreter.get_input_details()
10 output_details = interpreter.get_output_details()
11
12 interpreter.set_tensor(
13     input_details[0]['index'],
14     input_data
15 )
16
17 interpreter.invoke()
18
19 prediction = interpreter.get_tensor(
20     output_details[0]['index']
21 )
22
23 print(prediction)

```

Figure 3. ML execution code sequence in TensorFlow Lite

As usual, for communication between mobile applications and the blockchain network, React Native is used together with the Web3.js API, which among other things enables the creation of decentralized mobile applications. React Native is known among other things as one of the frameworks that offer cross-platform mobile development, and is very easily integrated with blockchain and AI infrastructure. This code sequence through Figure 4 represents the communication between mobile applications and smart contracts on the blockchain via Web3 API and the storage of AI results in a decentralized manner. This approach is used to reduce the risk of manipulation and provide a more reliable intelligent ecosystem with blockchain verification mechanisms.

```

1  import web3 js;
2  define contractAddress;
3  define contractABI;
4  contract= new web3.eth.contract ( contractABI, contractAddress)
5  define function AIResult (hash) {
6      accounts=await web3.eth.getAccount();
7  }
8  await contract.methods.storeResult(hash: from accounts;)

```

Figure 4. Code sequence in pseudocode form in React Native (mobile device - blockchain communication)

The use of decentralized identity systems and Self-Sovereign Identity (SSI) is also an important aspect of integrating AI and BT into mobile devices, where users control their digital identity without the need for centralized authorities and traditional databases. It is mainly applied in

face recognition, anomaly detection, while blockchain stores credentials and provides reliable authentication, directly affecting the privacy and control of personal data (Spomy et al., 2022).

Conclusion

The integration of AI and BT in mobile applications represents one of the innovative and transformative directions of mobile computing, which among other things enables the development of more secure, autonomous and more capable mobile intelligent systems to perform activities in real time. In this paper, the main concepts of Mobile AI, the role of Edge AI in mobile devices, data security and privacy issues in the integration of AI and BT in mobile devices, and even practical implementations of AI and BT integration in mobile devices and the most used frameworks for this purpose were analyzed in brief points. The implementation of Edge AI and on-device ML through TensorFlow Lite undoubtedly reduces latency and dependence on cloud servers, while blockchain guarantees transparency, integrity and automatic verification of results. The implementation of React Native, Web3 API, and Solidity smart contracts are practical examples of developing decentralized mobile applications with intelligent mechanisms for validation and authentication.

References

- [1]. Ale, L., Zhang, N., King, S. A., & Chen, D. (2024). Empowering generative AI through mobile edge computing. *Nature Reviews Electrical Engineering*, 1(7), 478-486.
- [2]. Ashok, M., & Katarya, R. (2025, June). Supervised Learning Approaches in Android Malware Detection: Survey and Analysis. In *2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 849-855). IEEE.
- [3]. Deval, V., Dwivedi, V. K., Dixit, A., Norta, A., Shah, S. A., Sharma, R., & Draheim, D. (2024). Mobile smart contracts: exploring scalability challenges and consensus mechanisms. *IEEE Access*, 12, 34265-34288.
- [4]. Dubiel, M., Barghouti, Y., Kudryavtseva, K., & Leiva, L. A. (2024). On-device query intent prediction with lightweight LLMs to support ubiquitous conversations. *Scientific reports*, 14(1), 12731.
- [5]. Gill, S. S., Golec, M., Hu, J., Xu, M., Du, J., Wu, H., ... & Uhlig, S. (2025). Edge AI: A taxonomy, systematic review and future directions. *Cluster Computing*, 28(1), 18.
- [6]. Grzesik, P., & Mrozek, D. (2024). Combining machine learning and edge computing: Opportunities, challenges, platforms, frameworks, and use cases. *Electronics*, 13(3), 640.
- [7]. Kwon, C., & Kang, D. (2024). Overlay-ML: Unioning memory and storage space for on-device AI on mobile devices. *Applied Sciences*, 14(7), 3022.
- [8]. Li, Y., Dang, X., Tian, H., Sun, T., Wang, Z., Ma, L., ... & Bissyandé, T. F. (2025). An empirical study of AI techniques in mobile applications. *Journal of Systems and Software*, 219, 112233.
- [9]. Na, M., & Lee, J. (2024). Generative AI-enabled energy-efficient mobile augmented reality in multi-access edge computing. *Applied Sciences*, 14(18), 8419.
- [10]. Pan, M., Huang, A., Wang, G., Zhang, T., & Li, X. (2020, July). Reinforcement learning based curiosity-driven testing of android applications. In *Proceedings of the 29th ACM SIGSOFT international symposium on software testing and analysis* (pp. 153-164).
- [11]. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature machine intelligence*, 1(5), 206-215.
- [12]. Rustemi, A., & Dalipi, F. (2026). From Concept to Practice: A Blockchain-Based Solution for Secure and Efficient Academic Credentials in Higher Education. *IET Blockchain*, 6(1), e70030.
- [13]. Rustemi, A., Dalipi, F., & Risteski, A. (2025, June). The Convergence of IoT, AI, and Blockchain in Agriculture: A Survey and Research Challenges. In *2025 32nd International Conference on Systems, Signals and Image Processing (IWSSIP)* (pp. 1-6). IEEE.
- [14]. Rustemi, A., Atanasovski, V., Angelkoska, V., & Risteski, A. (2024). Implementation and Performance Analysis of a Practical System for Diploma Verification Based on Blockchain and Artificial Intelligence Technologies. *Journal of Natural Sciences & Mathematics (JNSM)*, 9.
- [15]. Shaheen, M., Farooq, M. S., & Umer, T. (2024). AI-empowered mobile edge computing: inducing balanced federated learning strategy over edge for balanced data and optimized computation cost. *Journal of Cloud Computing*, 13(1), 52.

- [16]. Slyusar, V., Kondratenko, Y., Shevchenko, A., & Yeroshenko, T. (2024). Some aspects of artificial intelligence development strategy for mobile technologies. *Journal of Mobile Multimedia*, 20(3), 525-554.
- [17]. Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2022). Decentralized identifiers (dids) v1. 0. W3C Recommendation, 19.
- [18]. Usman, A., Salihu, I. A., Ghali, A. A., Bello, B. L. M., Mu'azu, A. A., & Magaji, A. S. (2025). A Scoping Review of Artificial Intelligence Research Trends in Mobile Applications. *Journal of Informatics and Web Engineering*, 4(3), 382–407. <https://doi.org/10.33093/jiwe.2025.4.3.23>
- [19]. Valdez-Solis, W., Parra-Ullauri, J., Simeonidou, D., & Kertesz, A. (2026). Privacy and security for 6G networks via Fog/Edge Computing, Blockchain, and Federated Learning: A survey and taxonomy. *Journal of Network and Computer Applications*, 104510.