ERCIM fellowship Programme

Final scientific report

ERCIM Alain Bensoussan Fellowship Programme

ERCIM
European Research Consortium for Informatics and Mathematics

Fellow	Michail **Sidorov**
Host Organisation	Norwegian University of Science and Technology
Scientific coordinator	Jingyue **Li**

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

Scientific activity primarily was carried out based on the proposed timeline at the beginning of the ERCIM tenure. However, additional research collaborations were done which resulted in a larger number of publications prepared during the fellowship.

Main research activity

This activity focused on the design of a scalable wireless sensor node containing various sensing elements that would allow logging the status of the goods while they are transported along the cold supply chain, with a secure and easy data storage and access via blockchain integration. Hence, this work was split into two parts mainly the blockchain research part, and the embedded design part of the sensor node that would satisfy the cold supply chain needs.

Out of the numerous public blockchains available we have studied those with the highest potential to be used for IoT applications, such as Helium, MatchX, Nodle Network, IOTA 2.0, IoTeX, and Ethereum, which was mainly included due to popularity.

With the main blockchain selected research has then moved to looking into how cold supply chain operates. Dedicated supply chain blockchains were examined as part of this activity. Current sensor nodes and loggers used for supply chain tracking were then examined. Using gathered information our sensor node requirements were set. Sensor node has to record temperature, accidental drops, geographical location, etc. while the goods are transported along the supply chain and send this data using a low power wireless communication protocol to an applicable public blockchain.

The embedded design consisted of the following:

- Picking the appropriate electronic components;
- Initial prototyping;
- Schematic capture;
- Printed Circuit Board (PCB) design and preparation for manufacturing;

- PCB assembly and initial testing;
- Embedded firmware development.

There were several PCB revisions as necessary changes had to be done to ensure proper functionality of the sensor node. After the final prototype was assembled it was evaluated based on several criteria such as temperature monitoring accuracy, GPS-based tracking and GPS-less tracking capabilities. Furthermore, lifetime of the node was estimated based on the predefined operating scenarios. An application to access and visualize the stored data to determine quick status of the goods was created using TagoIO and Helium integration.

Additional research activity

This additional research activity was two-fold. One part was the continuation of my PhD research in conjunction with my current and former supervisors from Toyohashi University of Technology, Japan. This work concentrated on reviewing all possible bolted joint monitoring approaches used for structural health monitoring purposes.

Other half consisted of research utilising blockchain for various applications, such as:

- Improving LoRaWAN authentication with the help of NFTs;
- zk-SNARK integration with low power IoT devices for anonymity purposes;
- Data integrity verification for Wi-Fi based IoT devices.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Published

[1] Jing Huey Khor, Michail Sidorov, Seri Aathira Balqis Zulqarnain, “Scalable Ultralightweight Protocol for Public Blockchain-based Interoperable Supply Chain Management,” in *MDPI Sensors* (Impact Factor 3.847) 2023, 23, 3433. DOI: 10.3390/s23073433.

Short abstract: Scalability prevents public blockchains from being widely adopted for IoT applications such as supply chain management. Several existing solutions focus on increasing the transaction count, but none of them address scalability challenges introduced by re-source-constrained IoT device integration with these blockchains, especially for the purpose of ownership management. This paper solves the issue by proposing a scalable public blockchain-based protocol for the interoperable ownership transfer of tagged goods that is suitable for use with resource-constrained IoT devices such as widely used RFID tags. The use of a public blockchain is crucial for the proposed solution as it is essential to enable transparent ownership data transfer, guarantee data integrity, and provide on-chain data required for the protocol. A decentralized web application developed using the Ethereum blockchain and an InterPlanetary File System is used to prove the validity of the pro-posed lightweight protocol. A detailed security analysis is conducted to verify that the proposed lightweight protocol is secure from key disclosure, replay, man-in-the-middle, de-synchronization, and tracking attacks.

[2] Jing Huey Khor, Michail Sidorov, Ming Tze Ong, Shen Yik Chua, “Public Blockchain-based Data Integrity Verification for Low-power IoT Devices,” in *IEEE Internet of Things Journal* (Impact Factor 11.043), March, 2023. DOI: 10.1109/JIOT.2023.3259975.

Short abstract: The integration of sensor nodes with public blockchains is possible with the help of low-power communication networks that use Bluetooth Low Energy and LoRa. However, power-consuming Wi-Fi is still the main means of communication for the existing sensor nodes, especially in the urban environments. Typically high power consumption, private key disclosure, and high transaction fees prevent battery-powered sensor nodes from being integrated with a public blockchain. Hence, this paper proposes a data protection protocol that is able to guarantee the data integrity of the stored sensor data, help reduce transaction fees, and prolong battery life for IoT devices. A proof of concept is presented using an ESP32S2 device to evaluate and verify the performance of the proposed data storage protocol. A smart contract is designed and analysed using a formal smart contract analysis tool. A decentralized web application is designed to display and verify the sensor data extracted from the public blockchain. The power consumption, memory usage, and security of the proposed solution are evaluated.

[3] Jing Huey Khor, Michail Sidorov, N.T.M Ho, and T.H Chia, "Public Blockchain-based Lightweight Anonymous Authentication Platform Using Zk-SNARKs for Low-power IoT Devices" *2022 IEEE International Conference on Blockchain,* Espoo, Finland, pp. 370-375., August, 2022. DOI: 10.1109/BLOCKCHAIN55522.2022.00058.

Short abstract: Anonymous authentication is an important factor for IoT applications. The zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARK) is one of the popular methods that has been used for transacting anonymously in public blockchains. However, heavy computations are needed to perform it, hence there is a barrier that prevents resource-constrained IoT devices from implementing zk-SNARKs for anonymous transactions. This paper takes a modular approach and proposes a public blockchain-based lightweight anonymous authentication platform that is suitable for low-power IoT devices based on zk-SNARKs. A lightweight anonymous authentication protocol was designed using the SHA256 hash function and the heavy proving processes of the zk-SNARK protocol were offloaded to a powerful IoT machine. A proof of concept was created and evaluated.

In review

[4] Michail Sidorov, Jing Huey Khor, Alvin Chern Hao Wong, Ying Ying Lee, and Jingyue Li, "A Secure Authentication Scheme for LoRaWAN Nodes using On-Chain Non-Fungible Tokens," in review at *IEEE Internet of Things Journal* (Impact Factor 11.043). Submitted November 2022.

Short abstract: LoRaWAN is a very popular long range low power communication protocol. However, LoRaWAN root keys are susceptible to disclosure attacks. This work proposes an improvement to the current communication protocol by integrating NFTs into the equation for improving the security. Hence, the improvement allows to mitigate this issue. NFT is designed based on the Ethereum Request for Comments 721 standard. This scheme is developed using the SHA256 hash function and exclusive-OR operations. The security of the proposed scheme has been analysed and is proven to be secure from replay, man-in-the-middle, and cloning attacks.

Prepared for submission

[5] Michail Sidorov, Jing Huey Khor, Ren Ohmura, Yukihiro Matsumoto, and Jingyue Li, "In-Situ and IoT-based Bolted Joint Inspection and Monitoring Approaches Used for Structural Health Monitoring Purposes: A Review," prepared for potential submission to *IEEE Internet of Things Journal* (Impact Factor 11.043)

Short abstract: This work reviews approaches used for inspection and monitoring of bolted joints. Computer vision-based, percussion-based, ultrasonic-based, fiber bragg-based, remote unattended, and other methods are analysed and compared. The article further provides an overview of the future trend and challenges associated with future bolted joint monitoring approaches and their integration with Smart City via IoT and blockchain technology.

[6] Michail Sidorov, Jing Huey Khor, and Jingyue Li, "Tracking Cold Chain Goods with Sensor Nodes and Blockchain," prepared for potential submission to *IEEE Sensors Journal* (Impact Factor 4.325)

Short abstract: This work describes the design, evaluation, and blockchain integration of a sensor node used for tracking goods along the cold supply chain. True IoT blockchains are reviewed and the best one is chosen for this work. Current sensor nodes are reviewed, their drawbacks are described. Based on the information gathered a blockchain based solution is proposed.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

The 5th IEEE International Conference on Blockchain (Blockchain 2022), August 22 - 25, 2022, Espoo, Finland.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

The REP program was not completed during the fellowship duration.