

Combinando Internet das Coisas, Inteligência Artificial e Blockchain para Monitorar a Cadeia de Agroquímicos

Emiliano S. Monteiro¹, Maria Eloisa Mignoni¹ Rodrigo R. Righi²,
Cristiano A. da Costa², Rafael Kunst², Antônio Alberti³

¹Univ. do Estado de Mato Grosso Carlos Alberto Reis Maldonado (UNEMAT, MT)

²Universidade do Vale do Rio dos Sinos (PPGCA-UNISINOS, RS)

³Instituto Nacional de Telecomunicações (Inatel, MG)

{emiliano, eloisa}@unemat.br¹, {rrrighi, cac, rafaelkunst}@unisinis.br², alberti@inatel.br³

Abstract. *The movement of agrochemicals in the production chain is immense, providing opportunities for theft, misuse and tax evasion. Current national control is precarious and needs improvement, thus opening up a vast field of research. According to the literature in the area, the current traceability proposals use only a few sensors, in addition to the fact that there is no combination and integration between them. In this context, this work presents a model that allows the traceability of pesticides, combining sensors of Internet of Things (IoT), machine learning, fog networks, radio frequency identification (RFID) and blockchain. The differential of the model is the contribution of a modular proposal that allows security and reliability in the control of products. The developed model presented concise and promising results. When moving objects inside and outside containers, sensors capture and send action data for storage and analysis of the following layers of the model.*

Resumo. *A movimentação de agroquímicos na cadeia produtiva é imensa, oportunizando roubos, mal uso e evasão de impostos. O controle atual é precário e necessita de melhorias, possibilitando um vasto campo de pesquisa. Conforme a literatura na área, as propostas atuais de rastreabilidade usam apenas poucos sensores, além do fato de não existir combinação e integração entre eles. Nesse contexto, este trabalho apresenta um modelo que permite a rastreabilidade de defensivos agrícolas, combinando sensores de Internet das Coisas (IoT), aprendizado de máquina, redes de neblina (fog), identificação por rádio frequência (RFID) e blockchain. O diferencial do modelo está na contribuição de uma proposta modular e que permite segurança e confiabilidade no controle dos produtos. O modelo desenvolvido apresentou resultados concisos e promissores. Quando realizada a movimentação de objetos dentro de containers e fora destes, sensores capturam e enviam os dados das ações para armazenamento e análise das camadas seguintes do modelo.*

1. Introdução

O controle da movimentação das embalagens dos defensivos agrícolas, necessita de uma rastreabilidade eficiente e eficaz, não apenas para combate ao roubo nas propriedades rurais, mas também por questões de poluição do meio ambiente, saúde da população, uso exagerado, evasão fiscal, perdas financeiras para o agricultor e para o

Estado. Para a rastreabilidade das embalagens de defensivos agrícolas é comum o emprego de uma única forma de identificação, porém um único meio, como código de barras pode não ser suficiente, [Guo and Zhang 2010] e [Lin et al. 2018]. A identificação das embalagens dos defensivos agrícolas, geralmente não é um processo automatizado, ou mesmo informatizado, ao longo de toda a cadeia, não existindo um registro permanente imutável, de todos os eventos ocorridos durante a movimentação, [Fuertes et al. 2016] e [Sila-Nowicka and Thakuriah 2019]. A Identificação de produtos e sua movimentação tem vários benefícios quando a monitoração é feita internamente pela fazenda. A rastreabilidade é um dos fatores para a adoção de blockchain no setor agrícola. Percebe-se que há falta de controle e rastreamento na movimentação das embalagens de defensivos agrícolas, principalmente utilizando tecnologia computacional, pois o uso de ferramentas como *Machine Learning* (ML) para operações de agrupamentos, classificações e regressão e *blockchain* são raros. Neste contexto, a rastreabilidade é de fundamental importância para a prevenção dos problemas já citados.

Nesse contexto, o presente artigo apresenta o modelo MRPA (Modelo de Rastreabilidade Pervasiva de Agroquímicos) que atua na combinação de múltiplos sensores de IoT, ML e blockchain em um modelo para rastrear as embalagens de agroquímicos. Em especial, o MRPA aborda a cadeia de defensivos agrícolas. O modelo tem os sensores e microcontroladores organizados para monitorar o estado e a localização de defensivos agrícolas, monitorando assim o processo completo de rastreabilidade da cadeia. O diferencial está na recepção e processamento utilizando ML desses dados IoT e posterior gravação da informação em uma rede blockchain. Em suma, o modelo permite uma análise da movimentação, se já estava planejada ou não e, aciona alarmes caso alguma atitude suspeita seja detectada. A contribuição deste trabalho reside na combinação das tecnologias apresentadas de modo a oferecer uma solução com amparo judicial, indo também ao encontro de questões como preservação do meio ambiente e da saúde das pessoas, aspectos econômicos, evasão fiscal, além de evitar roubos.

Este artigo está organizado em 6 seções. A Seção 2 apresenta trabalhos correlatos ao tema de rastreabilidade de produtos, identificação de produtos e uso de tecnologias como IA e blockchain aplicadas na cadeia de suprimentos. A seção 3 descreve o Modelo de Rastreabilidade Pervasiva de Agroquímicos (MRPA), destacando a sua arquitetura e seu funcionamento. A Seção 4 mostra a metodologia de avaliação utilizada para os experimentos, enquanto a Seção 5 apresenta e discute os resultados. A Seção 6 apresenta trabalhos futuros, Por fim a seção 7 apresenta as considerações finais, enfatizando como foi atingida a contribuição proposta, e também relaciona iniciativas que podem ser abordadas na continuação deste trabalho.

2. Trabalhos relacionados

Esta seção relaciona os trabalhos correlatos à pesquisa realizada, bem como mostra oportunidades existentes na área. Foram selecionadas strings de busca, relacionadas com o assunto, tais como: *agrochemical*, *supply chain*, *rfid*, *blockchain*, *pesticide*, *traceability*, *ia*, *edge*, *fog*. Posteriormente as *strings* foram combinadas em páginas de buscas de revistas científicas como IEEE, ACM, Tandfonline, Hindawi, Plos One, MDI e Science Direct. Os resultados foram selecionados após a leitura de título e *abstract*, e também pela busca de palavras-chave do assunto de interesse.

Cada trabalho relacionado apresenta uma solução específica ou atende parcialmente ao controle efetivo de defensivos agrícolas. Em particular, são citadas funcionalidades de um processo completo a seguir, mencionando estudos que atendem partes do processo. Os produtos de interesse, além de seu alto valor, também apresentam riscos ao meio ambiente, sendo importante a detecção de movimento e uso correto destes, que foi explorada de diversas formas por [Fuertes et al. 2016], [Sila-Nowicka and Thakuriah 2019] e [Michelucci and Venturini 2020]. O uso de sensores para a detecção e manipulação de produtos já foi citado como uma forma de perceber a pirataria de produtos, pelas próprias características intrínsecas à sua natureza, [Blankenburg et al. 2015]. Outro estudo utiliza uma rede de borda (*Edge*), para facilitar a coleta de dados, descentralizada através de sensores e pequenos pré-processamentos, [Gai et al. 2020]. O uso de identificação por radiofrequência (RFID), logística reversa, blockchain e indústria 4.0, tem aparecido na literatura consultada, [Rejeb et al. 2020]. No caso da blockchain, esta tecnologia tem aparecido lado a lado com as cadeias de suprimento [Hu et al. 2021]. Os dados, uma vez lançados na rede *Edge*, para uma rede mais interna da organização, podem fazer uso de IA para detectar padrões (correlações e variações), [Toorajipour et al. 2020] e [Min 2010]. Outras formas de detecção de eventos são via regras de negócios ou gatilhos em aplicações e bancos de dados (via *triggers*) que também são uma forma de reforçar políticas comerciais, [Leveling et al. 2014]. Existe a possibilidade de exploração da integração, padronização, uso de tecnologias emergentes e ML [Konovalenko and Ludwig 2019]. Um dos aspectos abordados, é a capacidade de extrair dados de grandes volumes de dados, por métodos analíticos para extração de conhecimento, [Bemthuis 2019].

Entre outros tópicos, os trabalhos estudados abordam as dificuldades da implementação de RFID, como: custos, falta de padronização, reduzido número de fornecedores, e problemas de implantação, [Michael and McCathie 2005], protocolos para segurança e troca de informações com o uso de RFID, [Guo and Zhang 2010]. A intervenção humana também é considerada dificuldade. Neste sentido, utiliza-se IoT para reduzir a intervenção humana em atividades agrícolas, que envolvem registro de dados e enviam para um blockchain, discutido por [Lin et al. 2018]. Por fim, percebe-se uma lacuna neles pois, tratam de problemas específicos e os que abordam tecnologias sobre rastreabilidade, não utilizam uma combinação de sensores, nem análise e pré-processamento de dados coletados de diversas fontes. Finalizamos apontando os trabalhos com maior contribuição para a área estudada são: [Fuertes et al. 2016], [Lin et al. 2018], [Gai et al. 2020], [Blankenburg et al. 2015] e [Hu et al. 2021]; os trabalhos com relação indireta porém com contribuição oportuna são: [Guo and Zhang 2010], [Michael and McCathie 2005], [Sila-Nowicka and Thakuriah 2019].

3. Modelo MRPA

Esta seção apresenta o modelo MRPA (Modelo de Rastreabilidade Pervasiva de Agroquímicos). A visão geral do funcionamento está ilustrada na Figura 1.

3.1. Decisões de projeto

Quanto à estrutura do modelo, suas partes integrantes estão organizadas de forma a constituir uma sequência de blocos de *softwares* que se interligam via chamadas de serviços e funções disponíveis nos blocos seguintes. O modelo é composto de *hardware* (na forma de sensores e microcontroladores) e software. Quanto à dinâmica funcional, o modelo

de numeração de nós da rede (como endereços para a localização dos integrantes). O objetivo do modelo é ser totalmente automatizado, sem necessitar de intervenção humana para movimentar arquivos. Desta forma, desde os sensores até os bancos de dados, utilizam formatos simples como *int*, *decimal* e *string*, os quais são enviados dos programas clientes até os servidores, pelas suas respectivas portas (de banco de dados e blockchain). Os dados são armazenados em tabelas, que mantêm campos com tipos de dados básicos. Dados enviados para a blockchain continuam usando tipos básicos e são transmitidos via *JavaScript Object Notation* (JSON). O objetivo da simplicidade é evitar conversão de tipos dentro do fluxo de dados no modelo.

3.2.1. Descrição das Camadas

A primeira camada do modelo é uma rede formada por diversos sensores e microcontroladores para coletar dados sobre trânsito de defensivos agrícolas. Este modelo considera a utilização de 6 sensores, trabalhando integrados como o mínimo para sua implementação. Estes sensores devem estar dispostos em um pequeno *container* (uma caixa ou armário com uma porta). Dispostos a seguir: dois sensores através da parte superior, um deles encosta na embalagem; dois outros sensores na parte traseira do produto a ser monitorado, uma tag RFID na base da embalagem, um sensor de peso (módulo de carga) na base do *container*. Os sensores são: S1 - Sensor de luminosidade, S2 - Sensor de vibração, S3 - Sensor de peso (balança), S4 - Sensor de distância, S5 - Sensor mini câmera e S6 - RFID tag. Em sequência, o desempenho de cada sensor: S1 (luminosidade) deve ser acionado quando o *container* for aberto; S2 (vibração) deve ser acionado quando a embalagem for tocada ou movida dentro do container; S3 (peso) será acionado quando o produto for levantado; S4 (distância) quando o produto se distancia da sua posição original (por exemplo, foi retirado do *container*) ele será acionado e em sequência acionará o próximo; S5 (câmera) a qual irá tirar uma foto do funcionário e produto saindo da caixa; S6 sensor (RFID), utilizado para rastrear o produto pelo seu código na tag via radiofrequência.

Após a camada de IoT, as camadas intermediárias seguintes utilizam servidores (camadas 2 e 3). Nestas camadas são utilizados bancos de dados, programas de *script* (os quais implementam regras de negócio e operações de aprendizado de máquina, servidores de aplicação, uma blockchain, *decentralized application* (dApps)). Na camada 2, estão as primeiras regras de negócio implementadas via *triggers* ou programas externos ao banco, que podem ler os dados, gerar os primeiros alertas e também movimentar dados de interesse para a camada seguinte. Na camada 3, temos as seguintes funcionalidades: Machine Learning pode ser utilizada de várias formas, as operações mais expressivas são de clusterização para agrupar objetos e regressão para prever valores de variáveis dos dados coletados dos sensores em um banco de dados contendo uma tabela para o modelo treinado e outra com os dados reais, a partir deste ponto qualquer biblioteca python pode ser usada entre elas PyTorch e Scikit-learn; também pode-se destacar que comandos SQL podem preparar e movimentar dados antes de seu tratamento por python com clausulas como *groupby* e *orderby*. Para visualização de dados: *seaborn.pairplot*), a emissão de alertas mais refinados, alimentação de um painel de visualização (uma página *web*) com gráficos estatísticos e finalmente é depositado o registro dos eventos na blockchain. A persistência de dados é implementada de duas formas, em uma tabela no banco de dado e em uma blockchain. No servidor de banco de dados, utiliza-se uma tabela com a mesma

estrutura em ambas as camadas 2 e 3. Os principais campos são: a) descrição; b) código de identificação do Arduino; c) um campo para guardar a captura de uma imagem; d) data e hora do dado coletado; e) o dado numérico coletado pelo sensor; f) um campo tipo de microcontrolador. Estes dados também são enviados para a blockchain, utilizando uma classe com tipos simples evitando-se assim conversões de tipo.

3.2.2. Atores e Fluxo de Dados

Os principais personagens envolvidos na interação com o modelo são: a) os funcionários responsáveis pela manipulação dos defensivos, b) o agricultor interessado em acompanhar a rastreabilidade. Os funcionários, ao interagirem com os defensivos, disparam uma série de sensores. A partir desse momento o modelo entra em funcionamento automaticamente. O agricultor acompanha toda a movimentação dos defensivos pela camada 4, onde ocorre a apresentação em uma página web via dApp. Partindo do pressuposto de que embalagens de defensivos são guardadas em locais fechados (como armários, cofres, caixas). Ao interagir com o armário e a embalagem, inicia-se o processo que movimenta o modelo. O trânsito de dados ocorre da seguinte forma: o funcionário, ao abrir o armário e manusear a embalagem, dispara os sensores. Estes sensores coletam e enviam os dados para o microcontrolador que, por sua vez encaminha esses dados para o banco de dados em uma tabela. Posteriormente, aplicam-se regras de negócio (via *triggers e store procedure*) e scripts de aprendizado de máquina, ambos enviam seus resultados para uma tabela temporária, os dados seguem dois caminhos: vão para a persistência em uma blockchain e são preparados para a exibição em um painel de visualização via web. A moitoração vai desde o momento que o funcionário pega o defensivo até a aplicação.

4. Metodologia de Avaliação

Para avaliar o modelo, foi desenvolvido um protótipo em escala reduzida. Foi observada: a capacidade de interconexão das camadas e a troca de dados entre elas. A implementação de cada camada foi feita de forma individual. O passo seguinte para as avaliações de interconexões. A constatação da funcionalidade operacional deste protótipo foi dada pela percepção do trânsito correto de dados, entre a origem, meio e fim do modelo. A carga de trabalho de entrada realizou-se pelo acionamento de sensores, que enviaram dados numéricos em formato decimal para o banco de dados. Os sensores foram alternados de forma a testá-los individualmente e depois em grupos de 2, conectados aos microcontroladores Arduinos. Tabelas do banco de dados foram enviadas via *script* entre bancos e a blockchain em intervalos regulares de 20 segundos. No cenário da avaliação consistiu na utilização de um analisador de protocolo (*wireshark*) para monitorar o trânsito de dados dentro do *pipeline* do processo deste modelo. Este acompanhamento do tráfego foi feito durante o funcionamento em cada camada. As métricas de avaliação foram: da camada 1 para a 2 e tempo de transmissão em intervalos de 1 segundo. Quanto à persistência de dados na camada 2, foi o tempo que o servidor do banco levou para receber e gravar os dados, medido via observação de *timestamp* dos registros recebidos, a blockchain pelo tempo de registro de transação em segundos e os processos em cada camada, de forma geral pela observação, via comando *top* do consumo de processador e memória. Durante a simulação, foi acompanhado desde o momento do disparo do sensor até a representação da informação no painel de visualização.

As atividades de banco de dados foram monitoradas pelas suas ferramentas. As estatísticas de consumo de processador e memória pelas ferramentas do próprio sistema operacional, inclusive de processos da blockchain. O tempo de carga da interface de visualização das dApps, foi fornecido pelas métricas de performance dos navegadores. As *tags* RFID foram registradas no banco de dados com campo do tipo *timestamp*. Onde foi indicado o uso de microcontrolador foi utilizado *hardware* Arduino. Onde foi indicado banco de dados e blockchain, foram utilizados MariaDB e Ethereum. Programas em python foram feitos e interpretados via Anaconda. A aplicação distribuída (dApp) para visualização de dados utilizou web3js. No protótipo desenvolvido, foi criado um mini armário, no qual os sensores foram posicionados para que pudessem ser testados. Na Figura 2, é possível observar: a) a parte interna do armário com componentes e um simulacro de embalagem, ainda nesta figura observa-se a parte traseira externa com os microcontroladores Arduino, *protoboard* e fiação.

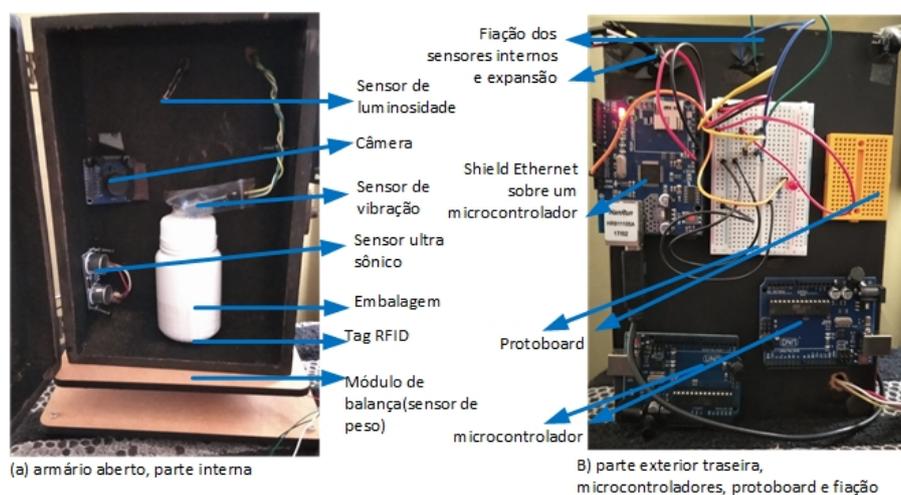


Figura 2. Protótipo desenvolvido: (a) armário aberto com sensores visíveis e simulacro de defensivo, (b) componentes da parte traseira externa.

5. Resultados

O modelo MRAP comportou-se dentro do esperado para as suas funções. Obteve-se o comportamento modular de cada camada e seus componentes, uma vez que podem ser trocados (desde os sensores, até programas de *script* e meios de armazenamento). As camadas intermediárias (2 e 3), foram implementadas via *virtual machine* (VM), com as seguintes características: sistema operacional Linux 64-bit, CPU: 2 vcpu, Disco: 40gb, Rede: ethernet, e memória no primeiro de 2500 MB, no segundo de 2300MB. Estas máquinas virtuais executaram sobre o *hypervisor Oracle Virtual Box*. Apesar da diferença de memória RAM entre elas, a execução consumiu recursos de forma similar: a) Processamento - consumo mínimo quando ocioso de até 5% de CPU, quando rodando Anaconda, Python outros softwares entre 28 a 31%; b) memória - Oscilando entre 22 e 34 MB, c) escritas foram realizadas usando até 41,6 MB/s.

Cada VM utilizando um endereço IP, fornecido via NAT pelo hypervisor, conseguiu enviar pacotes ICMP com um RTT próximos de 18.060 MS para a rede externa, passando pelo hypervisor. O hypervisor enviou pacotes para uma rede externa usando RTT

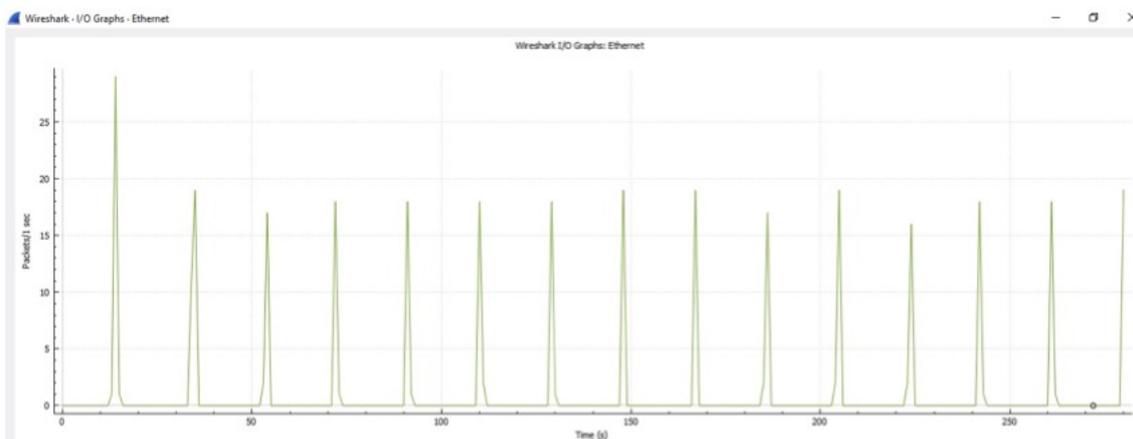


Figura 3. Frequência de transmissão e dados entre camadas.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IP Protocol Types	221				0,0002	100%	0,0300	17,962
TCP	221				0,0002	100,00%	0,0300	17,962

Display filter: `http`

Figura 4. Exemplo de coleta de pacotes mostrando comunicação entre camadas.

médio de 14 MS. O envio de pacotes dos sensores para o banco de dados, foi monitorado via analisador de protocolos durante a transmissão. Houve pouca variação, microcontrolador e o hypervisor estavam em redes com tráfego pré-existentes que não puderam ser totalmente isolados (Figura 3). Uma forma de envio de dados dos arduínos para os servidores de banco, foi via requisições HTTP GET, via TCP, (Figura 4). Não houve perda de pacotes nestas requisições. Processos rodando diretamente (localmente) nos servidores da camada 2 e 3, levam entre 4.67 e 5.97 MS para realizar operações de inserção de dados na instância de banco (MariaDB). Microcontroladores (na camada 1) enviando dados diretamente para uma instância de banco (na camada 2), levam 2 a 3 vezes mais tempo. Fatores que interferiram foram: a rede Ethernet, a rede 802.11 e se o servidor está ocupado com outro processo.

Processos como o editor *Spyder* com um *script* python podem ter picos de execução, gastando de 15 a 38% de CPU dentro das VMs, o que indica a necessidade das camadas 2 e 3 possuírem RAM e discos mais eficientes. Na camada 3, aplicações como Ganache (um simulador de blockchain), pode ocupar mais de 54% de CPU em execução e estabilizar em aproximados 16% em ociosidade. Um nó *geth* pode ocupar de 6,8 a 19,6% de RAM até 18,1% de CPU, durante execução de apenas 1 nó Ethereum. A entrega de dados na última camada pode ser vista na Figura 5, os picos com valores mais altos indicam abertura de porta do armário.

6. Trabalhos futuros

Identificam-se os seguintes pontos de melhoria e desenvolvimento futuros: a) testes, com tecnologias de rede diferentes, principalmente as redes de baixa potência ou 5G, onde houver; b) a possibilidade de desenvolvimento de painéis, para visualização sobre a execução e performance de códigos; c) na camada intermediária do modelo, estendê-lo



Figura 5. Painel usado na camada de visualização para apresentar dados do sensor de luminosidade. Elevações indicam abertura de porta do armário.

com web services para integração com ERPs; d) o monitoramento de elementos utilizando o conceito de cerca virtual, disparando alarmes quando o defensivo (ou outros objetos de interesse), sai da área delimitada; e) estudos futuros devem considerar problemas de interferência no campo causada pelas áreas de preservação permanente, água, folhagem do próprio plantio e máquinas operando nos talhões, permitindo inclusive mapear áreas de sombra de sinal em talhões; f) a alocação de uma das camadas responsáveis pelo processamento e a camada de visualização em serviços de nuvem.

7. Conclusão

Este artigo apresentou o modelo MRPA para realizar o monitoramento de defensivos agrícolas. Para tal, utiliza uma combinação de tecnologias emergentes como IoT, IA e *blockchain*. Além dos escopos técnico e científico, as contribuições para a sociedade podem ser vistas da seguinte maneira: a) acompanhar o tempo de exposição do funcionário ao defensivo, b) evitar mal uso do defensivo, o que acarreta problemas de saúde com doenças graves como o câncer, c) possibilita a redução de dano ambiental, d) sonegação fiscal pelo uso de produtos piratas. O protótipo em ambiente controlado teve resultados promissores enviando dados dos microcontroladores para os servidores de bancos de dados. Estes microcontroladores foram programados para transmitir em intervalos de 1 segundo. Os bancos de dados foram configurados para registrar dados em um campo extra do tipo timestamp, de forma que a diferença de tempo pudesse ser percebida e usada para análise da cadeia de suprimentos. A média de tempo de gravação de dados em uma blockchain com Ethereum foi de até 15 segundos. O tempo de carga de dados do banco e apresentação destes no painel de visualização é 4515 ms.

Até o momento, o modelo apresentou resultados promissores, pois os tempos de trânsito de dados no pipeline do fluxo de dados é aceitável e inferior a 19 segundos no total (contando todas as camadas). Sobre limitações do modelo, não foram utilizados sensores para análise de solo e água. Os autores destacam a necessidade de integração com outras plataformas proprietárias e com *web services* do poder público. Em adição, são necessários testes dentro de talhões produtivos para medir interferências de vegetação e distâncias na transmissão de dados.

Agradecimentos

Os autores gostariam de agradecer aos seguintes órgãos pelo apoio à pesquisa: CAPES, CNPq e FAPERGS.

Referências

- Bemthuis, R. (2019). Business logic for resilient supply chain logistics. In *IEEE 23rd Int. Enterprise Distributed Object Computing Workshop (EDOCW)*, pages 190–195.
- Blankenburg, M., Horn, C., and Krüger, J. (2015). Detection of counterfeit by the usage of product inherent features. *Procedia CIRP*, 26:430–435. 12th Global Conference on Sustainable Manufacturing – Emerging Potentials.
- Fuertes, G., Soto, I., Carrasco, R., Vargas, E., Sabattin, J., and Lagos, C. (2016). Intelligent packaging systems: Sensors and nanosensors to monitor food quality and safety. *Journal of Sensors*, 2016:1–8.
- Gai, K., Fang, Z., Wang, R., Zhu, L., Jiang, P., and Choo, K.-K. R. (2020). Edge computing and lightning network empowered secure food supply management. *IEEE Internet of Things Journal*, PP:1–1.
- Guo, Z. and Zhang, X. (2010). The application of rfid technology in the logistics supply chain. In *2010 3rd International Conference on Computer Science and Information Technology*, volume 2, pages 518–520.
- Hu, S., Huang, S., Huang, J., and Su, J. (2021). Blockchain and edge computing technology enabling organic agricultural supply chain: A framework solution to trust crisis. *Computers Industrial Engineering*, 153:107079.
- Konovalenko, I. and Ludwig, A. (2019). Event processing in supply chain management – the status quo and research outlook. *Computers in Industry*, 105:229–249.
- Leveling, J., Edelbrock, M., and Otto, B. (2014). Big data analytics for supply chain management. volume 2015.
- Lin, J., Shen, Z., Zhang, A., and Chai, Y. (2018). Blockchain and iot based food traceability for smart agriculture. In *Proceedings of the 3rd International Conference on Crowd Science and Engineering, ICCSE'18*, New York, NY, USA. Association for Computing Machinery.
- Michael, K. and McCathie, L. (2005). The pros and cons of rfid in supply chain management. In *International Conference on Mobile Business (ICMB'05)*, pages 623–629.
- Michelucci, U. and Venturini, F. (2020). New autonomous intelligent sensor design approach for multiple parameter inference. *Engineering Proceedings*, 2(1).
- Min, H. (2010). Artificial intelligence in supply chain management: Theory and applications. *International Journal of Logistics-research and Applications - INT J LOGIST-RES APPL*, 13:13–39.
- Rejeb, A., Simske, S., Rejeb, K., Treiblmaier, H., and Zailani, S. (2020). Internet of things research in supply chain management and logistics: A bibliometric analysis. *Internet of Things*, 12:100318.
- Sila-Nowicka, K. and Thakuriah, P. (2019). Multi-sensor movement analysis for transport safety and health applications. *PLOS ONE*, 14(1):1–28.
- Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., and Fischl, M. (2020). Artificial intelligence in supply chain management: A systematic literature review. *Journal of Business Research*, 122:502–517.