Scopus

Documents

Olanrewaju, R.F.[a] , Khan, B.U.I.[a] , Kiah, M.L.M.[b] , Abdullah, N.A.[b] , Goh, K.W.[c]

Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT

(2022) *Electronics (Switzerland)*, 11 (23), art. no. 3982, .

DOI: 10.3390/electronics11233982

[a] Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur, 50728, Malaysia

[b] Department of Computer System & Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

[c] Faculty of Data Science and Information Technology, INTI International University, Nilai, 71800, Malaysia

Abstract

The inclusion of mobility-based Internet-of-Things (IoT) devices accelerates the data transmission process, thereby catering to IoT users' demands; however, securing the data transmission in mobility-based IoT is one complex and challenging concern. The adoption of unified security architecture has been identified to prevent side-channel attacks in the IoT, which has been discussed extensively in developing security solutions. Despite blockchain's apparent superiority in withstanding a wide range of security threats, a careful examination of the relevant literature reveals that some common pitfalls are associated with these methods. Therefore, the proposed scheme introduces a novel computational security framework wherein a branched and decentralized blockchain network is formulated to facilitate coverage from different variants of side-channel IoT attacks that are yet to be adequately reported. A unique blockchain-based authentication approach is designed to secure communication among mobile IoT devices using multiple stages of security implementation with Smart Agreement and physically unclonable functions. Analytical modeling with lightweight finite field encryption is used to create this framework in Python. The study's benchmark results show that the proposed scheme offers 4% less processing time, 5% less computational overhead, 1% more throughput, 12% less latency, and 30% less energy consumption compared to existing blockchain methods.

Author Keywords

blockchain; Ethereum; Internet-of-Things; mobility; physical unclonable function; secure data transmission; side-channel attack; smart agreement

References

- Hassanien, A.E., Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V.
(2020) *Internet of Things, Smart Computing and Technology: A Roadmap Ahead*, Springer International Publishing, Cham, Switzerland

- Kumar, A., Balamurugan, B., Chatterjee, J.M., Raj, P.
(2020) *Internet of Things Use Cases for the Healthcare Industry*, Springer International Publishing, Cham, Switzerland

- Murugesan, S., Jain, S.
(2021) *Smart Connected World-Technologies and Applications Shaping the Future*, Springer International Publishing, Cham, Switzerland

- Ismail, Y.
(2019) *Internet of Things (IoT) for Automated and Smart Applications*, IntechOpen, London, UK

- Sun, J., Han, G., Wang, Y., Liu, P.
Memristor-based neural network circuit of emotion congruent memory with mental fatigue and emotion inhibition
(2021) *IEEE Trans. Biomed. Circuits Syst*, 15, pp. 606-616.
34156947

- Sun, J., Han, G., Zeng, Z., Wang, Y.
Memristor-based neural network circuit of full-function Pavlov associative memory with time delay and variable learning rate
(2020) *IEEE Trans. Cybern*, 50, pp. 2935-2945.
31751264

- Sun, J., Wang, Y., Liu, P., Wen, S., Wang, Y.
Memristor-based neural network circuit with multimode generalization and differentiation on Pavlov associative memory
(2022) *IEEE Trans. Cybern*, pp. 1-12.
36129863

- Ghazal, T.M., Hasan, M.K., Alshurideh, M.T., Alzoubi, H.M., Ahmad, M., Akbar, S.S., Al Kurdi, B., Akour, I.A.
IoT for smart cities: Machine learning approaches in smart healthcare—A review
(2021) *Future Internet*, 13.

- Staddon, E., Loscri, V., Mitton, N.
Attack categorisation for IoT applications in critical infrastructures, a survey
(2021) *Appl. Sci*, 11.

- Balogh, S., Gallo, O., PLoSzek, R., Špaček, P., Zajac, P.
IoT security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques
(2021) *Electronics*, 10.

- Sharma, G., Vidalis, S., Anand, N., Menon, C., Kumar, S.
A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues
(2021) *Electronics*, 10.

- Tsiknas, K., Taketzis, D., Demertzis, K., Skianis, C.
Cyber threats to industrial IoT: A survey on attacks and countermeasures
(2021) *IoT*, 2.

- Méndez Real, M., Salvador, R.
Physical side-channel attacks on embedded neural networks: A survey
(2021) *Appl. Sci*, 11.

- Hong, S.
(2019) *Side Channel Attacks*,
MDPI Books, Basel, Switzerland

- Dogruluk, E., Macedo, J., Costa, A.
A countermeasure approach for Brute-Force timing attacks on cache privacy in named data networking architectures
(2022) *Electronics*, 11.

- Randolph, M., Diehl, W.
Power side-channel attack analysis: A review of 20 years of study for the layman
(2020) *Cryptography*, 4.

- Lo, O., Buchanan, W.J., Carson, D.
Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)
(2016) *J. Cyber Secur. Technol*, 1, pp. 88-107.

- Azizi, N., Malekzadeh, H., Akhavan, P., Haass, O., Saremi, S., Mirjalili, S.
IoT–Blockchain: Harnessing the power of Internet of Thing and blockchain for smart supply chain
(2021) *Sensors*, 21.
34577261

- Shahbazi, Z., Byun, Y.C.
Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing
(2021) *Sensors*, 21.

- Gardas, B.B., Heidari, A., Navimipour, N.J., Unal, M.
A fuzzy-based method for objects selection in blockchain-enabled edge-IoT platforms using a hybrid multi-criteria decision-making model
(2022) *Appl. Sci*, 12.

- Heidari, A., Jabraeil Jamali, M.A., Jafari Navimipour, N., Akbarpour, S.
Deep Q-learning technique for offloading offline/online computation in Blockchain-enabled green IoT-edge scenarios
(2022) *Appl. Sci*, 12.

- Jafar, U., Aziz, M.J.A., Shukur, Z.
Blockchain for electronic voting system—Review and open research challenges
(2021) *Sensors*, 21.

- Srinivasu, P.N., Bhoi, A.K., Nayak, S.R., Bhutta, M.R., Woźniak, M.
Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network
(2021) *Electronics*, 10.

- Kwon, D., Hong, S., Kim, H.
Optimizing implementations of non-profiled deep learning-based side-channel attacks
(2021) *IEEE Access*, 10, pp. 5957-5967.

- Le, A.T., Hoang, T.T., Dao, B.A., Tsukamoto, A., Suzaki, K., Pham, C.K.
A real-time cache side-channel attack detection system on RISC-V out-of-order processor
(2021) *IEEE Access*, 9, pp. 164597-164612.

- Mukhtar, N., Fournaris, A.P., Khan, T.M., Dimopoulos, C., Kong, Y.
Improved hybrid approach for side-channel analysis using efficient convolutional neural network and dimensionality reduction
(2020) *IEEE Access*, 8, pp. 184298-184311.

- Moini, S., Tian, S., Holcomb, D., Szefer, J., Tessier, R.
Power side-channel attacks on BNN accelerators in remote FPGAs
(2021) *IEEE J. Emerg. Sel. Top. Circuits Syst*, 11, pp. 357-370.

- Ghandali, S., Ghandali, S., Tehranipoor, S.
Deep K-TSVM: A novel profiled power side-channel attack on AES-128
(2021) *IEEE Access*, 9, pp. 136448-136458.

- Ng, J.S., Chen, J., Chong, K.S., Chang, J.S., Gwee, B.H.
A highly secure FPGA-based dual-hiding asynchronous-logic AES accelerator against side-channel attacks
(2022) *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, 30, pp. 1144-1157.

- Vuppala, S., Mady, A.E.D., Kuenzi, A.
Moving target defense mechanism for side-channel attacks
(2019) *IEEE Syst. J*, 14, pp. 1810-1819.

- Ghosh, A., Nath, M., Das, D., Ghosh, S., Sen, S.
Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection
(2022) *IEEE Microw. Wirel. Compon. Lett*, 32, pp. 784-787.

- Jevtic, R., Otero, M.G.
Methodology for complete decorrelation of power supply EM side-channel signal and sensitive data
(2022) *IEEE Trans. Circuits Syst. II Express Briefs*, 69, pp. 2256-2260.

- Liu, W., Wang, R., Qi, X., Jiang, L., Jing, J.
Multiclass classification-based side-channel hybrid attacks on strong PUFs
(2022) *IEEE Trans. Inf. Forensics Secur*, 17, pp. 924-937.

- Ensan, S.S., Nagarajan, K., Khan, M.N.I., Ghosh, S.
SCARE: Side Channel Attack on In-Memory Computing for Reverse Engineering
(2021) *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, 29, pp. 2040-2051.

- Kim, T., Shin, Y.
ThermalBleed: A practical thermal side-channel attack
(2022) *IEEE Access*, 10, pp. 25718-25731.

- Antognazza, F., Barenghi, A., Pelosi, G.
Metis: An integrated morphing engine CPU to protect against side channel attacks
(2021) *IEEE Access*, 9, pp. 69210-69225.

- Ha, G., Chen, H., Jia, C., Li, M.
Threat model and defense scheme for side-channel attacks in client-side deduplication
(2023) *Tsinghua Sci. Technol*, 28, pp. 1-12.

- Kulow, A., Schamberger, T., Tebelmann, L., Sigl, G.
Finding the needle in the haystack: Metrics for best trace selection in unsupervised side-channel attacks on blinded RSA
(2021) *IEEE Trans. Inf. Forensics Secur*, 16, pp. 3254-3268.

- Liu, H., Han, D., Li, D.
Fabric-IoT: A blockchain-based access control system in IoT
(2020) *IEEE Access*, 8, pp. 18207-18218.

- Hasan, H.R., Salah, K., Yaqoob, I., Jayaraman, R., Pesic, S., Omar, M.
Trustworthy IoT data streaming using blockchain and IPFS
(2022) *IEEE Access*, 10, pp. 17707-17721.

- Rodrigues, C.K.D.S., Rocha, V.
Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions
(2021) *IEEE Lat. Am. Trans*, 19, pp. 1199-1206.

- Zhou, J., Feng, G., Wang, Y.
Optimal deployment mechanism of blockchain in resource-constrained IoT systems
(2022) *IEEE Internet Things J*, 9, pp. 8168-8177.

- Ren, J., Li, J., Liu, H., Qin, T.
Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT
(2022) *Tsinghua Sci. Technol*, 27, pp. 760-776.

- Xu, C., Qu, Y., Luan, T.H., Eklund, P.W., Xiang, Y., Gao, L.
A lightweight and attack-proof bidirectional blockchain paradigm for Internet of Things
(2022) *IEEE Internet Things J*, 9, pp. 4371-4384.

- Alrubei, S.M., Ball, E., Rigelsford, J.M.
A secure blockchain platform for supporting AI-enabled IoT applications at the Edge layer
(2020) *IEEE Access*, 10, pp. 18583-18595.

- Hao, X., Yeoh, P.L., Ji, Z., Yu, Y., Vucetic, B., Li, Y.
Stochastic analysis of double blockchain architecture in IoT communication networks
(2022) *IEEE Internet Things J*, 9, pp. 9700-9711.

- Whaiduzzaman, M., Mahi, M.J.N., Barros, A., Khalil, M.I., Fidge, C., Buyya, R.
BFIM: Performance measurement of a blockchain based hierarchical tree layered

fog-IoT microservice architecture
(2021) *IEEE Access*, 9, pp. 106655-106674.

- Ullah, Z., Raza, B., Shah, H., Khan, S., Waheed, A.
Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment
(2022) *IEEE Access*, 10, pp. 36978-36994.

- Qu, Y., Pokhrel, S.R., Garg, S., Gao, L., Xiang, Y.
A blockchained federated learning framework for cognitive computing in Industry 4.0 networks
(2020) *IEEE Trans. Ind. Inform*, 17, pp. 2964-2973.

- Qiu, C., Wang, X., Yao, H., Du, J., Yu, F.R., Guo, S.
Networking integrated cloud–edge–end in IoT: A blockchain-assisted collective Q-learning approach
(2021) *IEEE Internet Things J*, 8, pp. 12694-12704.

- Mothukuri, V., Parizi, R.M., Pouriyeh, S., Dehghantanha, A., Choo, K.K.R.
FabricFL: Blockchain-in-the-Loop Federated Learning for trusted decentralized systems
(2022) *IEEE Syst. J*, 16, pp. 3711-3722.

- Miao, Y., Liu, Z., Li, H., Choo, K.K.T., Deng, R.H.
Privacy-preserving Byzantine-robust federated learning via blockchain systems
(2022) *IEEE Trans. Inf. Forensics Secur*, 17, pp. 2848-2861.

- Weng, J., Weng, J., Zhang, J., Li, M., Zhang, Y., Luo, W.
DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive
(2021) *IEEE Trans. Dependable Secur. Comput*, 18, pp. 2438-2455.

- Qin, Z., Ye, J., Meng, J., Lu, B., Wang, L.
Privacy-preserving blockchain-based federated learning for marine Internet of Things
(2022) *IEEE Trans. Comput. Soc. Syst*, 9, pp. 159-173.

- Shahbazi, Z., Byun, Y.C.
Blockchain-based event detection and trust verification using natural language processing and machine learning
(2022) *IEEE Access*, 10, pp. 5790-5800.

- Peng, Z.
VFChain: Enabling verifiable and auditable federated learning via blockchain systems
(2022) *IEEE Trans. Netw. Sci. Eng*, 9, pp. 173-186.

- Sun, J., Wu, Y., Wang, S., Fu, Y., Chang, X.
Permissioned blockchain frame for secure federated learning
(2022) *IEEE Commun. Lett*, 26, pp. 13-17.

- Ayaz, F., Sheng, Z., Tian, D., Guan, Y.L.
A blockchain-based federated learning for message dissemination in vehicular networks
(2022) *IEEE Trans. Veh. Technol*, 71, pp. 1927-1940.

- Li, J., Niyato, D., Hong, C.S., Park, K.-J., Wang, L., Han, Z.
Cyber insurance design for validator rotation in sharded blockchain networks: A hierarchical game-based approach
(2021) *IEEE Trans. Netw. Serv. Manag*, 18, pp. 3092-3106.

- Feng, S., Wang, W., Xiong, Z., Niyato, D., Wang, P., Wang, S.S.
On cyber risk management of blockchain networks: A game theoretic approach
(2021) *IEEE Trans. Serv. Comput*, 14, pp. 1492-1504.

- Guo, S., Dai, Y., Guo, S., Qiu, X., Qi, F.
Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain
(2020) *IEEE Trans. Veh. Technol*, 69, pp. 5549-5561.

- Kruminis, E., Navaie, K.
Game-theoretic analysis of an exclusively transaction-fee reward blockchain system
(2022) *IEEE Access*, 10, pp. 5002-5011.

- Zhang, M., Eliassen, F., Taherkordi, A., Jacobsen, H.A., Chung, H.-M., Zhang, Y.
Demand–response games for peer-to-peer energy trading with the Hyperledger blockchain
(2022) *IEEE Trans. Syst. Man Cybern. Syst*, 52, pp. 19-31.

- Jiang, S., Li, X., Wu, J.
Multi-leader multi-follower Stackelberg game in mobile blockchain mining
(2022) *IEEE Trans. Mob. Comput*, 21, pp. 2058-2071.

- Arena, F., Pau, G., Severino, A.
A review on IEEE 802.11p for intelligent transportation systems
(2020) *J. Sens. Actuator Netw*, 9.

- Ahn, J., Kim, Y.Y., Kim, R.Y.
A novel WLAN Vehicle-To-Anything (V2X) channel access scheme for IEEE 802.11p-based next-generation connected car networks
(2018) *Appl. Sci*, 8.

- Zanaj, E., Caso, G., Nardis, L.D., Mohammadpour, A., Alay, O., Benedetto, M.G.D.
Energy efficiency in short and wide-area IoT technologies—A survey
(2021) *Technologies*, 9.

Correspondence Address
Khan B.U.I.; Department of Electrical and Computer Engineering, Malaysia; email: burhan.iium@gmail.com
Goh K.W.; Faculty of Data Science and Information Technology, Malaysia; email: khangwen.goh@newinti.edu.my

Publisher: MDPI

ISSN: 20799292
Language of Original Document: English
Abbreviated Source Title: Electronics (Switzerland)
2-s2.0-85143665386
Document Type: Article
Publication Stage: Final
Source: Scopus