Poster: DEAN: A Blockchain-Inspired Consensus Protocol Enabling Trustworthy Edge Computing

Abdullah Al-Mamun[1], Jun Dai[2], Xiaohua Xu[3], Mohammad Sadoghi[4], Haoting Shen[1], Dongfang Zhao[1,4]
[1]*University of Nevada, Reno* [2]*Cal State University, Sacramento* [3]*Kennesaw State University* [4]*UC Davis*

***Abstract*—One open challenge in the edge computing paradigm lies in the uncertain data integrity and fidelity on edge nodes and end devices, e.g., sensors and controllers. This paper proposes a cooperative consensus protocol across edge nodes and end devices, namely DEAN, to prevent data manipulation and falsification under resource constraints of limited storage, computing, and network capacity. Specifically, DEAN leverages an in-memory blockchain with an inexpensive proof-of-work mechanism, effectively achieving low resource consumption on edge nodes and end devices. Preliminary experiments show that DEAN exhibits high resilience to arbitrary failures and outperforms the state-of-the-art blockchain systems in terms of transaction throughput.**

I. Introduction

Edge computing offers an efficient means to process collected data (e.g., from sensors, controllers, and other end devices) at nearby edge nodes as opposed to transferring data back to remote data centers. Edge computing saves the network traffic and improves application performance, particularly for those latency-sensitive scenarios such as virtual reality [1]; yet, edge computing brings several new technical challenges, including security and privacy concerns with edge nodes and sensors [2], [3]. The root cause of these new concerns lies in the fact that most security techniques used in data centers and cloud computing [4] are hardly directly applicable to the edge nodes and sensors due to the various resource constraints on the edge device side in terms of CPU, memory, storage, network, and power. Notably, several notorious incidents [5], [6] were already reported regarding security concerns over edge computing.

This paper focuses on addressing the concerns that break data integrity and trustworthiness of edge devices. Specifically, encryption (e.g., hashing, salting, digital signature, etc.) can be used as a common way to ensure data integrity in cloud computing. However, the high requirement of computational capability makes it unfeasible in an edge computing environment. The blockchain-based approach has instead been explored as a more reliable solution to deliver integrity, as blockchain promises 51% nodes will remain fault-tolerant even with transparency and anonymity [7]. However, due to the excessive message passing overhead, the high computational power requirement, and full replication across nodes, the existing blockchain mechanisms are not directly applicable to the edge computing ecosystem.

Several orthogonal approaches have been proposed to guarantee security in edge computing, but with the focus only on application security. Leakscope [8] helps to identify the potential data leakage vulnerabilities from mobile apps. IOTGUARD [9] protects users from unsafe and insecure device states by monitoring the behavior of IoT and trigger-action platform apps. IoTMon [10] includes an assessment of the safety risk of each discovered inter-app interaction chain based on its physical influence. Ifttt [11] has proposed a framework for information flow tracking in IoT applications. None of these techniques are modeled to support the blockchain-like yet **lightweight** solution that could guarantee the fault-tolerance of data.

We propose a unique blockchain-like solution crafted with a light-weight consensus protocol that makes the blockchain technique fully applicable to the edge ecosystem under extreme resource constraints. We leverage the constrained resources in edge computing based on two steps. *First*, to address the pressure on limited memory, the edge sensors keep only the recent blocks while the edge nodes keep the full replica[1]. The sensors can always update the memory with the latest blocks from the connected edge nodes whenever it is necessary. *Second*, to minimize the requirement for computational power, and massive communication overhead, the block validation process is mainly controlled by the interconnected edge nodes, while the sensors participate only when more than 50% edge nodes are compromised, but with an especially designed light-weight proof-of-work consensus mechanism.

II. Models and Assumptions

We consider the worst case in which an internal adversary has got authenticated to either an edge node or edge sensor. With the authorized access to the edge devices, the attacker may attempt to alter or modify a transaction record, commit a false transaction (i.e., fraud), perform a denial-of-service attack on other users through an artificial escalation of security level, or even send unauthenticated messages. To be more specific, we are interested to see if the internal adversary can compromise data in 51% edge devices powered by the proposed mechanism.

We make the following assumptions in regards to the proposed mechanism. The edge nodes have enough resources (e.g., storage, computational power, and network bandwidth), while edge sensors have the resource constraints. We also consider that edge sensors will work with the minimum resources (e.g., small memory or low battery powered). Besides, the

[1]In our architecture, *edge nodes* refer to the computing nodes that do not suffer from resource constraints, and are nearest to the *edge sensors*. DEAN is located between edge sensors and edge nodes.

hashing mechanism (e.g., SHA256) is cryptographically secure and computationally irreversible.

III. Proposed Approach

We have designed an energy-efficient consensus protocol, namely DEAN: Decentralized-Edge Autonomous Network. DEAN leverages the idea of in-memory blockchain [12], but with different approaches specially designed for edge computing. It exhibits two key technical novelties compared to the traditional edge computing model and the mainstream blockchain systems.

DEAN employs a unique persistence protocol tailored to support the limited storage capacity of edge computing infrastructure. One of the biggest challenges lies in difficulty in implementing a blockchain-like secured system in the edge ecosystem as the edge devices contain limited persistent storage. Our protocol overcomes this barrier in two ways. First, the protocol persists the entire blockchain in the edge nodes that usually consist of larger storage. Second, only recent blocks are queued in the edge sensors, which helps with in-memory computation by avoiding unnecessary communication.

DEAN is crafted with a two-stage consensus protocol to support the edge infrastructure backed by constrained resources (e.g., limited bandwidth, low computational power). First, the edge nodes take over the control of the block validation process to impose less (communication and computation) burden on the sensors. If at least 51% of edge nodes succeed with the validation, the block is then stored both in the edge nodes and the sensors. Second, if more than 50% of edge nodes fail, only then the sensors participate in the validation process to reach the maximum consensus but with a light-weight proof-of-work (i.e., PoW), as the sensors can communicate through the inter-connected edge nodes.

The benefit of the new protocol is two-fold. First, we can achieve blockchain-like fault-tolerance across the edge network, as it (i.e., DEAN) requires minimum support (e.g., limited memory and computational power) from the edge sensors. Hence, DEAN can successfully be applied to the present edge ecosystem. Second, the sensors can continue the block validation process with the available blocks in memory. They can always pull the new blocks from edge nodes in case of any failure (e.g., hardware failure or block unavailability). Hence DEAN reduces massive unnecessary communications.

IV. Preliminary Results

Test Bed. DEAN prototype is implemented with JAVA and is deployed to a Mac workstation with Intel Core-i7 4.2 GHz CPUs along with 32 GB 2400 MHz DDR4 memory. The network latency between edge and sensor nodes is set to 95 milliseconds; among the edge nodes, the latency is set to 150 milliseconds. The ratio between edge and sensor nodes is set to 1:3 by default, i.e., $\frac{|S|}{|M|} = 3$.

Workloads. The main workload under evaluation is comprised of 2.8 million queries, same as YCSB [13], which is similar to funds transfer between bank accounts. YCSB is widely adopted in measuring the performance of blockchain systems (e.g., BlockBench [14]).

Results. We evaluated the DEAN prototype from two perspectives: resilience and throughput. First, we measure the resilience of DEAN on 100 nodes, and experiments show that more than 60% nodes hold valid blockchains in all of the 15 executions. Note that, by definition, a consensus is reached by having more than 50% of nodes holding valid blockchains. We report the throughput of the DEAN-based blockchain system prototype and compare its performance to other leading blockchain systems: Ethereum [15], Parity [16] and Hyperledger [17]. We measured the performance of DEAN on up to 32 nodes (the ratio of edge and sensor nodes is 1:3) over five minutes, where each senor node issues up to 10,000 queries per second, and each block contains 14 transactions. DEAN outperforms the state-of-the-art and provides up to $88.8\times$, $16.6\times$, and $6.7\times$ more throughput compared to Parity, Ethereum, and Hyperledger, respectively.

Acknowledgement

This work is in part supported by the U.S. Department of Energy under contract number DE-SC0020455. This work is also supported by a Google Cloud award and an Amazon research award.

References

[1] B. Haynes, A. Mazumdar, A. Alaghi, M. Balazinska, L. Ceze, and A. Cheung, "Lightdb: A dbms for virtual reality video," *Proc. VLDB Endow.*, vol. 11, no. 10, pp. 1192–1205, Jun. 2018.

[2] O. Alrawi, C. Zuo *et al.*, "The betrayal at cloud city: an empirical analysis of cloud-based mobile backends," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 551–566.

[3] E. Ronen, A. Shamir *et al.*, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2017, pp. 195–212.

[4] K. Borgolte, T. Fiebig *et al.*, "Cloud strife: mitigating the security risks of domain-validated certificates," in *NDSS*, 2018.

[5] Hackers Remotely Kill a Jeep on the Highway, " https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway," Accessed 2019.

[6] J. Li, L. Sun *et al.*, "Significant permission identification for machine-learning-based android malware detection," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 3216–3225, 2018.

[7] Y. Lu, Q. Tang, and G. Wang, "Zebralancer: Private and anonymous crowdsourcing system atop open blockchain," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 853–865.

[8] C. Zuo, Z. Lin, and Y. Zhang, "Why does your data leak? uncovering the data leakage in cloud from mobile apps," in *Proc. IEEE Symposium on Security and Privacy*, 2019.

[9] Z. B. Celik, G. Tan, and P. D. McDaniel, "Iotguard: Dynamic enforcement of security and safety policy in commodity iot." in *NDSS*, 2019.

[10] W. Ding and H. Hu, "On the safety of iot device physical interaction control," in *CCS*. ACM, 2018, pp. 832–846.

[11] I. Bastys, M. Balliu, and A. Sabelfeld, "If this then what?: Controlling flows in iot apps," in *CCS*. ACM, 2018, pp. 1102–1119.

[12] A. Al-Mamun, T. Li, M. Sadoghi, and D. Zhao, "In-memory blockchain: Toward efficient and trustworthy data provenance for hpc systems," in *IEEE International Conference on Big Data (BigData)*, 2018.

[13] YCSB, " https://github.com/brianfrankcooper/YCSB/wiki/Core-Workloads," Accessed 2018.

[14] T. T. A. Dinh, J. Wang *et al.*, "Blockbench: A framework for analyzing private blockchains," in *SIGMOD*, 2017.

[15] Ethereum, " https://www.ethereum.org/," Accessed 2018.

[16] Parity, " https://ethcore.io/parity.html/," Accessed 2018.

[17] Hyperledger, " https://www.hyperledger.org/," Accessed 2018.

DEAN: A Blockchain-Inspired Consensus Protocol Enabling Trustworthy Edge Computing

Abdullah Al-Mamun[1], **Jun Dai**[2], **Xiaohua Xu**[3], **Mohammad Sadoghi**[4], **Haoting Shen**[1], **Dongfang Zhao**[1,4]

[1]University of Nevada, Reno [2]Cal State University, Sacramento [3]Kennesaw State University [4]UC Davis

Abstract

This work proposes a cooperative protocol, namely DEAN, across edge nodes and end devices to prevent data manipulation under resource constraints of limited storage, computing, and network capacity. Specifically, DEAN leverages an in-memory blockchain with an inexpensive proof-of-work consensus mechanism, effectively achieving low resource consumption on edge nodes and end devices. Preliminary results show that the system prototype exhibits high resilience to arbitrary failures: the percentile of trusty nodes is much higher than the required 50% in most cases. Performance-wise, DEAN-based blockchain implementation outperforms the state-of-the-art blockchain systems.

Motivation

1. Loosely coupled heterogeneous edge participants.
2. Vulnerable system infrastructure.
3. Extreme security mechanism can not be applied on the edge devices.

State-of-the-Art

- Permissioned blockchains: Hyperledger [1].
- Public blockchains: Ethereum [2], Parity [3].
- In-memory blockchains: IMB [4].
- Edge computing solutions: Leakscope [5], Iotguard [6], and Iotmon [7].

Open Challenges

1. Constrained resources:
   - Battery powered.
   - Limited persistent storage.
   - Limited network bandwidth.
2. Existing blockchain mechanisms are costly.
   - Extreme computational resources.
   - Large persistent storage.
   - Massive communication.

Proposed Approach

1. **Goal:** Efficiency and security within constrained resources.
2. Developed a blockchain-like mechanism.
3. Crafted for edge devices
   - Two stages of PoW :
     - First: Edge nodes.
     - Second: Edge sensors.
   - Work under constrained resources.
   - Support limited persistent space.
4. Ameliorates the storage pressure on the end devices.
   - Cost effective PoW (proof-of-work).
   - In-memory computation.
5. Implemented a blockchain simulator for edge computing.
6. Equipped with a full stack of blockchain system:
   - Decentralized in-memory protocols.
   - Large numbers of participating nodes.
   - SHA256: Security guarantee.
   - Distributed network queues.

Architecture

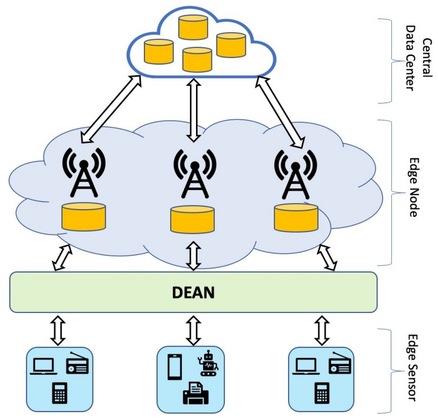
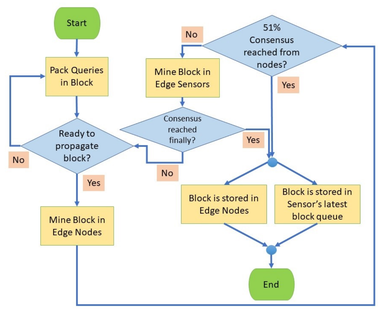


Figure 1: Proposed Four-Tier Edge Computing Architecture with DEAN.

DEAN's Workflow



Preliminary Results

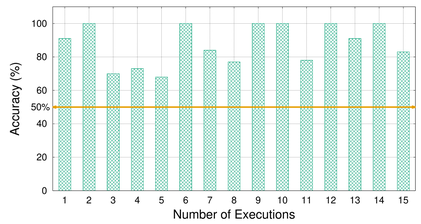


Figure 2: DEAN's Resilience. DEAN guarantees that more than 50% of nodes hold valid blockchain in practice.

- **Workload:** 2.8 million of random transactions (i.e., YCSB [8]).
- Scale: 100 nodes.
- Experiments: 15 times.
- 60% nodes hold valid blockchains.
- **Reminder:** A blockchain works correctly if 51% of nodes hold valid blockchains.
- Important phenomenon: 40% hold 100% correct blockchain.

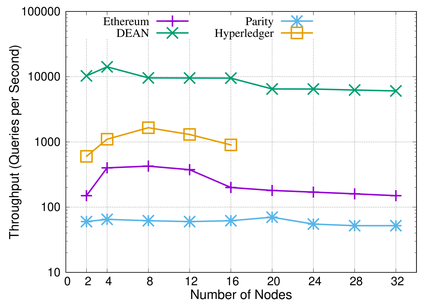


Figure 3: Throughput Comparison between DEAN and state-of-the-art blockchain systems. DEAN outperforms major blockchain systems with orders of magnitude higher throughput.

- Compared with Ethereum, Parity and Hyperledger.
- Scale: 32 nodes.
- Workload: 10,000 queries (i.e., transactions) by each sensor.
- Each block contains 14 transactions.
- DEAN provides up to 88.8×, 16.6× and 6.7× more throughput compared to Parity, Ethereum and Hyperledger, respectively.
- DEAN exhibits significantly higher throughput.
  - **DEAN Protocol guarantees:**
    - Effective but short puzzle-solving time.
    - No compromise with security.
    - Needs less persistent storage: in-memory computation.
    - Unique properties of edge computing.

Conclusion

- DEAN protocol serves high data fidelity under constrained resources.
- DEAN is partly enlightened by blockchains.
- Protocol safety is experimentally verified.
- Exhibits significant reliability and throughput on up to 100 nodes.

Future Work

1. Evaluate DEAN at larger scales.
2. Investigate the other aspects: latency, scalability, and staleness of blocks etc.

References

[1] Hyperledger. `https://www.hyperledger.org/`, Accessed 2018.

[2] Ethereum. `https://www.ethereum.org/`, Accessed 2018.

[3] Parity. `https://ethcore.io/parity.html/`, Accessed 2019.

[4] Abdullah Al-Mamun, Tonglin Li, Mohammad Sadoghi, and Dongfang Zhao. In-memory blockchain: Toward efficient and trustworthy data provenance for hpc systems. In *Proceedings of the 6th IEEE International Conference on Big Data (BigData)*, 2018.

[5] Chaoshun Zuo, Zhiqiang Lin, and Yinqian Zhang. Why does your data leak? uncovering the data leakage in cloud from mobile apps. In *Proc. IEEE Symposium on Security and Privacy*, 2019.

[6] Z Berkay Celik, Gang Tan, and Patrick D McDaniel. Iotguard: Dynamic enforcement of security and safety policy in commodity iot. In *NDSS*, 2019.

[7] Wenbo Ding and Hongxin Hu. On the safety of iot device physical interaction control. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 832–846. ACM, 2018.

[8] YCSB. `https://github.com/brianfrankcooper/YCSB/wiki/Core-Workloads`, Accessed 2019.

Contact Information

Email: dzhao@unr.edu