Towards a Blockchain and Fog-Based Proactive Data Distribution Framework for ICN

Somnath Mazumdar[1][0000−0002−1751−2569] and
Thomas Dreibholz[2][0000−0002−8759−5603]

[1] Department of Digitalization, Copenhagen Business School,
Solbjerg Plads 3, 2000 Frederiksberg, Denmark
sma.digi@cbs.dk
[2] Centre for Digital Engineering, Simula Metropolitan,
Pilestredet 52, 0167 Oslo, Norway
dreibh@simula.no

Abstract. Most of today's IP traffic is cloud traffic. Due to a vast, complex and non-transparent Internet infrastructure, securely accessing and delegating data is not a trivial task. Existing technologies of Information-Centric Networking (ICN) make content distribution and access easy while primarily relying on the existing cloud-based security features. The primary aim of ICN is to make data independent of its storage location and application. ICN builds upon traditional distributed computing, which means ICN platforms also can suffer from similar data security issues as distributed computing platforms. We present our ongoing work to develop a secure, proactive data distribution framework. The framework answers the research question, i.e., *How to extend online data protection with a secure data distribution model for the ICN platform?* Our framework adds a data protection *layer* over the content distribution network, using blockchain and relying on the fog to distribute the contents with low latency. Our framework is different from the existing works in multiple aspects, such as *i)* data are primarily distributed from the fog nodes, *ii)* blockchain is used to protect data and *iii)* blockchain allows statistical and other information sharing among stakeholders (such as content creators) following access rights. Sharing statistics about content distribution activity can bring transparency and trustworthiness among the stakeholders, including the subscribers, into the ICN platforms. We showed such a framework is possible by presenting initial performance results and our reflections while implementing it on a cloud/fog research testbed.

Keywords: Blockchain · Cloud · Data · Distribution · Fog · ICN · Security

1 Introduction

Data[3] distribution technologies, e.g. Information-Centric Networking (ICN), primarily use data caching and data replication to distribute the contents [3].

[3] We use the term content and data interchangeably in this paper.

Named Data Networking (NDN) [21] and Content-Centric Networking (CCN) are two popular ICN framework implementations. Using the existing IP ecosystem, ICN facilitates content access only by name. A scalable name-based routing and an efficient name-resolution process are required to support data-centric communication because it can improve network bandwidth utilization. ICN applies content-focused security rather than on the communication process [25]. The ICN framework generally suffers from multiple security attacks, such as unauthorized content access, denial-of-service and network-cache pollution [12]. In cache attacks, node caches are filled with unpopular content, decreasing throughput and increasing delay. As a result of such attacks, ICN infrastructure suffers from lower performance and higher energy consumption. ICN lacks data confidentiality and employs cryptography protocols to authenticate the name-to-content binding [24]. However, such cryptographic techniques can be computationally expensive, and name-to-content verification does not guarantee the quality and trustworthiness of the requested data. For efficient data distribution in ICN, in-network caching is introduced, allowing the content to be copied and distributed across [2] without strong authentication and authorization mechanism. Overall, it complicates ICN content access control management, but it is highly required for better performance.

Applying blockchain on top of ICN can reduce security-related issues. Blockchain can inherently support content tamper resistance and integrity checking, thanks to hashing. Data immutability is also supported by blockchain. It can further offer added security checks via the private blockchain platform. Blockchain is attack-resistant but not attack-proof and can bring performance benefits to ICN platforms. For instance, blockchain-based data distribution in NDN platforms is more efficient than IP networking [23]. In some cases, blockchain fits better to NDN than IP, offering better message delay [11]. Blockchain has found its way into secure media content delivery over the Internet [19] and is also used for ICN to trace malicious nodes thanks to its traceability feature [14].

In a traditional ICN network, only the content service providers (CSPs) manage everything. There are multiple cases where CSPs are non-transparent to content creators. It is arguable whether the current content distribution platforms are skewed towards the network owner's profit and non-transparent. However, the current content distribution platforms are out of the reach of content creators. Existing non-blockchain-based decentralized access control schemes for ICN-based content distribution and protection lack multi-level security and content access audits [1, 15, 18]. In this paper, we are presenting one blockchain and fog-based data distribution framework. It relies on blockchain for content protection and access delegation among the subscribers and other stakeholders, while fog can offer lower latency. Our framework differs from existing works in many ways. First, we rely on fog to enhance the content-delegation performance of latency-sensitive ICN applications. Second, we are using blockchain to protect the data and also incorporated a two-tier access control policy via the smart contract. The proposed two-tier access delegation model allows ICN stakeholders and subscribers to securely and legitimately access the data. We have implemented the framework using our cloud/fog research testbed. Further-

more, we have also reported our results on delegating the media files and the data distribution capacity of the testbed.

2 Related Work

Multiple works propose decentralized access control schemes to overcome content access problems without blockchain [18, 1, 15]. Mishra et al. offer an access control framework for ICN to guarantee trusted content to legitimate subscribers [18] and aim to increase content availability and quality of experience. Abdallah et al. propose a decentralized access control protocol for subscribers and nodes using the self-certifying naming scheme [1], while for the content provider, Li et al. developed an integrity verification process by distributing integrity verification tokens to authorized nodes [15].

Asaf et al., in their survey, show how blockchain is implemented in NDN and presents some challenges concerning blockchain over NDN [5]. Authors in [23] propose an NDN-based Ethereum client to enhance the data delivery with in-network caching and multicasting features of NDN. Lyu et al. propose a blockchain-based access control model to achieve hierarchical access for a content provider and present an access token mechanism [17]. It aims to find a balance between privacy and audit. In another work, blockchain is implemented over NDN to support transactions broadcasting by switching from the IP-based push protocol to NDN-based pull protocol [9]. Li et al. propose a blockchain-based tracing mechanism for content delivery in ICN [14], which stores the behaviours of ICN nodes to trace the malicious nodes. However, the authors have not completely clarified how much data blockchain and the cloud will store. A blockchain-based data life-cycle protection framework is proposed to offer a trusted ICN. The framework can exploit transactions and smart contracts after identifying the attack patterns and design requirements [16]. Conti et al. propose a blockchain-based authentication technique for mobility management in ICN [6]. Tan et al. propose an access control mechanism for ICN, where the contents are divided into multiple original blocks [22]. Next, the model applies the XOR-coding algorithm to encode blocks for recovering original contents later. Blockndn shows that a blockchain-based NDN is better for data broadcasting regarding message delay and traffic generation [11]. A name-based security mechanism to secure content distribution in ICN is also proposed to counter the key escrow problem by leveraging hierarchical identity-based encryption [7].

Finally, our work proposes a blockchain-based data/content distribution framework for a content provider. Fog will store frequently accessed content, and the rest will be in the cloud. Fog will reduce access latency, and the blockchain will store the metadata of the contents. The blockchain-based two-tier model supports a content access control policy. Here, one tier is dedicated to the subscriber, and the other allows the stakeholders (e.g., content creators) to view transactions related to their content. Such information can help stakeholders to understand the content's popularity and associated financial transactions.

3 Proposed Framework

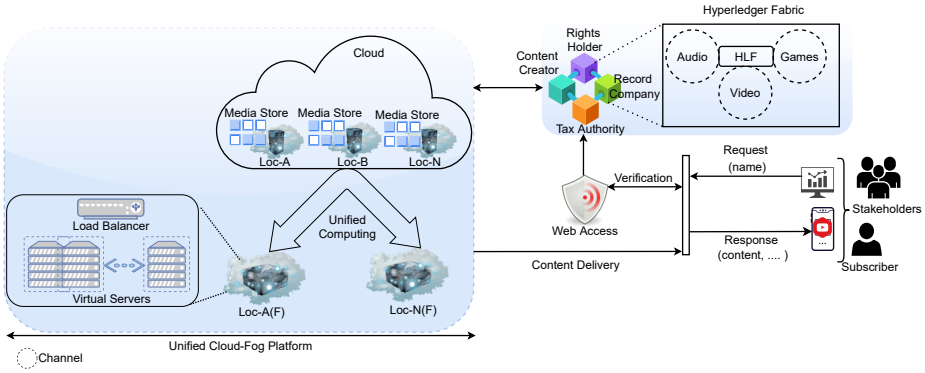

Fig. 1. Architecture of the proposed secure data/content distribution framework.

Figure 1 presents the proposed blockchain- and fog-based secure content distribution framework. It aims to complement the existing ICN by *i)* increasing the content's security (from the current security level) using blockchain and *ii)* improve the performance by relying on fog for a better subscriber experience, while cloud platforms are a good fit for applications that can tolerate delays up to 100 ms [20]. We have considered this framework from a CSP's perspective. CSPs will maintain the whole distribution platform. However, it will be tough for CSPs to manipulate the stored blockchain records without informing other stakeholders. Such a blockchain-based ICN solution adds content protection and access control while delegating content to the subscribers/stakeholders. Blockchain can make the ICN platform more transparent. For instance, stakeholders can access content-related details, such as content access statistics, content popularity, revenue from content, and others. It is worth noting that customizing the smart contract can also allow access to more detailed information. The current framework considers six stakeholders, but more can be added easily. The current list of stakeholders is as follows: *i)* CSP, *ii)* Subscribers, *iii)* Content Creator(s), *iv)* Right Holder(s), *v)* Record Companies or Labels, *vi)* Public authority for tax and copyright protection (and violation). Adding more stakeholders can make it more transparent and a more acceptable solution.

3.1 Framework Overview

The framework (refer to Figure 1) has two primary components. They are *i)* cloud/fog platform to host content (off-chain storage), and *ii)* blockchain to provide data protection and access delegation. We can see from Figure 1 that after successfully checking subscribers' credentials (by the blockchain), their request is routed based on the designated access tiers. We have considered pro-

tected visibility as tier one[4] and private visibility as tier zero[5]. The level of content visibility as per tiers should be decided before the network implementation. The subscribers belong to tier one, and stakeholders are associated with tier zero. A subscriber requests content (e.g. a movie) by sending the content name. Next, a relevant REpresentational State Transfer (REST) API call will be generated to process the viewer's request. The related smart contract will be invoked, and after successful access rights verification, another API call will be made to initiate the media file transfer via the nearby fog nodes. Users can have only age-appropriate content access (thanks to a tier-based access control policy), while inappropriate content related to explicit content, violence, and other inappropriate documentaries is filtered out via the rules embedded into the smart contracts. Such content delegation based on the access control policy feature makes our framework *proactive*. Generally, content fragmentation is done at the transport layer. From the content delivery request side, ICN supports *Name packets* for request, and *Data packets* for the response. The ICN uses protocol data units to distribute the contents larger than standard maximum transmission units. Data transmission can be based on a pull protocol (such as HTTP Live Streaming) instead of widely used push protocols to achieve higher efficiency in the application layer. Content data authenticity and encryption are automatically performed (at an off-chain storage level) by the blockchain using the hashing and digital signature. The proposed platform is private, which means all the network subscribers, including the stakeholders, are verified before conducting any network activity. Thus, content added to the framework is always trusted. After adding metadata to the content, manipulating content (or viewing manipulation) is tough. We have used the Hyperledger Fabric (HLF) blockchain platform for the implementation [4]. HLF applies a more traditional byzantine fault-tolerant consensus mechanism, which does not require mining and is one of the few platforms to develop enterprise-level applications. HLF also offers channels which are a secure form of communication. Each channel can be dedicated per content type (refer to the top right of Figure 1). Finally, primary contents are stored in the cloud/fog platform, and the metadata is stored in the blockchain, which helps to preserve the content's integrity.

3.2 Framework Data Flow

Figure 2 shows how data flows inside the framework. It is worth mentioning that such a seamless information flow can improve the service optimization of the platform. All important events are recorded on the blockchain. The flow starts when movie 'X' is listed on the platform after buying the media rights by a CSP. The file of the movie 'X' will be stored in the cloud storage, but the movie's metadata (including the storage location) will be stored in the blockchain. The storage location is also added to the metadata and later hashed before adding to the blockchain to ensure no changes can be made to the media content. After the movie is listed on the network, subscribers can watch the movie. Later,

[4] allows access services based on the subscribed plan.
[5] allows stakeholders to access the blockchain.

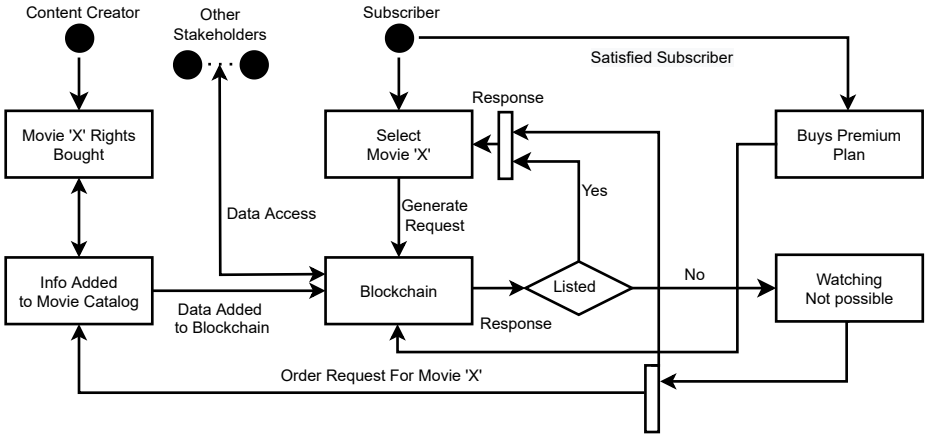

Fig. 2. Seamless data flow inside the framework.

media usage metrics can be accessible to the stakeholders, including the original content creator. If a subscriber subscribes to a premium plan, the stakeholders can also see such information. Based on the implementation, stakeholders can see how much revenue is generated using the advertisement and subscription plans. Finally, if any movie is not listed (rare at this time), the framework can also inform the CSP to include it.

3.3 Security-Related Advantages

ICN wraps all network functionalities around the content name by supporting the name resolution system. It builds upon traditional distributed computing, which means ICN also suffers from similar security issues as distributed computing platforms. Here, we will qualitatively discuss how blockchain offers better security than legacy ICN platforms following the STRIDE model [13]. Spoofing-related events result from low physical security measures of nodes, but taking down the whole network using one blockchain node is technically not possible. Next, data tampering and repudiation are very hard to achieve, thanks to the employed hashing and digital signature of data blocks. The hash connects data blocks. HLF uses the SHA-256 hashing algorithm and the elliptic curve digital signature algorithm as the digital signature to counter such issues. Information disclosure leads to user data compromise, which is hard because of employed blockchain-based access control. Denial-of-service forces the ICN platform to be temporarily unavailable. In such cases, an attacker needs enormous computing power relative to the blockchain-based ICN network size. Finally, elevation of privilege cannot be done easily on the private platform because a network administrator verifies all network users before delegating access rights to them. So, overall, blockchain brings advantages primarily related to content security compared to non-blockchain-based ICN platforms. Data integrity is maintained by

employing a hashing algorithm, and a digital signature is used to authenticate the subscribers.

3.4 Block Structure

```
{
"content_data": {
      "content_name": "file_name",
      "content_type": "video",
      "content_id": "2ede927-..-8a26a2665aea",
      "content_owned_by": "content owner/copyright owner name",
      "content_location": "list of caching locations/storage locations/urls",
      "content_manifest": " list of connected payloads",
      "content_length": "value",
      "content_price": "current price",
      "content_misc_name": "other partial content names",
      "content_meta_data": {
            "content_rating": "general/parental guidance/mature/...",
            "content_genre": "genre name",
            "content_timestamp": "adding to blockchain",
            "content_added_by": "content service provider",
            "content_format": "MP4/MOV/AVCHD"
            }
      }
}
```

Fig. 3. Representation of current block structure for managing a video/movie file.

Blockchain is a linear-linked-list representation of a distributed ledger and is primarily a collection of distributed transactions. Here, a transaction represents one named content accessed by viewers, while a data block holds n transactions. n is implementation-dependent, but it should not be too large because larger block sizes reduce the scalability of the network. Figure 3 shows our customized block structure to wrap the content's information (work in progress). Such customization speeds up video content processing (access and delegation). Our current version of the block structure holds both content-specific data and metadata. `content_id` is the message digest after applying an SHA-256 function on the content's primary name and the content itself. Such an approach ensures that no modification can go unnoticed after adding the content to the blockchain (i.e. supporting data immutability). One of the problems with the named content in ICNs is that the content might have multiple partial names. The name might be partial when a viewer requests the content via its name. In that case, `content_misc_name` will hold a list of possible words that can help to look up the content faster. `content_price` is also a piece of important information for the content creator. Generally, the CSPs use dynamic pricing models so that price manipulation can be visible to the relevant stakeholders. It is worth noting that the framework does not support any cryptocurrency (or tokens). Similar to video content, it is possible to create other blocks for audio, games and other

content. We keep the meta information in data blocks, while primary content (such as video or audio files) is stored in the cloud/fog.

4 Performance Results

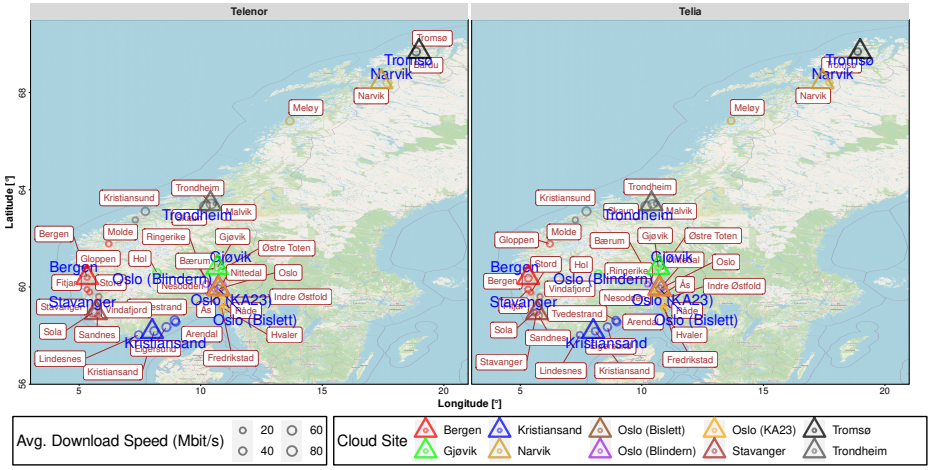

Fig. 4. Fog nodes and their cloud mappings with their average downloading speed.

To showcase the feasibility of our framework, we created the setup shown in Figure 4, which is an extended part of our cloud/fog research testbed distributed over Norway [8]. The cloud sites are marked with triangles, and the fog nodes are shown as circles. Each fog node is connected using 4G modems relying on broadband connections. These connections are from two Internet service providers (ISPs), i.e., Telenor and Telia. The left-hand part of Figure 4 presents the Telenor-based layout, while the right-hand part shows the Telia-based layout. The circle size corresponds to the average download speed. To show the fog performance, we had chosen three typical media sizes[6]: 1 GiB for standard definition (SD), 3 GiB for high definition (HD), and 7 GiB for ultra-high definition (4K). Table 1 presents the resulting average download time for each media file size per fog site location (municipality-level aggregation) over each of the two ISPs (if available) for municipalities with a population of at least 10,000. Furthermore, the table contains the mapping to the geographically nearest cloud.

As shown in Table 1, streaming the 4K media to Telenor-backed fog nodes took just more than 14:28 min (as best case, for Telenor in Trondheim) and a maximum of 167 min (worst case, for Telenor in Malvik), while the other ISP can stream 4K video in 19:17 min (best case, for Telia in Trondheim) to almost 167 min (worst case, for Telenor in Malvik). Theoretically, our cloud setup (all

[6] `https://help.netflix.com/en/node/87/us` (accessed Oct. 20, 2022).

Table 1. Content downloading time (minutes:seconds) from fog nodes (only for locations with population of at least 10,000).

Cloud Loc.	Fog Loc.	Telenor			Telia		
		SD	HD	4K	SD	HD	4K
Bergen	Bergen	11:34	34:44	81:02	5:02	15:07	35:17
	Stord	11:33	34:40	80:54	12:44	38:12	89:09
Gjøvik	Gjøvik	6:16	18:50	43:57	8:50	26:30	61:50
	Østre Toten	13:15	39:47	92:50	3:18	9:54	23:07
Kristiansand	Arendal	3:52	11:38	27:09	4:38	13:54	32:26
	Eigersund	2:50	8:30	19:51	3:32	10:36	24:44
	Kristiansand	2:59	8:58	20:55	4:40	14:01	32:43
	Lindesnes	3:39	10:59	25:39	6:39	19:58	46:35
Narvik	Narvik	2:51	8:34	20:00	5:51	17:34	41:01
Oslo (Bislett)	Oslo	3:48	11:24	26:38	4:21	13:03	30:29
Oslo (Blindern)	Bærum	11:48	35:25	82:40	–	–	–
	Nittedal	2:10	6:32	15:15	2:45	8:16	19:17
	Ringerike	6:00	18:01	42:04	12:48	38:25	89:39
Oslo (KA23)	Ås	5:48	17:24	40:36	6:00	18:01	42:04
	Bærum	–	–	–	9:00	27:01	63:04
	Fredrikstad	9:11	27:33	64:17	10:39	31:59	74:38
	Indre Østfold	5:44	17:12	40:09	6:07	18:22	42:51
	Nesodden	14:36	43:48	102:14	8:11	24:35	57:23
Stavanger	Sandnes	12:59	38:59	90:58	5:03	15:10	35:24
	Sola	2:30	7:32	17:36	8:33	25:39	59:53
	Stavanger	3:00	9:01	21:03	5:46	17:18	40:22
Tromsø	Tromsø	3:19	9:58	23:17	5:20	16:01	37:22
Trondheim	Kristiansund	3:38	10:56	25:31	2:47	8:21	19:30
	Malvik	23:50	71:32	166:56	13:10	39:30	92:10
	Molde	9:34	28:44	67:04	9:04	27:13	63:31
	Trondheim	2:04	6:12	14:28	2:47	8:21	19:30

Table 2. Content downloading time (minutes:seconds) from public cloud providers.

Cloud	Region	Avg. Download Speed (Mbit/s)	SD	HD	4K
Amazon Cloud	Stockholm	100.95	1:27	4:22	10:11
Microsoft Azure	Norway East	113.55	1:17	3:53	9:04
Google Cloud	Finland	102.62	1:25	4:17	10:01

sites; not shown in the table) can deliver the same 4K file in 61 s (best case) to a maximum of 10 min (worst case). The actual download time significantly varies in rural areas, leading to increased download times. Caching and more intelligent content distribution can improve the network performance (e.g. by avoiding unnecessary transfers during peak hours, trying to utilise non-peak hours, and using nearby download locations). We also have reported the content downloading time from public cloud service providers in Table 2. These values reflect the CDN service network performance offered by the three popular cloud service providers. It is worth noting that they do not offer any fog-based services. For all three video file types, the Trondheim facility (Telenor as ISP) is the best among all our testbed facilities compared to the Microsoft Azure CDN service (Norway).

Table 3. Average network latency of compute services of three public cloud service providers and the testbed.

Cloud	Region	Avg. Latency (ms)
Amazon Cloud	Stockholm	32
Microsoft Azure	Norway East	41
Google Cloud	Finland	40
NorNet Cloud	Norway	27
NorNet Fog	Norway	59

Table 3 compares the average network latency (round trip times using IPv4 packets) among all platforms and the cloud/fog testbed. Our fog testbed units are slower than the cloud because the fog nodes are connected via 4G mobile broadband. We can see that the NorNet Cloud has an average latency of 27 ms for a 4G-based connection and 12.75 ms for a fibre-based link (not reported in the table). It is worth noting that commercial infrastructures are highly resourceful and professionally maintained compared to a research testbed. Our aim was never to beat the commercial providers but to show that our framework has been implemented on a realistic testbed, and the comparison proves it. We can also infer that adding fog by the commercial facility will surely improve the latency of content delegation, and adding blockchain will distribute content securely.

4.1 Lesson Learned

To offer a better viewing experience, the Open Connect program[7] from Netflix aims to develop a better content caching infrastructure using ISPs' resources. Here, we aim to build a framework to offer better content security and improved cache coordination with effective network storage management. While working on the performance data, we also started looking into *How to optimize storage cost by intelligent fog-level content caching?* In such a scenario, machine learning (ML) can lower content access latency and storage costs by predicting

[7] `https://openconnect.netflix.com/en/` (accessed Oct. 20, 2022)

content popularity. ML is already used for predicting popular video contents [10]. Currently, an ML module is being developed using user-ID (hashed value/anonymous for privacy), content viewing patterns (such as genre, content type) and other information (model-dependent) related features to improve the quality of experience.

5 Conclusion and Future Work

ICN aims to offer location-independent data access via improved caching and replication. We propose a blockchain-based content distribution framework to provide better content security and make the distribution process transparent to the relevant stakeholders. We do not use blockchain for content storage but to protect it. All content-related metadata in hashed format is stored in the blockchain. We reported performance results related to our content distribution while handling video files. We aim to complete the benchmarking of our platform before implementing ML for smart caching of popular content as future work. To the best of our knowledge, there is no prototype similar to ours which uses blockchain to secure ICN and is implemented using a cloud/fog testbed.

References

1. AbdAllah, E.G., Zulkernine, M., Hassanein, H.S.: DACPI: A Decentralized Access Control Protocol for Information-Centric Networking. In: IEEE International Conference on Communications. pp. 1–6. IEEE (2016)
2. Abdullahi, I., Arif, S., Hassan, S.: Survey on Caching Approaches in Information-Centric Networking. Journal of Network and Computer Applications **56**, 48–59 (2015)
3. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., Ohlman, B.: A Survey of Information-Centric Networking. IEEE Communications Magazine **50**(7), 26–36 (2012)
4. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A.D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J.: Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: 13th EuroSys Conference. EuroSys '18, Association for Computing Machinery (2018)
5. Asaf, K., Rehman, R.A., Kim, B.S.: Blockchain Technology in Named Data Networks: A Detailed Survey. Journal of Network and Computer Applications **171**, 1–15 (2020)
6. Conti, M., Hassan, M., Lal, C.: BlockAuth: BlockChain-based Distributed Producer Authentication in ICN. Computer Networks **164**, 1–15 (2019)
7. Fotiou, N., Polyzos, G.C.: Decentralized Name-based Security for Content Distribution using Blockchains. In: IEEE Conference on Computer Communications Workshops. pp. 415–420. IEEE (2016)
8. Gran, E.G., Dreibholz, T., Kvalbein, A.: NorNet Core – A Multi-Homed Research Testbed. Computer Networks **61**, 75–87 (2014)
9. Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., Zhang, Y.: Enabling Blockchain Applications over Named Data Networking. In: International Conference on Communications. pp. 1–6. IEEE (2019)

10. Jeon, H., Seo, W., Park, E., Choi, S.: Hybrid Machine Learning Approach for Popularity Prediction of Newly Released Contents of Online Video Streaming Services. Technological Forecasting and Social Change **161**, 1–17 (2020)
11. Jin, T., Zhang, X., Liu, Y., Lei, K.: Blockndn: A Bitcoin Blockchain Decentralized System over Named Data Networking. In: International Conference on Ubiquitous and Future Networks. pp. 75–80. IEEE (2017)
12. Kim, D., Bi, J., Vasilakos, A.V., Yeom, I.: Security of Cached Content in NDN. IEEE Transactions on Information Forensics and Security **12**(12), 2933–2944 (2017)
13. Kohnfelder, L., Garg, P.: The Threats to Our Products. Microsoft Interface, Microsoft Corporation **33** (1999)
14. Li, H., Wang, K., Miyazaki, T., Xu, C., Guo, S., Sun, Y.: Trust-enhanced Content Delivery in Blockchain-based Information-Centric Networking. IEEE Network **33**(5), 183–189 (2019)
15. Li, Q., Zhang, X., Zheng, Q., Sandhu, R., Fu, X.: LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking. IEEE Transactions on Information Forensics and Security **10**(2), 308–320 (2014)
16. Li, R., Asaeda, H.: A Blockchain-based Data Life-cycle Protection Framework for Information-Centric Networks. IEEE Communications Magazine **57**(6), 20–25 (2019)
17. Lyu, Q., Qi, Y., Zhang, X., Liu, H., Wang, Q., Zheng, N.: SBAC: A Secure Blockchain-based Access Control Framework for Information-Centric Networking. Journal of Network and Computer Applications **149**, 1–17 (2020)
18. Misra, S., Tourani, R., Natividad, F., Mick, T., Majd, N.E., Huang, H.: AccConF: An Access Control Framework for Leveraging In-Network Cached Data in the ICN-enabled Wireless Edge. IEEE transactions on Dependable and Secure Computing **16**(1), 5–17 (2017)
19. Nazarian, A., Arana, M., Prestegard, D.L.: Blockchain Configuration for Secure Content Delivery. Patents (2021)
20. Pelle, I., Czentye, J., Dóka, J., Sonkoly, B.: Towards Latency Sensitive Cloud Native Applications: A Performance Study on AWS. In: IEEE 12th International Conference on Cloud Computing. pp. 272–280. IEEE (2019)
21. Saxena, D., Raychoudhury, V., Suri, N., Becker, C., Cao, J.: Named Data Networking: A Survey. Computer Science Review **19**, 15–55 (2016)
22. Tan, X., Huang, C., Ji, L.: Access Control Scheme based on Combination of Blockchain and XOR-coding for ICN. In: 5th International Conference on Cyber Security and Cloud Computing/4th International Conference on Edge Computing and Scalable Cloud. pp. 160–165. IEEE (2018)
23. Thai, Q.T., Ko, N., Byun, S.H., Kim, S.M.: Design and Implementation of NDN-based Ethereum Blockchain. Journal of Network and Computer Applications **200**, 1–18 (2022)
24. Wissingh, B., Wood, C.A., Afanasyev, A., Zhang, L., Oran, D., Tschudin, C.: Information-Centric Networking (ICN): Content-Centric Networking (CCNx) and Named Data Networking (NDN) Terminology. Informational RFC 8793, IETF (Jun 2020)
25. Zhang, Z., Yu, Y., Zhang, H., Newberry, E., Mastorakis, S., Li, Y., Afanasyev, A., Zhang, L.: An Overview of Security Support in Named Data Networking. IEEE Communications Magazine **56**(11), 62–68 (2018)