IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

An Information Centric Network for Distributed Registery with Content Unique Identifier (DID) and Verifiable Credentials

Prof. Aravinda Thejas Chandra[1], Chandan R[2], B Kiran[3], Hemanth Kumar N[4]
Associate Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4]
S. J. C. Institute of Technology, Chickballapur, Karnataka, India

Abstract: *Decentralised Identifiers (DIDs), a new self-manageable method of authentication that is currently being standardised by the World Wide Web Consortium (W3C), are new standards for Content Unique Identifiers. Verifiable credentials (VCs), another ongoing standardisation (by the same W3C working group) that permits private and secure proofs of attribute ownership, are closely related to DIDs. Both of these methods rely on a central immutable decentralised registry (such as a blockchain or peer-to-peer network) where crucial meta-data is stored. Using the newly developing paradigm of Information Centric Networking (ICN), we design, construct, and evaluate a secure DID/VC registry service. The "search by name" feature of ICN, together with a secure protocol, are combined with the decentralised nature and our goal is to achieve technique for keeping in sync copies of an object at several locations. Our design has little network cost and provides quick lookup speeds because to ICN's built-in multicast and caching functionality.*

Keywords: DID registry, publish subscribe, privacy, and identity management

I. INTRODUCTION

Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), two closely linked authentication and authorization standards, are currently being specified in response to the requirement for decentralisation and privacy protection. [1] A DID can be thought of from a high level as a random public string that is mapped to some public data kept in a "registry" as well as to some private data safely kept by the DID "owner." The latter private data is utilised to create ownership proofs, which are examined using the registry's information. Similar to this, a VC consists of some "claims" given to the "holder" of the VC. A VC is linked to certain publicly available information, which is once more kept in the registry, as well as some personally identifiable information that is kept by the holder. [1] A VC holder, like DID holders, uses the private information to give claim ownership evidence, which are confirmed using the registry's publicly available data.

The main benefit of these identification and authorisation techniques is that they strengthen self-sovereignty, which has a number of essential advantages. Persistence: Even if the underlying cryptographic keys are changed, [1] a DID may still remain unchangeable. Portability: A DID or VC's information and services are portable. DIDs and VCs can be widely used, even across silos, because to interoperability. Access: DID owners are able to change their own identity-related information without the assistance of outside parties. Owners of DIDs and holders of VCs must give their permission for other parties to utilise their personal information. Only the information required to complete a task is released in minimal disclosure.

The DID/VC registry, hereafter referred to as the registry, is a crucial part of these systems. To ensure that registry records are appropriately secured without introducing lock-in circumstances, a registry should be constructed in a secure and effective manner. In this research, we create such a registry using a novel networking architecture called Information-Centric Networking (ICN). Our system takes into account a single network (for example, the network of an ISP) that has edge-nodes that are "ICN-enabled"; users communicate with these edge-nodes via HTTP, and these edge-nodes translate HTTP requests into the proper ICN flows. We offer a service to within the ICN network We take

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

advantage of the multicast and caching aspects of ICN and provide a quick and secure solution for maintaining immutable, append-only records associated with a DID/VC. Finally, this paper makes the following contributions:
Using standard ICN methods, we build a register that enables concurrent use of the internal ICN network for various goals.
We design a record-management system that requires as little faith from ICN nodes as possible. The user is able to select the edge-node of their choosing and to change their mind later. We provide guidelines for integrating available DID/VC tools with our solution.
This essay's remaining sections are organized as follows. We examine similar research in this area and provide background information on DIDs, VCs, and ICN. We explain our strategy. Then, we outline how we'll put our solution into practise.

II. RELATED WORK

The following system is taken into account before creating our application.:

1.Title: A Primer for Decentralized Identifiers.

Abstract: A new kind of identifier known as a Decentralised Identifier (DID) is cryptographically verifiable, globally unique, and resolvable with high availability. DIDs are usually connected to service endpoints and cryptographic resources like public keys for creating secure communication channels. DIDs are beneficial for any application that needs self-administered, cryptographically verifiable identifiers, including identifiers for Internet of Things scenarios, organisational identifiers, and personal identifiers. Decentralised Identifiers are used extensively in current commercial deployments of W3C Verifiable Credentials, for instance, to identify persons, organisations, and things and to uphold a number of security and privacy-protecting assurances. Introduction to the idea of decentralised identifiers is provided in this document.

2. Title: Edge- ICN and application to the Internet of Things.

Abstract: Although Information-Centric Networking (ICN) research is thriving, widespread adoption of ICN seems to be an elusive objective. We suggest Edge-ICN in this study as a cutting-edge method for installing ICN in a single, sizable network, such as the network of an Internet Service Provider. Even though Edge-ICN only needs an SDN-based network that supports the OpenFlow protocol and ICN-aware nodes only at the network's edges, it still provides the same advantages as a clean network. ICN architecture, but without the difficulties of deployment. All current applications may run without any problems because to the transparent forwarding of legacy traffic over the Edge-ICN nodes, which also provides important benefits to applications including native support for scalable anycast, multicast, and multi-source forwarding. In this context, we demonstrate how the proposed network edge capability can in particular help CoAP-based IoT applications. Our research demonstrates that Edge-ICN allows IoT applications to be built on anycast, multicast, and multi-source forwarding primitives without causing, on average, the same control plane overhead for name resolution as a centralized method.

3. Title: A brief introduction to NDN dataset synchronization (NDN Sync).

Abstract: State Vector Sync (SVS), a sync mechanism for Named Data Networking (NDN), is briefly introduced in this report. Sync protocols synchronize the data names of a shared dataset among participants in order to facilitate distributed applications. In this study, we define the SVS protocol and its functions to enable experimentation with the SVS library implementations and explain how the SVS design is affected by the lessons learned from the designs of earlier sync protocols.

4. Title: A network in a laptop: Rapid prototyping for software-define networks.

Abstract: Mininet is a technology for quickly developing massive networks using just one laptop's limited resources. It can expand to hundreds of nodes thanks to the lightweight method of employing OS-level virtualization features, such as processes and network namespaces. The results of our early implementation indicate that real-time running, poking, and debugging constitutes a qualitative shift in workflow. We provide case examples that illustrate our arguments, drawn from more than 100 users at 18 different universities who have created software-defined networks (SDN). Since

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

anyone with a PC can download, run, evaluate, explore, tweak, and build upon self-contained SDN prototypes, we believe that Mininet's greatest value will be in supporting collaborative network research.

III. METHODOLOGY USED

The illustration below shows how we create a registry using conventional ICN techniques, allowing us to utilise the internal ICN network concurrently for various uses. We create a record-keeping system that calls for ICN nodes must have a minimum of trust. Users can interact with any edge-node of their choosing, and we can change that option at a later time. whenever it was first possible to retrieve a DID document using the DID resolver. It had just finished sending a related registrar an HTTP request. The ICN network was sending documents to the registrar. was responding to the resolver, and the procedure is implemented without changing any of the libraries that are used.

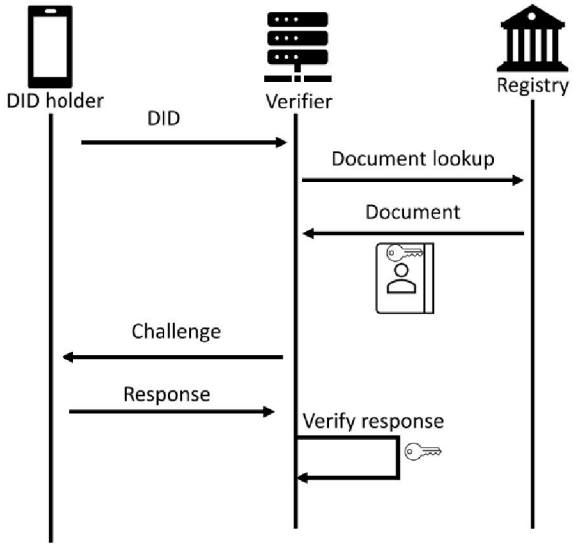

Figure 1: The Implementation of the read API call.

Decentralized Identifiers and Verifiable Credentials: A Decentralised Identifier (DID) [2] is a brand-new class of Uniform Resource Name (URN)-encoded globally unique identifier. A DID is connected to a DID Document, which includes details about the DID, such as public keys, authentication procedures, and service endpoints that are accessible. Listing shows a simple DID document that has been JSON-LD [3] encoded. The DID 'id is the topic of this example. When a public key is defined, the key definition contains the key's id, type, and actual value. It implies that the DID holder can be "authenticated" using the defined key. It also includes a proof of the document in Linked Data proof [4] that can be checked using the specified key.

Information Centric Networking: The scientific community and the industry are paying more attention to the growing paradigm of information-centric networking. Although there are noticeable differences between the main ICN architectures. [7] The content ID is an identifier that is used to uniquely identify each item of content in ICN architectures. Furthermore, the publish-subscribe paradigm is used by the majority of ICN architectures content producers advertise content IDs that they control, and content subscribers "subscribe" for a certain content ID. The interested subscribers are eventually "forwarded" the content pieces. Multicast and caching are facilitated by focusing all networking operations on content ID. The latter is typically accomplished by combining subscriptions for the same item and concurrently sending it to all subscribers via a multicast delivery tree.

Distributed DID registry is the suggested remedy. Using an ICN architecture that is explained in the following section, all registrars are connected to one another. Using HTTP, users communicate with the registrar(s) of their choice. As a result, each registrar has two interfaces: an internal ICN interface for communicating with the ICN network and an external HTTP interface used by users. Figure 2 depicts a condensed overview of the proposed system. The core

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

component of our solution is an SDN-based ICN network that connects registrars, as this image illustrates. A few data structures relating to ICN state and DID documents are maintained by registrars (covered in more detail in the following subsections).

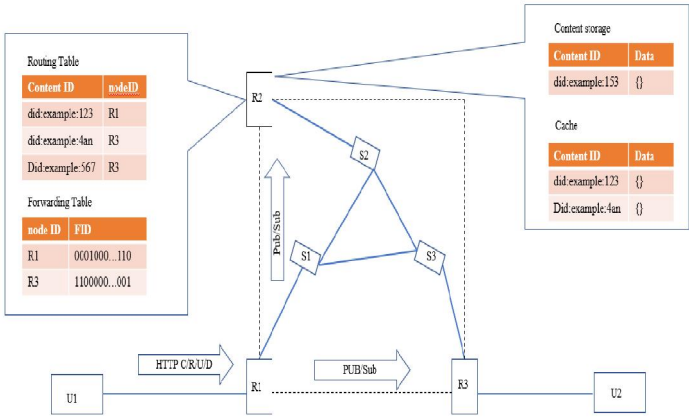

Figure 2: The entities of the proposed system and their main components. User1 and User2 are user terminals, Registry1, Registry2 and Registry3 are registrars. SDN1, SDN2 and SDN3 are SDN switches.

The Core ICN-Based Architecture: We mix the Edge-ICN design from with the hybrid IP-ICN [2] design for our registry. Our design presupposes an SDN core for connecting the edge nodes. Bloom filters are used to implement packet forwarding between edge nodes through the core network using the methodology outlined in. The path that a packet should take is encoded in a Bloom filter, known as the Bloom filter, and each link in the core network is identified by a bit array called the link identifier. Forwarding Identifier (FId), constructed by O Ring the identifiers of the links that compose that path.

DID and DID Document Data Model: A user generates a public-private key pair to produce a DID; the DID is the hash of the public key. The DID document is then initially created by him. In that initial version, the public key, an authentication strategy based on it, and a proof produced by the private key are all included. The public key used in the authentication technique of the xth version of a DID document is referred to as Pub x throughout the remaining sections of the article, and the associated private key is referred to as Prv x. Therefore, in a more formal sense, DID is defined as "prefix0 + hash (Pub0)," where prefix is a string unique to the DID technology that is being used, and the initial DID document also contains Pub0 and a proof that was generated. with Prv0. A chain of document versions is created by including Pub m and a proof produced using Prvm1 in every successive version m of the DID document. Using Pubm1, the proof contained in the m th version of the DID document (where m > 0) is validated.

DID Registry Operations: In our network, edge-nodes might serve as registrars. Both storing and retrieving DID documents fall under the purview of each registrant. Each registrant provides the Create, Read, Update, and Deactivate document management techniques for this purpose, which can be accessible via an HTTP REST API. Users rely on particular registrars to keep their DID papers up to date and/or to retrieve the DID records of others. To guard against Sybil attacks, registrars implement a throttling mechanism for the Create method. On the other hand, any number of DID documents may be read by a user. For both reading and writing and controlling his own papers, a user may use numerous registrars as a backup.

CACHE Maintenance: Registrars can cache the documents they obtain from the ICN network, as was already mentioned. The cached entries must constantly be current. Because of this, each DID owner stipulates in the accompanying DID document how long a DID can spend in a cache. Registrars can subscribe using the channel mode for DID/current to maintain cached entries current and avoid cache evictions. With this subscription, customers will

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

periodically receive the sequence number of the most recent DID document version. This serves two purposes: first, it is used to identify any missed document versions, and second, it is used to update the related entry's cache expiration time.

Security Analysis: Our system only relies on registrars to react to subscription requests and advertisement requests when it comes to DID document management. In fact, registrars (or any other business) are not permitted to produce a new version of a DID record, provided that the user's private keys are safeguarded. The level of confidence required from registrars is higher when it comes to reading DID documents since they are trusted to confirm the chain of DID document versions and provide the most recent version. It's a trade-off between convenience and security. The entire chain can be handed off to the user if registrars are not trusted to carry out this verification. But in that case, user applications must be adjusted appropriately.

IV. IMPLEMENTATION

Request handling: It performance specific actions, such as checking the content in cache or route table, subscribing to content, advertising the request, updating the content, or deleting the content.

Cache table handling: It check the content is available in the cache table and sends it to the user if it is available. If the content is not available in the cache table, the code updates the cache table when new content is created or updated.

Route table handling: The content is available in route table and subscribes to it available. If the content is not available in the route table, the code advertises the request and subscribes to the content if it is advertised.

Pseudocode:

```
Given: Route Table RT, Cache Table CT
Obtain: Null
Start
 Read RT &CT
While True
 Receive Request R from user
 if R. Type is Read then
 if content in cache then
 send content to user
 elseif content in Route Table then
 subscribe content
 if published then
 send no user
 else
 announce content Not found
 end
 else
 Advertise the request
 if content Advertised then
 subscribe content
 if published then
 send content to user.
 else
 Announce content is found.
 end.
 else
 Announce content Not found.
 end
 end
```

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

elseif R. Type is create then
if content is in cache then
update content.
elseif content is in Route table then
send update to Router
if content published then
update content
verify key, signature, credentials.
else
Announce content Not found.
end.
elseif content not Advertised then
Announce content Not found.
end
elseif R. Type is update then
if content is in cache then
verify key, signature
update the content
else if content is in Route table then
verify key, signature.
subsite content.
update content.
else
Announce content Not Available.
end
elseif
R. Type is update then
if content in cache the
check credential & delete
elseif content in Route table then
subscribe content & delete.
end
end
end
stop

Content verification: The code verifies the key, signature, and credentials of the content when it is created or updated.

Error handling: The code announces "content not found" if the content is not available in cache table, route table, or advertised**.**

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

V. RESULTS

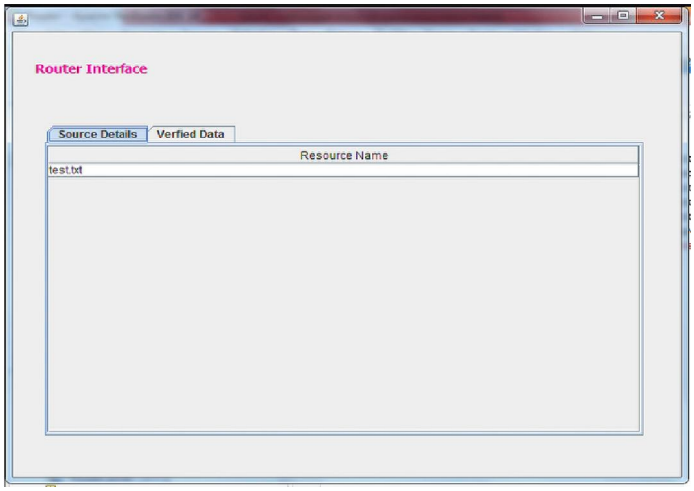

Figure 3: File in the Router DID.

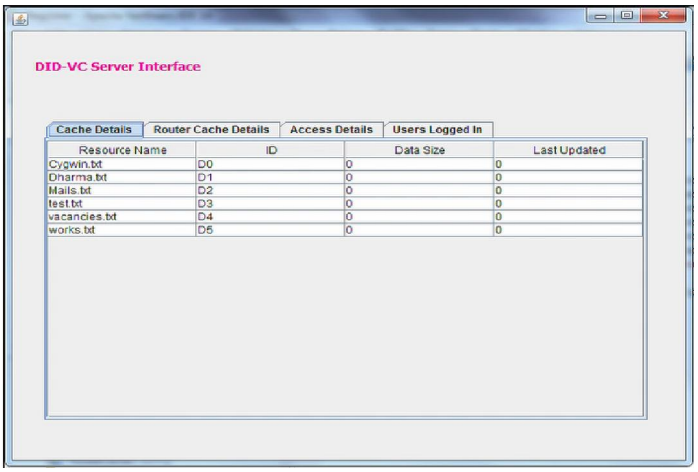

Figure 4: Register file in DID.

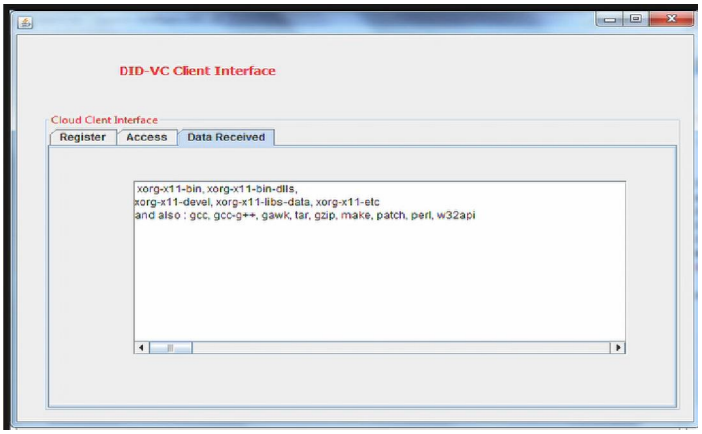

Figure 5: Accessing the DID file.

VI. CONCLUSION

By utilising an ICN architecture, the suggested project, a Decentralised Identifiers and Verifiable Credentials registry, was designed, put into practise, and evaluated. The layout provided in this work takes into It can be readily deployed in an existing ICN instance because it takes advantage of the ICN functions and primitives. The proposed solution hides ICN internals from legacy DID applications, which can use our system with little to no modification because it takes

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

into account the Edge-ICN architecture. The suggested approach can quickly supply append-only records of DID document versions because to ICN's intrinsic capability for caching and multicast. With this method, the ICN nodes' level of trust is minimally required. The majority of DID/VC registries use blockchain technology. However, using this technology comes with some extra overhead, such as a rise in communication and computation costs, storage costs, and oftentimes financial costs. A group of untrusted nodes can cooperatively maintain a blockchain thanks to Unlike our method, which allows each user to self-manage their own section of the DID registry, the DID registry. We contend that our strategy is equally decentralised and more secure.

REFERENCES

[1]. (2019) W3C Credentials Community Group. Decentralised Identifiers: A Primer. [Online]. accessible at https://w3c-ccg.github.io/did-primer.

[2]. N. Fotiou, V. A. Siris, G. Xylomenos, G. C. Polyzos, K. V. Katsaros, andG. Petropoulos, ‘‘Edge- ICN and application to the Internet of Things,’’in Proc. IFIP Netw. Conf., Jun. 2017, pp. 1– 610.23919/IFIPNetwork-ing.2017.8264880.

[3]. A quick introduction to NDN dataset synchronisation (NDN Sync), by T. Li, W. Shang, A. Afanasyev, L. Wang, and L. Zhang, appeared in the proceedings of the IEEE Military Communications Conference (MILCOM), in October 2018, pp. 612–618.

[4]. B. Lantz, B. Heller, and N. McKeown, ‘‘A network in a laptop: Rapid prototyping for software-define networks,’’ in Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw., New York, NY, USA, 2010, p. 19.

[5]. B. Pfaff, J. Pettit, T. Koponen, E. Jackson, A. Zhou, J. Rajahalme, J. Gross,A. Wang, J. Stringer, P. Shelar, K. Amidon, and M. Casado, ‘‘The designand implementation of open vswitch,’’ in Proc. 12th Symp. Netw. Syst. Des.Implement., Oakland, CA, USA, 2015, pp. 117–130.

[6]. Unbounded HIBE and attribute-based encryption, by A. B. Lewko and B. Waters, in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 6632, edited by K. G. Paterson, Springer, Tallinn, Estonia, 2011, pp. 547-567.

[7]. "Space/time trade-offs in hash coding with allowable errors," B. H. Bloom ACM Commun., vol. 13, no. 7, 1970, p. 422-426.

[8]. D. Longley and M. Sporny. 1.0 Linked Data Proofs. [Online]. Available at: https://ld-proofs.w3c-ccg.github.io.

[9]. M. Sporny, n.d. Data Model for Verifiable Credentials 1. [Online].Verifiable claims data model is accessible at https://www.w3.org/TR/.