International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature Access Control for Information Centric Networks

Aravinda Thejas Chandra*[1], Rajashekara Murthy S.[2]

Submitted: 11/12/2023 **Revised**: 25/01/2024 **Accepted**: 01/02/2024

Abstract: The internet applications of present data are immensely compassionate and on the other hand, users are found to be more specific about the desired content speed upon comparison to their location being accessed. In such circumstances the targeted users have to be provided finer if the intrinsic network permits to acquire the content being requested without as a matter of course depending on the existing producer of the data. Obviously, both authenticity and security require to be maintained for such types of data being retrieved. The Information Centric Networking (ICN) is intended to validate data access from anywhere taking into account all the requisite safety measures. The ICN is concentrated on minimizing content delivery latency and improving throughput by validating data from any data store upon comparison with the data producers. For the purpose of doing so, numerous changes in the prevailing Internet architecture like decentralized contextual attribute, unique content naming, access control, digital signature, etc. In this work a method called, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks is proposed. The TSDCA-DKS method is split into two sections, namely, Contextual Attribute Assignment using time windows synchronization and digital signature generation using Doubling-oriented Doche–Icart–Kohel model. The validation of the decrypted contextual input vector attribute guarantees data integrity, where the signer or the employer public key is used to ensure authenticity. The proposed method takes shorter access request processing time for the entire signature operation, including signing and verification, compared to other traditional methods. The implementation results of the proposed method manifested encouraging performance in terms of accuracy and robustness. The results confirmed that the proposed method is significant and efficient for employee's role within an organization and the resources to which they have access to.

Keywords*: Information Centric Network, Time Windows Synchronization, Contextual Attribute Assignment, Doubling-oriented, Doche–Icart–Kohel, Digital Signature*

1. Introduction

Information Centric Networking (ICN) is a novel standard or prototype where network communications is experienced by requesting named content in preference to sending packets to destination addresses.

To be more specific, clients or users in the ICN network make content or data search by describing content name instead of using host IP address of content producer as in conventional network.

While making possible the circulation of content to users and characterizing finer utilization of the network resources, ICN is also susceptible in that malicious users can inject corrupted content and segregate users from valid sources. Though the inception of signature verification can efficiently circumvent this attack, but it also institutes great amount of computation overhead.

A collaborative, secure, and efficient content validation protection method called, CSEVP was proposed in [1] to institute a collaborative defense procedure for ICN. Content verification was also made by means of probabilistic mechanism to get rid of the computation overhead of content verification. Also, bloom filter was applied for sharing verification results to additionally ease a more significant content validity, therefore reducing communication and storage overhead considerably.

Most access control policy executes authorization policies in a centralized manner bumping up serious security and privacy concerns. In [2], a Dynamic Access Control Policy (DACP) was proposed reinforcing dynamic cross-domain authorization. The DACP method integrated conventional attribute based access control (ABAC) model and attribute based group signature (ABGS). On one hand, ABAC was utilized for ensuring access control and on the other hand, ABGS was utilized for managing user's attributes between users and authorities. As a result, the user's attributes were distributed in a secure manner in addition to the access structure while protecting user's privacy, therefore reducing the decision time considerably.

[1]SJCIT, Chickballapur – 562101,
Visvesvaraya Technological University, Belagavi, INDIA
ORCID ID : 0000-0002-2978-6225
[2] RVCE, Bangalore – 560059,INDIA
Visvesvaraya Technological University, Belagavi, INDIA
ORCID ID : 0000-0003-2633-8125
** Corresponding Author Email: thejaschandra@gmail.com*

Due to the emergence of data-intensive applications, the prevailing Internet Protocol (IP) based internet features several issues in its host-centric framework. A prototype transposition from a host-centric framework to an information-centric framework is advantageous in data-intensive applications for content retrieval on the Internet. The information-centric framework concentrates on dispersing information objects upon comparison to the exchange between hosts. This mechanism has surfaced the course of action for novel restrategized Information-Centric Networks (ICNs).

A review of ICN concerning its privacy, security, scalability was investigated in [3]. ICN is a promising alternative data transmission technique that brings out much more cost-efficient communication in a highly mobile environment. However, due to the characteristic of IC, content poisoning emerges as a possible threat. A two phase security method was presented in [4] with the purpose of reducing the system overhead considerably. Yet another security protocol for ICN employing a public type of cryptography was proposed in [5]. Nevertheless, there involves a very few surveys on the ICN standardization status. To analyze on this aspect, history of global activities on ICN along with the recent improvement in the ICN standardization was investigated in [6].

The ICN is concentrated on minimizing content delivery latency and improving throughput by accrediting content (Data) serving to the client from any data store in the network rather than depending only on data producers. With the intention of doing so, it recommends numerous changes in the prevailing Internet architecture to name a few being, unique naming of content, routing based on name policy and self-secured data, etc.

A role based access control model was designed in [7] to address the specific requirements of managing information in cooperative model. Yet another method to secure attribute based information in industrial contexts was presented in [8]. Here both attribute based access control and attribute based encryption was provided for secured data sharing. Nevertheless, possessing a predictive method prior to forwarding may efficiently enhance the performance of contents being retrieved. In [9], a machine learning (ML) algorithm, called, Support Vector Machine (SVM) was utilized in forecasting interest packet success rate.

In this work, a method, called, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks is proposed. The main objective of this work is to improve the access request processing time and accuracy with minimal error rate. Several works have been proposed using optimization techniques for ICN. In contrast, the TSDCA-DKS method combines the decentralized contextual attribute and digital signature to ensure access request in an efficient and significant manner. First contextual attributes were provided based on time synchronization. Followed by Doubling-oriented Doche–Icart–Kohel-based Digital Signature algorithm is applied for ICN to ensure smooth and robust data access with minimal error.

1.1 Contribution

To overcome the issues from the above state-of-the-art works, TSDCA-DKS method is introduced with the novel contributions as listed below,

- To ensure computationally efficient access request processing for ICN, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) method is introduced by exploiting two different processes namely, time synchronization and digital signature.
- To acquire computationally efficient access request processing with minimal time and error, Time windows synchronization-based Contextual Attribute Assignment is applied based on Active Directory Domain Services as contextual attributes.
- Doubling-oriented Doche–Icart–Kohel-based Digital Signature is then applied therefore ensuring decentralization with improved access control for ICN, therefore reducing the improving the request access processing time and accuracy significantly.
- Immense experiments are organized to measure the performance of the TSDCA-DKS method and state-of-the-art methods. The results achieved shows that the proposed, TSDCA-DKS method achieved better performance in terms of access request time, access request accuracy, error and overhead.

1.2 Organization of the work

The rest of the paper is structured as follows: Section 2 introduces related works concerning access control, decentralized contextual attribute and application of digital signature for ICN. Section 3 describes the dataset description and proposes Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) method for ICN. The experimental results and the implementation details of the algorithm are given in section 4 and section 5 respectively. Followed by which performance analysis with the aid of table and graphical representations are provided in section 6. Section 7 concludes the paper.

2. Related Works

Information-centric network (ICN) is a novel networking paradigm wherein the contents are said to be utilized as objects. Hence, ICN is said to be specifically based on content. To be more specific, requests are made by the client for content by its name. Hence, it necessitates highly flexible and allocation of well-organized contents that can be accomplished by the ICN. For handling security mechanisms, like confidentiality, content integrity and authentication, in [10], a Digital Signature based Access Control method in ICN with the purpose of improving the security was designed. With this the confidentiality and integrity were said to be improved considerably. This nevertheless, opens a door for several security issues necessitate numerous security mechanisms. One of those is significant access control mechanism for ICN. In [11], an effective and secure access control method for ICN was designed keeping in these objectives.

Nevertheless, the message in the form of physical transfer is specifically said to be out of the peer's control. Originator-signed signatures essential in ICN ensure integrity and message sources exchanged between peer users that makes it probable to realize moderator-controlled information sharing. But moderated content necessitates multiple signatures that in turn increase the exchanged message size. To address on this aspect, an Identity-Based Aggregate Signatures (IBAS) to reduce the overhead was presented in [12].

With the mushrooming growth in the volume of internet usage and distribution of content services, several researchers have proposed a better mechanism for distributing content utilizing name instead of location. Subsequently, ICN set off the conclusive future internet architecture to restore the host-centric TCP/IP architecture in place of the content-based architecture.

A privacy preserving content retrieval scheme employing proxy encryption was presented in [13] that specifically did not required communication between consumers and providers. This type of architecture ensured minimal overhead and delay consecutively. Yet another method employing hierarchical identity-based security model was designed in [14] to minimize delay and average arrival rate of data packets significantly. Access control enforcement was provided in [15] employing efficient and secure content distribution. This in turn minimized the retrieval time reduction significantly.

A method that develops the base functioning of ICN and influences identification of content at the network layer, permitting to retrieve partial information pieces from content already present in ICN was proposed in [16]. Moreover, this mechanism also permitted information producers to offload certain content processing tasks into the network therefore minimizing traffic and storage consumption significantly. An elliptical access control mechanism was presented in [17] to circumvent unauthorized access on information in ICN.

A holistic literature review on the introduction of ICN in the context of internet of things (IoT) was discussed in detail in [18]. A comprehensive survey on access control mechanisms in ICN was investigated in [19]. Yet another time based access control mechanism was designed in [20]. Here, identity based encryption and proxy re-encryption were employed to prove efficiency and reliability.

The methods and techniques recommended above either considered access request processing time or accuracy into account without taking into consideration the error rate involved in designing or are specifically concentrated on accuracy of prevailing access control mechanism for ICN. However, the overhead was not taken for analysis. In this work, to improve the accuracy and time and allocate the request made with minimal delay and error a method called, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) is proposed. The elaborate description of the TSDCA-DKS method is provided in the following sections.

3. Methodology

There is an appreciable amount of data concerning an employee's role within an organization and also with the resources with which they have access to. Given with the data or information pertaining to the present employees (i.e., considered for simulation) and their corresponding access being provided by a supervisor, models can be configured to determine access privileges. Also, the prevailing internet framework is observing an outburst magnification in terms of both associated devices and the volume of content being generated. With this surge would results in several issues, like, access request processing efficiency and the overall accuracy. To bridge the gap in this, work a novel method called, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks. With the aid of the Information Centric Networks (ICN) more focus would more on the content centric communication pattern that targets the contents instead of the host address. Figure 1 shows the structure of Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for ICN.

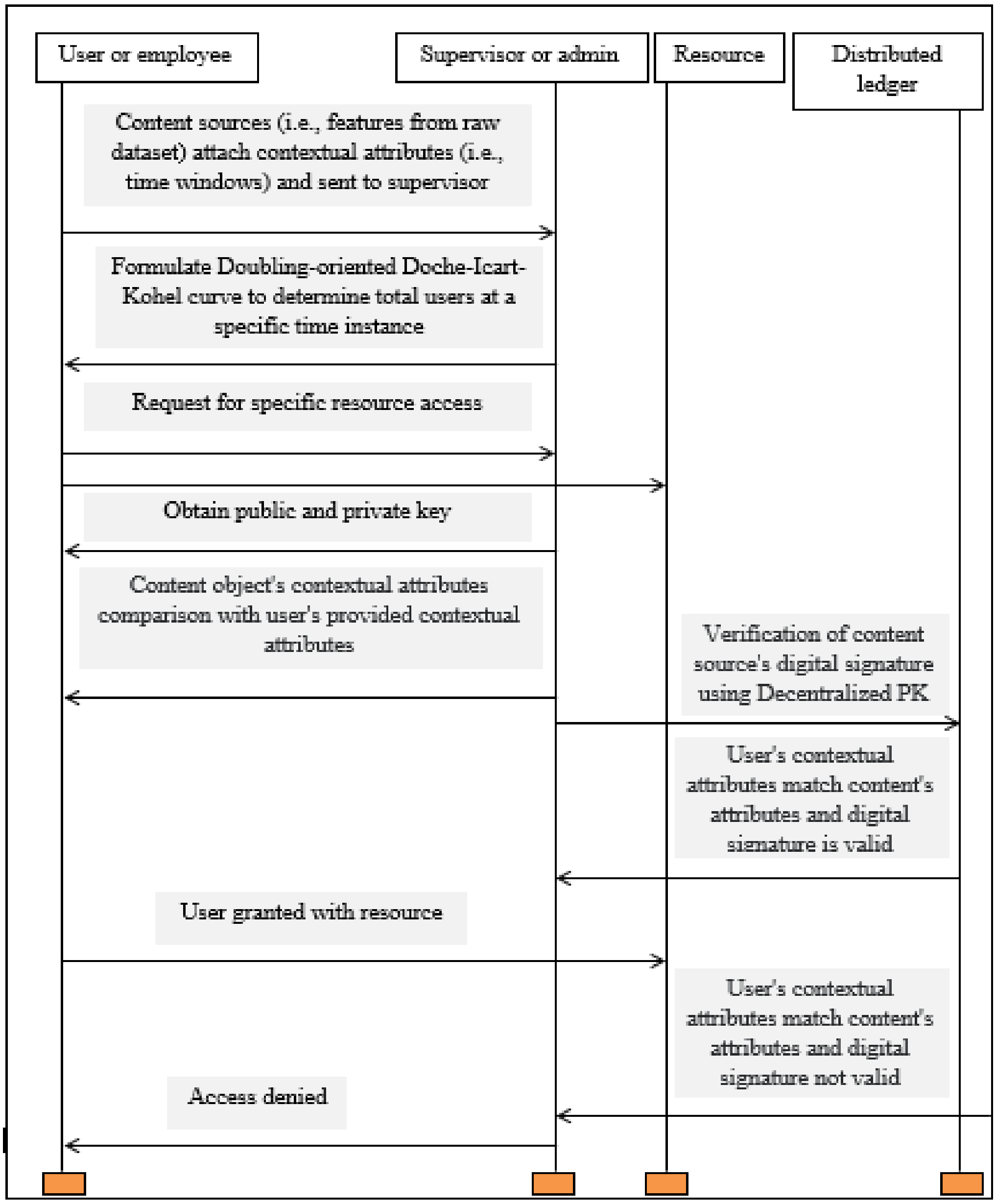
User or employee
Supervisor or admin
Resource
Distributed ledger
Content sources (i.e., features from raw dataset) attach contextual attributes (i.e., time windows) and sent to supervisor
Formulate Doubling-oriented Doche-Icart-Kohel curve to determine total users at a specific time instance
Request for specific resource access
Obtain public and private key
Content object's contextual attributes comparison with user's provided contextual attributes
Verification of content source's digital signature using Decentralized PK
User's contextual attributes match content's attributes and digital signature is valid
User granted with resource
User's contextual attributes match content's attributes and digital signature not valid
Access denied

Fig 1 Structure of Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for ICN

As illustrated in the figure, four entities are said to be formed, namely, user or employee, supervisor or admin, resource and distributed ledger. The user or employee here forms the core entity that makes an access request for a specific resource via supervisor or admin. The supervisor or admin initially forms the content objects via the content sources and the contextual attributes (i.e., time domain) by utilizing Time windows synchronization-based Contextual Attribute Assignment model. Following which key generation and digital signature is formulated by the supervisor via Decentralized public key using distributed ledger for each user by means of Doubling-oriented Doche–Icart–Kohel-based Digital Signature algorithm. Finally, the access decision is made by the supervisor by matching the user's contextual attributes with the content's attributes and the digital signature. Upon successful matching, access is said to be granted and accordingly resource is said to be accessed and on contrary, access is said to be denied and process is said to be proceeded with other set of users.

3.1 Dataset description

In this work, an employee’s action needs are predicted given his/her job role. In addition, also a signature based access control is introduced for ensuring security while supplying with the needs of the corresponding employee. The dataset used is employee access challenge acquired from https://www.kaggle.com/competitions/amazon-employee-access-challenge . The overall dataset is split into three csv files, namely, sample submission, test and train. Employees were permitted or denied access to resources over time in a manual fashion. In the training set each row possesses an ACTION and each employee's role information at approval time. On the other hand, in the testing set each row validates whether an employee having the registered features should have access to the resource or not. The column descriptions are provided below.

Table 1. Dataset column descriptions

S. No	Column name or feature name	Description
1	ACTION	Action is said to be '1' if the resource was approved and '0' if the resource was not approved
2	RESOURCE	An ID for each resource
3	MGR_ID	The employee ID of the manager
4	ROLE_ROLEUP_1	Company role grouping category ID 1 (US Engineering)
5	ROLE_ROLEUP_2	Company role grouping category ID 1 (US Retail)
6	ROLE_DEPTNAME	Company role department description (Retail)
7	ROLE_TITLE	Company role business title description
8	ROLE_FAMILY_DESC	Company role family extended description
9	ROLE_FAMILY	Company role family description
10	ROLE_CODE	Company role code

With the aid of the above dataset column descriptions the dataset for ensuring signature based access control for information centric networks is formulated as given below.

$$DS \rightarrow \{sample, test, train\} \tag{1}$$

$$sample \rightarrow \{ID, action\};\ test \rightarrow \{f_1, f_2, \dots, f_{10}\}; train \rightarrow \{f_1, f_2, \dots, f_{10}\} \tag{2}$$

The input vector matrix is mathematically stated as given below.

$$IV = \begin{bmatrix} S_1F_1 & S_1F_2 & \dots & S_1F_n \\ S_2F_1 & S_2F_2 & \dots & S_2F_n \\ \dots & \dots & \dots & \dots \\ S_mF_1 & S_mF_2 & \dots & S_mF_n \end{bmatrix} \tag{3}$$

From the above equation (3), the input vector matrix 'IV' is formulated based on the 'm' samples and 'n' features in action. Following which with the above generated input vector matrix,

3.2 Time windows synchronization-based Contextual Attribute Assignment

In the contextual attribute assignment phase the content sources from the above input vector 'IV' are attached with the contextual attributes to content objects. These contextual attribute in turn define when and where the content can be accessed. The contextual attributes could consist of either time windows, network conditions, device types or geographical locations or so on. In our work time windows synchronization synchronizing the date and time running in Active Directory Domain Services (ADDS) is employed. Figure 2 shows the structure of Time windows synchronization-based Contextual Attribute Assignment.

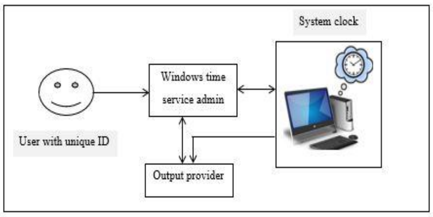

Fig 2 Structure of Time windows synchronization-based Contextual Attribute Assignment

As illustrated in the above figure, the users or the employees with unique ID request and receive time samples from network time protocol. These obtained time samples are then forwarded to the windows time service admin that with the aid of system clock selects the best time sample.

$$CIVA \rightarrow IV\ U\ TS \rightarrow CIVA \tag{4}$$

From the above equation (4), the contextual input vector attribute '$CIVA$' is formulated based on the actual input vector matrix 'IV' and the time sample 'TS' obtained from time windows synchronization process.

3.3 Doubling-oriented Doche–Icart–Kohel-based Digital Signature model

To start with a user requests access to a specific content object, providing their identity and any relevant contextual attributes (e.g., current time, location). Contrary to transmission control protocol/internet protocol, (TCP /IP), ICN security has been transposed from securitizing the path to securitizing the content. Hence, ICN is referred to as the content-based security. To ensure content-based security, ICN imparts digital signature for security and privacy of content. In other words, contents are said to be authenticated with digital signature and hence one of the main reasons that ICN is said to be more secure than TCP/IP. In practical applications, when an employee at any organization initiates works, they initially require to obtain computer access requisite to accomplish their role. This access in turn permits an employee to read resources via numerous applications or web portals. As a result, only those employees accomplishing the tasks of a given role will access same or similar resources.

Then, each user needs to sign on those documents provided with a given role to ensure smooth and robust access as a proof of confirmation. In this work, are going to propose a novel digital signature model for applying to the above case. Content sources digital sign context objects utilizing their private keys. The digital signature on the other hand, ensures the authenticity and integrity of content.

In this paper, we studied the formation of an accompanying signature for cryptographic algorithms that have a linear and very special public key generated using Doubling-oriented Doche–Icart–Kohel independently and also doubling speeds up considerably. Also, both the parameters (i.e., both the public key and private key) are said to be created over an affine coordinates that can assist in classifying a system (i.e., providing access control to authorized user). Figure shows the structure of Doubling-oriented Doche–Icart–Kohel-based Digital Signature model.

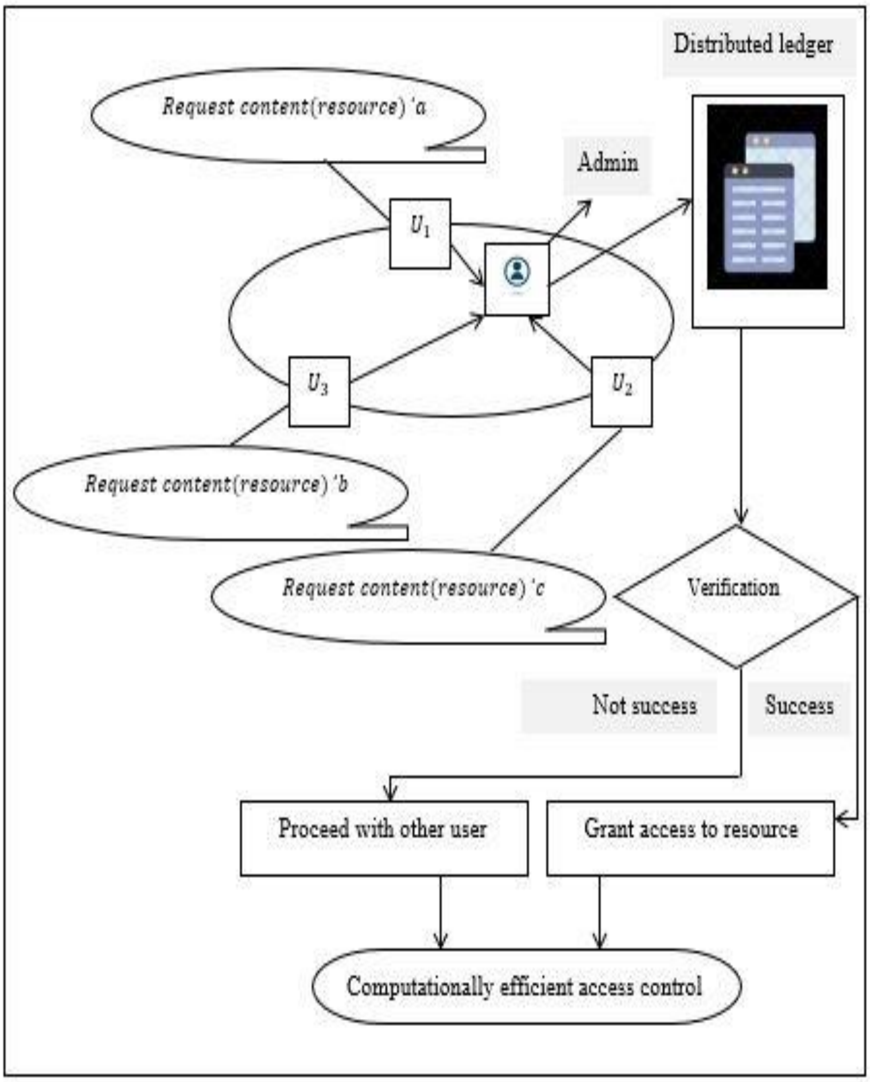
Distributed ledger
Request content(resource) 'a
Admin
U_1
U_3
U_2
Request content(resource) 'b
Request content(resource) 'c
Verification
Not success
Success
Proceed with other user
Grant access to resource
Computationally efficient access control

Fig 3 Structure of Doubling-oriented Doche–Icart–Kohel-based Digital Signature model

As illustrated in the above figure, let 'K' represent a field (i.e., overall data related to employee's role) and let '$S \in K$' then, the Doubling-oriented Doche–Icart–Kohel curve with parameter or sample 'S' in affine coordinates is mathematically represented as given below.

$$y^2 = x^3 + Sx^2 + 16Sx \qquad (5)$$

With the above Doubling-oriented Doche–Icart–Kohel curve, the number of users at a time ready for validating user access to access a resource is generated. Then, the affine space is formulated with points at infinity is mathematically stated as given below.

$$ZY^2 = X^3 + SZX^2 + 16SXZ^2 \qquad (6)$$

$$x = \frac{X}{Z}; y = \frac{Y}{Z} \qquad (7)$$

From the above equations (6) and (7) 'x' employees with an average or 'y' resources are necessitated and formulated via the Doubling-oriented Doche–Icart–Kohel curve that in turn aid in doubling the speed. Now let us formulate the digital signature formulation by initially initiating the sender random number 'RN' divided into two distinct random numbers 'RN_1' and 'RN_2' and formulated as given below.

$$RN = RN_1 * RN_2 \qquad (8)$$

With the above random number generated for the corresponding sender 'RN', the sender private key and public key are obtained as given below by means of Distributed Ledger.

$$PrivK_S = (privk_S, RN_2) \qquad (9)$$
$$PubK_S = (pubk_s, l, RN_1), pubk_s = privk_S + RN, l$$
$$= a * b \qquad (10)$$

From the above equations (9) and (10), private key '$PrivK_S$' and public key '$PubK_S$', are generated for each sender (i.e., employee) by employing the random number 'RN_2' and with the aid of two large prime numbers 'a' and 'b' respectively. This is performed by means of Distributed Ledger and provided with the public and private key for each sender for a specific session. The advantage of using this Distributed Ledger functionality is that it does not requires a separate administrator or third party and hence is said to be more secured and hence does not have a single point of failure. Following which each content object's contextual attributes '$CIVA$' is encrypted by the encryption function 'Enc' with the aid of receiver public key '$PubK_R$' and is as formulated as given below.

$$Enc_{PubK_R}(CIVA) = CT \qquad (11)$$

In the signing process, we need to go through the encryption process each content object's contextual attributes are compared with the user's provided contextual attributes to determine whether the content is within the user's access context. Here, the cipher text will be utilized in the verification process for extracting the original input vector and ensure data integrity. The content source's digital signature is verified using the sender or source's public key from a decentralized public key infrastructure (PKI) by means of a Distributed Ledger. Followed by which the sender or the employee who wants to access for certain resources signs the contextual input vector attribute '$CIVA$' by calculating 'f_1' and 'f_2' that contain their private keys '$PrivK_S$', 'RN_2' and 'p' as given below.

$$f_1 = (CIVA)^{PrivK_S} mod\ n \qquad (12)$$

$$f_2 = (CIVA)^{RN_2} mod\ n \qquad (13)$$

The digital signature then sent to the receiver or the admin who assigns the specific resources satisfying the access control is as given below.

$$DigS(CIVA) = (f_1, f_2) \qquad (14)$$

With the above said digital signature generation process as given in equation (14), the signing process for each user or entity request access to a specific content object is said to be accomplished. Followed by which the verification process is said to be initiated. After decrypting the cipher text 'CT' and retrieving the original message or contextual input vector attribute '$CIVA = Dec_{PrivK_R}(CT)$', the receiver or the admin evaluate the check value of 'u' with the aid of the sender's (i.e., sender employee's) public key '$PubK_S$' as given below.

$$u = CIVA^{PubK_S} mod\ n \qquad (15)$$

Following which the receiver or the admin utilizes the evaluated value of '$CIVA$' to detect any exploitation of the cipher text and ensure data integrity. Then, the scrutiny value 'v' is measured as given below.

$$v = \left(f_1 * f_2^{RN_1}\right) mod\ n \qquad (16)$$

With the above check value 'u' and scrutiny value 'v' final comparison is made to make access decision and access enforcement. Accordingly, the access decision is made if the user's contextual attributes match the content's attributes and the digital signature is valid, the access is said to be granted. Then, the user or employee can access the content object or resource. On the other hand, if any of the conditions, like, user's contextual attributes does not matches the content's attributes and the digital signature is not valid, access is said to be denied by the admin from further processing. The pseudo code representation of Doubling-oriented Doche–Icart–Kohel-based Digital Signature is given below.

Algorithm 1: Doubling-oriented Doche–Icart–Kohel-based Digital Signature model

```
Input: Dataset '$DS$', Samples '$S = \{S_1, S_2, \dots, S_m\}$', Features '$F = \{F_1, F_2, \dots, F_n\}$'
Output: computationally efficient access request content object
Step 1: Initialize '$m$', '$n$', random numbers '$RN_1$' and '$RN_2$', '$a$', '$b$'
Step 2: Begin
Step 3: For each Dataset '$DS$' with Samples '$S$' and Features '$F$'
    Step 4: Formulate input vector matrix as given in equations (1), (2) and (3)
    Step 5: Obtain time sample '$TS$'
    Step 6: Evaluate contextual input vector attribute '$CIVA$' as given in equation (4)
    Step 7: Formulate Doubling-oriented Doche–Icart–Kohel curve based affine coordinates to obtain user access at a specified time instance as given in equations (5), (6) and (7)
    //Primitives
    Step 8: Formulate sender random number as given in equation (8)
    Step 9: Obtain private and public key of sender as given in equations (9) and (10)
    //Signing process
    Step 10: Perform encryption function '$Enc$' using each content object's contextual attributes as given in equation (11)
    Step 11: Evaluate '$f_1$' and '$f_2$' as given in equations (12) and (13)
    Step 12: Formulate digital signature as given in equation (14)
    Step 13: Return digital signature '$DigS(CIVA)$'
    //Verification process
    Step 14: Evaluate the check value of '$u$' as given in equation (15)
    Step 15: Evaluate the scrutiny value of '$v$' as given in equation (16)
    Step 16: If '$u = v$'
        Step 17: Then access is granted
        Step 18: According to employee's role resources are said to be accessed
        Step19: Go to step 8
    Step 20: End if
    Step 21: If '$u \neq v$'
        Step 22: Then access is not granted
        Step 23: Go to step 8
    Step 24: End if
Step 25: End for
Step 26: End
```

As given in the above algorithm with the purpose of obtaining computationally efficient access request, a decentralized contextual attribute and signature based access control model is presented. With the contextual input vector attribute formed from the raw dataset via time windows synchronized contextual attributes, initially an input vector is formulated. Following which curve based affine coordinates employing Doubling-oriented Doche–Icart–Kohel curve is designed that being a doubling speeds up considerably, therefore improving access request processing time significantly. Following which key primitives for ensuring access control is formulated. Next, signing process is done for each content object's contextual attributes and accordingly digital signature is formed. Finally, verification is done by the admin to verify and validate the matching of user's contextual attributes with the content's attributes and digital signature. Upon successful accomplishment, the corresponding user access is granted with the requested resource and on contrary, the corresponding user access is denied and proceeds with the other set of users.

4. Experimental Setup

In this section, experimental evaluation of the proposed, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks and two existing methods A Collaborative, Secure, and Efficient Content Validation Protection (CSEVP) [1] and Dynamic Access Control Policy (DACP) [2] are implemented using **NDN simulator for NS3 using python**. The dataset used in this work is employee access challenge dataset acquired from

https://www.kaggle.com/competitions/amazon-employee-access-challenge where upon satisfying the access control via digital signature resource access is provided to the respective user or employee. The entire experiment is conducted in an Intel Core i5- 6200U CPU @ 2.30GHz 4 cores with 4 Gigabytes of DDR4 RAM. On the basis of the above analysis, experimental evaluations are performed with four performance metrics, access request processing time, access request processing accuracy, access request processing error and key generation time. To ensure fair comparisons same samples are obtained from the dataset and is applied to all the three methods and measured for an average of 10 simulation runs.

5. Implementation details

In this study, we developed a digital signature based access control method called, Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks as provided ground truth in table 1.

- The TSDCA-DKS method comprises of contextual attribute assignment and digital signature generation.
- We compared our TSDCA-DKS method to two existing methods, A Collaborative, Secure, and Efficient Content Validation Protection (CSEVP) [1] and Dynamic Access Control Policy (DACP) [2] using employee access challenge dataset to validate the results.
- Initially, 30000 samples were obtained from employing access challenge dataset.
- The samples were provided as input to the contextual attribute assignment model where time windows synchronization was employed to form content objects.
- With different user or entity requests access to a specific content object, providing relevant contextual attribute via time windows synchronization was then subjected to access enforcement.
- The method then applied decentralized public key infrastructure via distributed ledger with this public and private key were generated for each user or entity requests.
- The number of requests was then formulated using Doubling-oriented Doche–Icart–Kohel curve wherein user or entity requests for each session were obtained.
- Upon successful match of the user's contextual attributes with the content's attributes and the digital signature is valid, access is granted and corresponding resources are said to be access by the user and on contrary access is denied and process proceeds with other set of users.

6. Discussion

6.1 Performance analysis of request access processing time

In this section the request access processing time is analyzed. Once the request access has been made by the users a significant amount of time is said to be consumed in accessing the corresponding request and this is referred to as the request access processing time. This is mathematically formulated as given below.

$$RAP_{time} = \sum_{i=1}^{m} S_i * Time\ [RAP] \qquad (17)$$

From the above equation (17), the request access processing time 'RAP_{time}' is measured based on the samples involved in the simulation process 'S_i' and the time consumed in processing the request access '$Time\ [RAP]$'. It is measured in terms of milliseconds (ms). Table 2 shows the values of the request access processing time obtained for each of the three methods, TSDCA-DKS, CSEVP [1] and DACP [2].

Table 2. Comparisons of request access processing time

Samples	Request access processing time (ms)		
	TSDCA-DKS	CSEVP	DACP
3000	105	129	165
6000	135	185	235
9000	185	245	305
12000	215	290	385
15000	255	335	455
18000	285	385	525
21000	315	425	585
24000	355	485	635
27000	400	535	700
30000	455	585	735

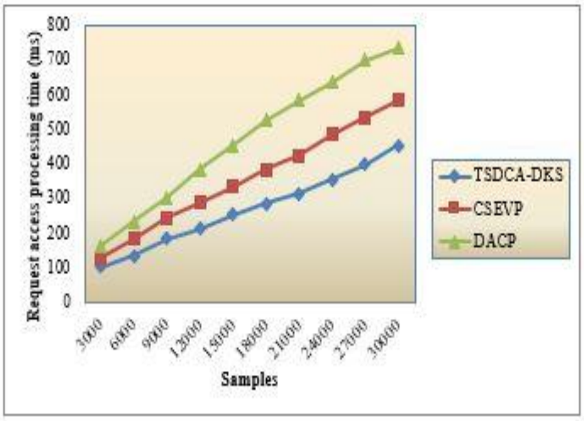

Fig 4. Graphical representation of request access processing time

Figure 4 given above shows the graphical plot of request access processing time for 30000 different samples involved in access control for ICN. To validate the results and make elaborate comparison with existing methods, CSEVP [1] and DACP [2] employee access challenge dataset was considered and simulations were performed for 10 different runs. From the above figure, blue line denotes the proposed TSDCA-DKS method, maroon red line indicates CSEVP [1] whereas green line points out the DACP [2] method. An increase in request access processing time was observed using all the three methods because with the increase in the samples for access control towards the use of resource heavy congestion is said to occur globally. While performing simulations with 3000 samples, request access processing time of 105ms, 129ms and 165ms were observed using TSDCA-DKS method, [1] and [2] respectively. From the simulation results it is inferred that the resource access processing time incurred using TSDCA-DKS method was comparatively lesser than [1] and [2]. The reason behind the minimization of request access processing time using TSDCA-DKS method was due to the application of Time windows synchronization-based Contextual Attribute Assignment. With this function, content sources from the above input vector were subjected to the Time windows synchronization-based Contextual Attribute forming the overall content objects. Accordingly, with the obtained time samples were are then forwarded to the admin that with the aid of system clock selected the best time sample and consecutively was provided to each samples or users. This in turn minimized the resource access processing time using TSDCA-DKS method by 25% compared to [1] and 42% compared to [2].

6.2 Performance analysis of request access processing accuracy

In this section the request access processing accuracy is measured to evaluate the efficiency of the method. The request access processing accuracy is mathematically stated as given below.

$$RAP_{acc} = \sum_{i=1}^{m} \frac{S_{ARA}}{S_i} \qquad (18)$$

From the above equation (18), the request access processing accuracy 'RAP_{acc}' is measured by taking into considerations the samples involved in the simulation process 'S_i' and the samples accurately provided with corresponding request access 'S_{ARA}'. It is measured in terms of percentage (%). Table 3 given below list the results of request access processing accuracy using the three methods, TSDCA-DKS, CSEVP [1] and DACP [2].

Table 3. Comparisons of request access processing accuracy

Samples	Request access processing accuracy (%)		
	TSDCA-DKS	CSEVP	DACP
3000	96.66	94.33	91.66
6000	95.15	93	90
9000	94	92.15	89.15
12000	93.35	91	87
15000	93	91	86
18000	92.15	90.35	85.25
21000	93	90.85	86
24000	93.55	91	87
27000	94	91.35	88.35
30000	95.25	92	89

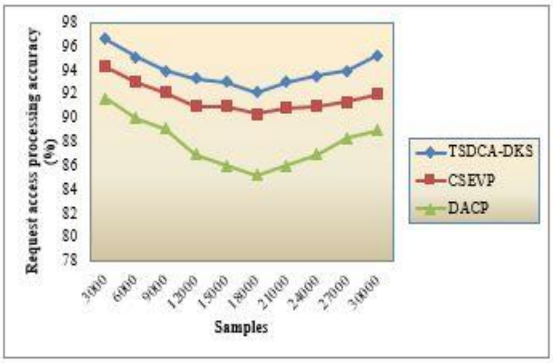

Fig 5 Graphical representation of request access processing accuracy

Figure 5 shows the comparison results of request access processing accuracy efficiency. The more samples the admin stores for simulation purpose, the lower the request access processing accuracy efficiency is. It can be seen clearly from figure 5 that the request access processing accuracy efficiency is not influenced by number of samples involved in simulation. This is evident from the result that even with the increase in the number of samples involved in simulation, the accuracy was also said to be improved. As shown in figure 5, the request access processing accuracy efficiency of our method is the best in these three methods. Moreover, as the number of samples increases, the processing efficiency gap among these three methods becomes larger and larger. In these three methods, the request access processing accuracy efficiency of our method is the highest. The state-of-the-art methods, CSEVP [1] and DACP [2] and the proposed TSDCA-DKS method, automated large class time synchronization to ensure accurate prediction. This time synchronization though can enhance the accuracy, but it also needs additional storage space to store the access request of each user. Nevertheless, this additional storage space is unavoidable. On the other hand, by applying Doubling-oriented Doche–Icart–Kohel curve, where the incoming access requests were monitored for a particular time instances aided in ensuring accuracy. This in turn improved the request access processing accuracy using TSDCA-DKS method by 3% compared to [1] and 7% compared to [2].

6.3 Performance analysis of request access processing error

Third in the section the request access processing error rate is measured. This performance metric is of high significance because of the reason that while providing access to users a small amount of error is said to occur and hence has to be measured. It is evaluated as given below.

$$RAP_{error} = \sum_{i=1}^{m} \frac{S_{IARA}}{S_i} \tag{19}$$

From the above equation (19), the request access processing error rate 'RAP_{error}' is evaluated by taking into considerations the samples involved in simulation 'S_i' and the samples inaccurately provided with request access 'S_{IARA}'. It is measured in terms of percentage (%). Table 4 given below lists the results of request access processing error using the proposed TSDCA-DKS and existing methods [1], [2].

Table 4 Comparison of request access processing error

Samples	Request access processing error (%)		
	TSDCA-DKS	CSEVP	DACP
3000	3.33	5.66	8.33
6000	4.15	6.15	9
9000	4.85	7.35	9.85
12000	5.35	8.95	10.35
15000	6	9.35	11
18000	7.25	10.15	12.15
21000	6.85	9.55	12
24000	5.35	9	11.35
27000	5.55	10	11.85
30000	6	10.25	12

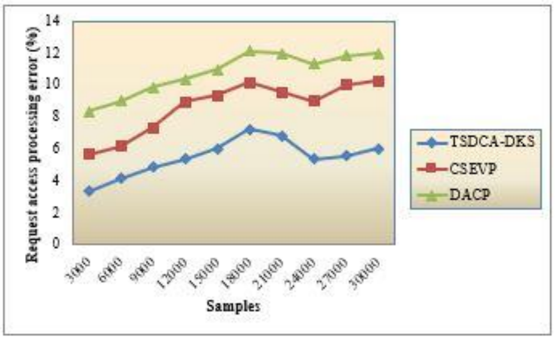

Fig 6. Graphical representation of request access processing error

Figure 6 given above shows the request access processing error involved in analyzing the decentralized contextual attribute for access control in ICN. An overall of 10 iterations were performed for an average of 30000 samples acquired from different employee with distinct role. Lower the error rate more efficient the method is said to be. In other words, lowering the number of incorrect predictions made or samples inaccurately provided with the access of certain resources predicted lower the error rate and vice versa. Simulations performed with 3000 sample observed error rate of 3.33% using TSDCA-DKS, 5.66% using [1] and 8.33% using [2]. With this simulation results the TSDCA-DKS method showed lower error rate upon comparison to [1] and [2]. As a result, the overall error rate observed for access requests made by the user or employee in an organization for corresponding resources to be accessed were found to be comparatively lower when applied with TSDCA-DKS method upon comparison to [1] and [2]. The reason behind the error minimization using TSDCA-DKS method was owing to the application of digital signature via Distributed Ledger functionality. By applying this functionality, a separate administrator is not said to be required for providing public and private key and hence it is not only said to be secured and also with the property of single point of failure assists in minimizing samples inaccurately provided with request access. This in turn reduced the request access processing error using TSDCA-DKS method by 37% compared to [1] and 50% compared to [2].

6.4 Performance analysis of request access processing overhead

Finally, in this section the request access processing overhead is measured. Owing to the reason that while granting request access for certain users or employees the signing in actions and verifications have to be stored in the intermediate layer, therefore consuming certain amount of memory. This is referred to as request access processing overhead and evaluated as given below.

$$RAP_{OH} = \sum_{i=1}^{m} S_i * Mem[RAP] \tag{20}$$

From the above equation (20) the request access processing overhead 'RAP_{OH}' is measured taking into consideration the samples 'S_i' involved in the simulation and the actually memory being consumed in the request access process '$Mem[RAP]$'. It is measured in terms of kilobytes (KB). Finally, table 5 given below lists the request access processing overhead results using the three methods, TSDCA-DKS, CSEVP [1] and DACP [2].

Table 5 Comparison of request access processing overhead

Samples	**Request access processing overhead (KB)**		
	TSDCA-DKS	CSEVP	DACP
3000	150	240	330
6000	185	275	355
9000	225	315	415
12000	250	355	435
15000	295	385	485
18000	315	415	515
21000	300	400	500
24000	285	365	455
27000	255	345	420
30000	200	300	380

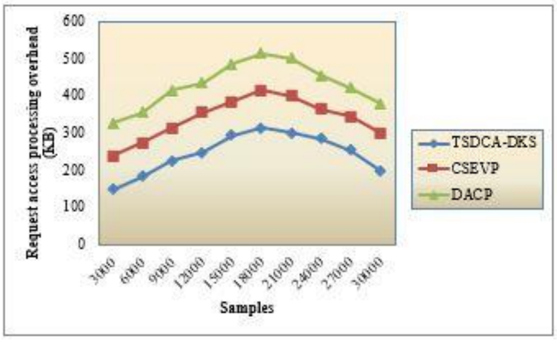

Fig 7 Graphical representation of request access processing overhead

We provide a comparison of request access processing overhead in figure 7. We arbitrarily sorted out 3000, 6000,…..,30000 samples from the dataset to do experiments. When the total number of samples is proportionately negligible, the request access processing overhead of the three methods, TSDCA-DKS, CSEVP [1] and DACP [2] are less. Also, from the figure it is inferred that increasing samples does not have negative influence on the overhead. Also, from the above analysis it is inferred that the overhead is comparatively better using TSDCA-DKS upon comparison to [1] and [2] with an overhead of 150KB using TSDCA-DKS for 3000 samples, 240KB using [1] and 330KB using [2]. The reason behind the improvement was owing to the application of Doubling-oriented Doche–Icart–Kohel-based Digital Signature algorithm. By applying this algorithm, contextual input vector attribute was first obtained using Time Synchronization. Followed by which digital signature was formed for each user or samples employing Doubling-oriented Doche–Icart–Kohel curve based affine coordinates via distributed ledger. This in turn reduces the overhead involved in the overall process using TSDCA-DKS by 28% compared to [1] and 43% compared to [2]. In conclusion, compared with methods [1], [2], our proposed TSDCA-DKS method has shown good efficiency in terms of request access processing accuracy, time, error and overhead.

7. Conclusion

Decentralized contextual attribute methods make over eminent results in providing access control for ICN. In this study, a new Time Synchronized Decentralized Contextual Attribute and Doubling Kohel Signature-based access control (TSDCA-DKS) for Information Centric Networks. First, to identify the incoming requests made by the user or employee in this work Contextual Attribute Assignment using time windows synchronization is made. Followed by which, to make computationally efficient access request processing, Doubling-oriented Doche–Icart–Kohel-based Digital Signature algorithm was designed that initially with the aid of Doubling-oriented Doche–Icart–Kohel curve the number of user request for respective resources was made. Following which digital signature employing decentralized public key via distributed ledger was generated that in turn improved the time and accuracy involved in granting access. For the purpose of exemplifying the efficiency of the method, models were constructed in different performance metrics and compared with CSEVP [1] and DACP [2]. This result exhibits that the framework and application designed yielded successful results in terms of accuracy, time, error and overhead.

References

[1] Kaiping Xue, Jiayu Yang, Graduate, Qiudong Xia, David S. L. Wei, Jian Li, Qibin Sun, Jun Lu, "CSEVP: A Collaborative, Secure, and Efficient Content Validation Protection Framework for Information Centric Networking", IEEE Transactions on Network and Service Management, Vol. 19, No. 2, June 2022 [A Collaborative, Secure, and Efficient Content Validation Protection (CSEVP)]

[2] Ahmad Salehi, Runchao Han, Carsten Rudolph, Marthie Grobler, “DACP: Enforcing a dynamic access control policy in cross-domain Environments”, Computer Networks, Elsevier, Mar 2023 [Dynamic Access Control Policy (DACP)]

[3] Lalitha Chinmayee M. Hurali and Annapurna P. Patil, “Application Areas of Information-Centric Networking: State-of-the-Art and Challenges”, IEEE Access, Nov 2022

[4] Jiancong Zhang, Shining Li, and Changhao Wang, “A Secure Dynamic Content Delivery Scheme in Named Data Networking”, Security and Communication Networks, Wiley, Jun 2022

[5] Bárbara Vieira, Erik Poll, “A security protocol for Information-Centric Networking in smart grids”, ACM, Nov 2013

[6] Keping Yu, Suyong Eum, Toshihiko Kurita, Qiaozhi Hua, Takuro Sato, Hidenori Nakazato, Tohru Asami, Ved P. Kafle, “Information-Centric Networking: Research and Standardization Status”, IEEE Access, Sep 2019

[7] Xuan Hung Le, Terry Doll, Monica Barbosu, Amneris Luque, Dongwen Wang, “An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow”, Journal of Biomedical Informatics, Elsevier, Jun 2012

[8] Alex Chiquito, Ulf Bodin, Olov Schelen, “Attribute-Based Approaches for Secure Data Sharing in Industrial Contexts”, IEEE Access, Feb 2023

[9] Nitul Dutta, Sudeep Tanwar, Shobhit K. Patel & Gheorghita Ghinea, “SVM-based Analysis for Predicting Success Rate of Interest Packets in Information Centric Networks”, Applied Artificial Intelligence An International Journal, Oct 2022

[10] Zaki Ullah, Samiullah Khan, “DSAC-Digital Signature for Access Control in Information Centric Network”, Sensors, Oct 2021

[11] Danye Wu, Zhiwei Xu, Bo Chen, Yujun Zhang Zhu Han, “Enforcing Access Control in Information-Centric Edge Networking”, IEEE Transactions on Communications, Jul 2020

[12] Tohru Asami, Byambajav Namsraijav, Kohei Sugiyama, Tomohiko Yagyu, Kenichi Nakamura, Toru Hasegawa, “Moderator-controlled Information Sharing by Identity-based Aggregate Signatures for Information Centric Networking”, ACM, Oct 2015

[13] Cesar Bernardini, Samuel Marchal, Muhammad Rizwan Asghar, Bruno Crispo, “PrivICN: Privacy-preserving content retrieval in information-centric networking”, Computer Networks, Nov 2018

[14] Bing Li, Maode Ma, “An Advanced Hierarchical

[15] Identity-Based Security Mechanism by Blockchain in Named Data Networking”, Journal of Network and Systems Management, Springer, Nov 2022

[16] Htet Hlaing, Yuki Funamoto, Masahiro Mambo, “Secure Content Distribution with Access Control Enforcement in Named Data Networking”, Sensors, Jun 2021

[17] José Quevedo, Daniel Corujo, “Selective Content Retrieval in Information-Centric Networking”, Sensors, Oct 2022

[18] Eslam G. AbdAllah Mohammad Zulkernine Hossam S. Hassanein, “Preventing unauthorized access in information centric networking”, Security Privacy, Wiley, Oct 2018

[19] Marica Amadeo, Claudia Campolo, José Quevedo, Daniel Corujo, Antonella Molinaro, Antonio Iera, Rui L. Aguiar, and Athanasios V. Vasilakos, “Information-Centric Networking for the Internet of Things: Challenges and Opportunities”, IEEE Network, Apr 2016

[20] Boubakr Nour and Hakima Khelifi, Rasheed Hussain, Spyridon Mastorakis, Usa Hassine Moungla, “Access Control Mechanisms in Named Data Networks: A Comprehensive Survey”, ACM Computing Surveys, Vol. 54, No. 3, Article 61. Publication date: April 2021

[21] Liehuang Zhu, Nassoro M.R. Lwamob, Kashif Sharif, Chang Xu, Xiaojiang Du, Mohsen Guizani, Fan Li, “T-CAM: Time-based content access control mechanism For ICN subscription systems”, Future Generation Computer Systems, Elsevier, Jan 2020