

A novel scheme for enhanced content integrity, authentication, and privacy in information centric network using lightweight blockchain-based homomorphic integrity and authentication

Aravinda Thejas Chandra¹, Rajashekara Murthy Shivarudraiah², Nagaraja Gadde³,
Ravi Kumar Begur Nagarajappa⁴

¹Department of Information Science Engineering, S.J.C. Institute of Technology, Chickballapur, Visvesvaraya Technological University, Belagavi, India

²Department of Information Science Engineering, R. V. College of Engineering, Bangalore, Visvesvaraya Technological University, Belagavi, India

³Department of Artificial Intelligence and Data Science, S.J.C. Institute of Technology, Visvesvaraya Technological University, Belagavi, India

⁴Department of Information Science Engineering, BMS Institute of Technology and Management, Bangalore, Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Jun 23, 2024

Revised Aug 25, 2024

Accepted Sep 3, 2024

Keywords:

Blockchain

Homomorphic encryption

Information centric networks

Lightweight blockchain-based

homomorphic integrity and authentication

Named data network

Privacy

ABSTRACT

Information-centric networks (ICNs) face challenges in ensuring content integrity and authentication while preserving user privacy. Homomorphic encryption has been widely used to protect content privacy within ICNs. Blockchain technology is widely applied in ICNs to ensure content integrity. Conventional blockchain-based authentication schemes rely on computationally expensive homomorphic encryption to perform secure data transmission. Also, the existing cryptography methods comprise confidentiality, and integrity while sharing content in ICNs. This paper proposes a novel lightweight blockchain-based homomorphic integrity and authentication (Light-BHIA) scheme to increase the integrity and privacy of content within ICNs. This scheme leverages the transparency and immutability of blockchain, the privacy-preserving properties of homomorphic encryption, and decentralized trust mechanisms to achieve secure and verifiable content delivery. The proposed work utilizes a lightweight homomorphic encryption scheme specifically designed for ICNs, reducing computational burdens by using resource-constrained devices. Light-BHIA uses the permissioned blockchain with an efficient consensus mechanism for increasing the trustworthiness of content delivery within ICNs. Authorized recipients can perform integrity and authentication checks on the encrypted content without decryption, maintaining confidentiality. The comparative study reveals proposed scheme achieved a 25% reduction in registration delay and confirms higher integrity, privacy, and confidentiality.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Aravinda Thejas Chandra

Department of Information Science Engineering, S.J.C. Institute of Technology, Chickballapur,

Visvesvaraya Technological University

Belagavi, Karnataka, India

Email: thejaschandra@gmail.com

1. INTRODUCTION

Information-centric networks (ICNs) offer a content-centric approach to data communication, shifting the focus from location-based addressing to named data objects. Content objects are confined data

elements that carry meaningful information [1]. However, ensuring content integrity and authentication in ICNs poses significant challenges due to the distributed nature of the network and the need to protect user privacy. Traditional cryptographic approaches often involve decryption for verification, which lacks confidentiality [2]. Also, the traditional cryptographic methods unable to provide centralized trust and compromise the content integrity in the verification process. Relying on a single public key for verification raises concerns about centralized trust and potential single points of failure. ndnSIM provides modules for signing and verifying data packets using traditional cryptographic algorithms. The existing system has configured content providers and consumers with specific keys and signature schemes. Named data networking (NDN) simulations tracked the flow of signed data packets, verified signatures at designated nodes, and analyzed the potential privacy implications of decryption-based verification. Unlike traditional client-server architectures with central authorities, NDNs lack a single point responsible for verifying content integrity. This makes it difficult to establish a trusted source for authenticity checks.

Some of the existing research based on providing security in content sharing for ICNs is described as the secure content delivery and deduplication model has been designed to get secure access in ICNs with many content suppliers [3]. A scalable key-policy attribute-based encryption (SKP-ABE) was developed to offer fine control and permit diverse attribute authorities to distribute some public attributes to simplify key management. A simple but effective mechanism was employed to eliminate redundant content. It minimized the lower storage overhead and better retrieval efficiency. Based on the proxy re-signature (PRS) cryptography, an anonymous authentication protocol was developed for content delivery networks [4]. A revocable PRS scheme was secure in the improved computational Diffie-Hellman hypothesis. The authentication protocol facilitates the origin server to assign and revoke the authentication potential to the network nodes without leaking its private key. It achieves anonymity, authentication, session key establishment, and forward security. A new trust-aware framework has been developed through the incorporation of ICN and blockchain for content security [5]. By applying authenticated data, content integrity was ensured across the network resulting in effective and efficient security measures. In addition, a collaborative, secure, and proficient content validation protection approach was investigated for ICN [6]. A joint regulating method depended on the threshold secret sharing and blockchain mechanism was introduced in study [7]. The suspicious data are censored with the help of authentication and the whole process is recorded as blockchain transactions. A proxy re-encryption approach to secure data sharing in internet of things (IoT) was described in study [8]. Identity-based encryption was employed to outsource the information and proxy re-encryption construction enables genuine user access to the data. Also, features of ICN were used to distribute cached content in the proxy effectively and enhance the quality of service. An elliptic curve-based data authentication model was introduced in the content-sharing process [9].

Blockchain technology is a fresh tool for numerous applications in diverse organizations, which allows for secure transactions in a decentralized authority [10]. Blockchain is adequate and mature enough to defend the data in its network. However, the information coming from outside of the world does not have any guarantee of data confidentiality and security. A key agreement protocol-based authentication approach for IoT devices was presented to provide a solution to the data confidentiality issue [11]. The developed approach prevents unauthorized access while exchanging information. Also, the IoT blockchain lightweight cryptographic (IBLWC) mechanism has been introduced to secure information in intelligent applications [12]. Other lightweight and secure authentication approaches were described in [13]–[15] to attain high-level security features.

Blockchain implementation architecture has been introduced to secure the processing of data through cryptographic proof of smart contracts [16]. A cryptographic and statistical privacy-preserving method has been designed for intruder discovery in blockchain networks [17]. A new model using blockchain and quantum cryptography was developed in study [18] for safeguarding data sensitivity and attaining security in internet of things. An approximation-based Homomorphic encryption model was introduced for blockchain-driven watermarking data [19]. A two-degree verification model was introduced to provide security during the data-sharing cloud IoT [20]. The model was worked on a rough set of rules and needs the secret key of the authorized user and is powerful enough to resist tracing attacks and insider user attacks. However, the authentication schemes and blockchain techniques were not used. Moldamurat *et al.* [21] explored new methods of cryptographic protection in authentication and authorization techniques for cellular networks.

A blockchain-based scheme for secure data sharing in NDN, a variant of ICN was proposed in [22]. Secure data transactions within the industrial internet of things (IIoT) using a lightweight blockchain approach were explored in [23]. The performance of homomorphic encryption for content verification in ICNs was evaluated in [24]. By evaluating the performance implications of homomorphic encryption in content verification, this research provides valuable insights for optimizing privacy-preserving ICN solutions. The scalability and efficiency concerns were addressed in lightweight blockchain protocols for resource-constrained devices [25]. A detailed survey on the use of homomorphic encryption within blockchain

systems is presented in study [26]. This survey explores various homomorphic encryption schemes and their applications in enhancing privacy and security within blockchain-based systems. The integration of blockchain technology with the IoT was explored in study [27]. While focusing on IoT, this survey offers valuable insights applicable to ICNs.

Despite cryptography methods having been used for secure sharing, the trustworthiness of content delivery within ICNs was not enhanced. Existing BHIA schemes may impose computational burdens on ICNs due to the use of homomorphic encryption. Also, conventional cryptography methods may compromise confidentiality during the verification process. While existing solutions offer promising functionalities, there remains a need for further advancements in areas like security, integrity, privacy, delay, authentication, centralized trust, scalability, and efficiency, particularly for resource-constrained ICN environments.

In response to the challenges faced by ICNs, this paper introduces a novel lightweight blockchain based homomorphic integrity and authentication (Light-BHIA) scheme to achieve content integrity, authentication, privacy, and security. Our proposed scheme strategically integrates the advantages of blockchain technology, homomorphic encryption, and decentralized trust mechanisms to establish a robust framework for secure and verifiable content delivery within ICNs.

The contribution of the research is as follows: i) The study contributes towards developing a novel and efficient scheme called Light-BHIA to ensure the integrity of content sharing in ICNs. ii) It also addresses the research challenges to avoid the drawbacks associated with the existing methods such as integrity, confidentiality, scalability, and delay, and attempts to improve the security of content transmission with permissioned blockchain and efficient consensus mechanisms. iii) The proposed work study also contributes to the decentralized trust mechanisms to minimize the pitfalls associated with the single public key. iv) The computational complexity of using homomorphic encryption is reduced by using resource-constrained devices in ICNs. v) The evaluation of the proposed methodology is carried out with the implementation of smart contract algorithms blockchain technologies where the robustness is checked for validating its real-time working prospects and experimental outcome found that the study accomplishes improved content security, integrity, authentication, user privacy, and overall network efficiency with lower delay. The present manuscript is organized as follows: section 2 describes the proposed method of this work. Section 3 illustrates the results and discussion. Section 4 provides a conclusion of the work.

2. PROPOSED METHOD

Light-BHIA scheme is proposed to enhance the content integrity, and privacy during the transmission in ICNs. The Light-BHIA scheme capitalizes on the transparency and immutability inherent in blockchain technology. A blockchain-based framework is designed to enhance the trustworthiness of content delivery within ICNs. Blockchain supports immutability, meaning it is unfeasible to remove or change recorded data. Therefore, the blockchain avoids data tampering in the network. Blockchain manages a decentralized and secure record of transactions or communications. Thus, the blockchain can ensure the fidelity and security of data records and generate the need for a third party. Also, the integration of homomorphic encryption is used with the advantages of preserving the privacy of outsourced storage and enhancing security by only allowing authorized users to access sensitive data. Security vulnerabilities happen when the resources are not managed properly. Hence, the lightweight scheme is particularly designed for resource-constrained devices to improve security and minimize computational complexity issues. Thus, the Light-BHIA scheme is a better choice to improve content privacy, authentication, and confidentiality in ICNs.

A permissioned blockchain platform is used for implementing the Light-BHIA scheme. The smart contract algorithms and cryptography algorithms are employed in the implementation process. The smart contract algorithm is applied to record the transactions or communications and get the data from the blockchain whereas the cryptography algorithms are applied to verify the functions. Additionally, simulations conducted using ndnSIM assess the scheme's performance, analyzing its effects on content delivery, privacy preservation, and overall network efficiency [28]. Figure 1 shows the architecture diagram of the Light-BHIA scheme.

The architecture diagram of the Light-BHIA scheme is used to improve content authentication and integrity within ICNs. Initially, the content requester (or user) registers their details with the ICN server (content provider). The server then stores the user's data in its database and generates a unique user ID and secret key for each registered content requester. Then the content provider (sender) encrypts data using Brakerski-Fan-Vercauteren homomorphic encryption. Whenever the user wants to access the data, verification is performed to check the authenticity of the user and decrypt the content with a digital signature. With this, integrity and privacy of the content transmission is ensured in ICNs.

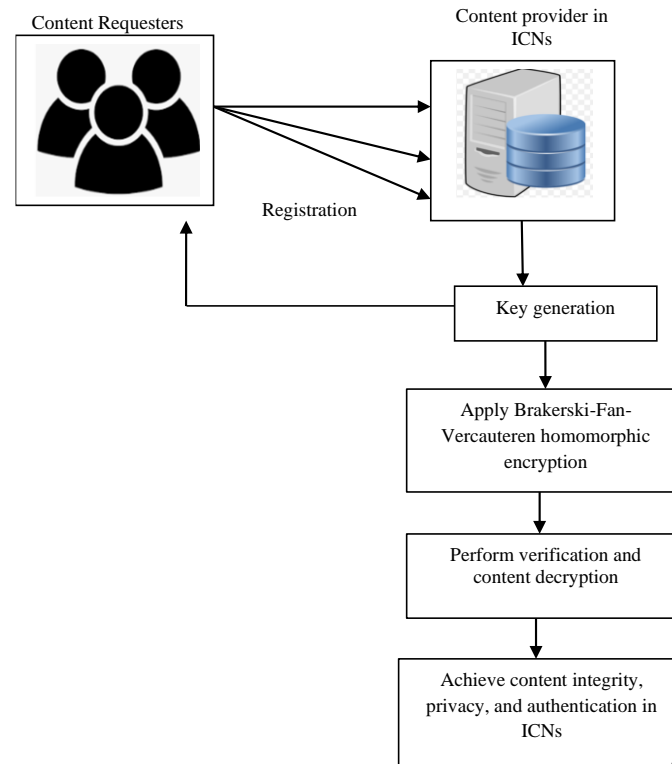


Figure 1. Architecture diagram of the Light-BHIA scheme

2.1. System model

Content requesters, acting as users or devices within the ICN, are responsible for initiating content requests. They play a crucial role in the system by sending requests to content providers, seeking specific content. Additionally, content requesters undergo an authorization check to verify their eligibility for accessing requested content. Their involvement in the homomorphic authentication process ensures the confidentiality of content during authentication checks, contributing to the overall security and privacy of the ICN.

Content providers serve as the sources of requested content and have distinct responsibilities within the system. They sign content objects with their private keys before distribution, ensuring the integrity and authenticity of the data. Content providers also encrypt content objects, adding a layer of privacy during the authentication process. Furthermore, they maintain a tamper-resistant record of content transactions by storing content transaction hashes on the blockchain.

Blockchain nodes maintain and validate the blockchain within the ICN. They record content transactions, creating a transparent and immutable ledger. Efficient consensus mechanisms ensure secure and reliable validation of content transactions. Moreover, they manage the blockchain ledger, facilitating integrity verification during the authentication process.

Authorization nodes verify the authorization of content requesters to access specific content. They execute smart contracts, enforcing predefined rules for content access authorization. Collaboration with content requesters during the authorization check phase ensures that only eligible entities gain access. By contributing to decentralized trust mechanisms, authorization nodes enhance system resilience and trustworthiness.

Homomorphic authentication nodes maintain the confidentiality of content during the authentication process. They perform computations on encrypted data using homomorphic encryption, enabling authentication checks without decryption. This addresses concerns related to content privacy and confidentiality, making the ICN more robust in safeguarding sensitive information. Decentralized trust mechanism participants distribute the responsibility for content verification across multiple nodes, minimizing risks associated with single points of failure. Their involvement in the verification process enhances the overall resilience and trustworthiness of the ICN.

New users undergo a verification process to establish their identity and authorization. Upon successful authorization, they receive certification generation, allowing access to content within the ICN. This ensures a seamless onboarding process for new participants, aligning with the scheme's goal of secure, privacy-preserving, and efficient content delivery in information-centric networks.

2.2. Blockchain technology integration

The Light-BHIA scheme leverages blockchain technology as a fundamental component. Blockchain, originally developed for secure and transparent transactions in cryptocurrencies, is utilized to enhance the trustworthiness and integrity of content delivery within ICNs. In the Light-BHIA scheme, each content transaction is recorded as a block in the blockchain, creating an immutable and transparent ledger [29]. This integration ensures that the history of content transactions remains tamper-resistant, providing a robust foundation for verifying the authenticity of data.

2.3. Homomorphic encryption for privacy preservation

One of the key elements in the Light-BHIA scheme is the integration of homomorphic encryption. This cryptographic technique allows computations to be performed on encrypted data without the need for decryption. In the context of ICNs, where user privacy is paramount, homomorphic encryption plays a crucial role in preserving the confidentiality of content during the verification process [30]. By enabling computations on encrypted data, Light-BHIA ensures that the privacy of the content is maintained, even when verifying its integrity. This represents a privacy-preserving feature that distinguishes the scheme from traditional cryptographic approaches.

2.4. Decentralized trust mechanisms

Addressing concerns related to centralized trust and potential single points of failure, the Light-BHIA scheme incorporates decentralized trust mechanisms. In ICNs, where traditional client-server architectures may lack a single point responsible for verifying content integrity, the Light-BHIA scheme distributes the responsibility for verification across the network [31], [32]. This decentralization mitigates risks associated with relying on a single public key, fostering a more resilient and trustworthy system. By spreading the verification process across multiple nodes, the scheme enhances security and reduces vulnerabilities.

2.5. Lightweight design for resource-constrained devices

Unlike some existing BHIA schemes that might impose computational burdens, the Light-BHIA scheme is specifically designed for resource-constrained devices within ICNs. The lightweight nature of the scheme ensures efficient utilization of resources, making it suitable for dynamic and content-centric environments. This design consideration addresses the practical challenges associated with deploying sophisticated cryptographic solutions on devices with limited processing power and memory [33]. In summary, the Light-BHIA scheme strategically combines blockchain technology, homomorphic encryption, and decentralized trust mechanisms to create a secure, privacy-preserving, and efficient framework for content delivery within ICN. This integration aims to overcome the challenges related to content integrity, authentication, and user privacy, offering a novel and comprehensive solution for the evolving needs of ICNs [34].

The ICN serves as the overarching framework within which content is requested and delivered. In this network, the primary actors include the content requester, who represents the users or devices initiating content requests, and the content provider, who serves as the source of the requested content [35]. The interaction between these entities forms the basis of the content delivery process in the ICN.

The Light-BHIA scheme, designed to enhance the trustworthiness, integrity, and privacy of content delivery within ICNs, comprises several integral components. Firstly, blockchain integration establishes a dedicated layer for recording content transactions. Each transaction is securely documented as a block in the blockchain, creating an immutable and transparent ledger. This blockchain integration ensures tamper-resistant historical records, forming a foundation for content authenticity verification. The decentralized trust mechanism represents the distribution of content verification across multiple nodes [36]. Secondly, Homomorphic Encryption is a crucial layer within the Light-BHIA Scheme, focusing on preserving user privacy during content verification. This cryptographic technique enables computations on encrypted data without requiring decryption, ensuring the confidentiality of content remains intact throughout the verification process.

The Figure 2 illustrates the system model for the Light-BHIA scheme in an ICN. The content requester (user/device) communicates with content providers through the Light-BHIA scheme. The scheme incorporates a decentralized trust mechanism and a lightweight design to enhance the security and efficiency of content sharing. The decentralized trust mechanism ensures trust without relying on a central authority, while the lightweight design optimizes performance for resource-constrained environments.

To address concerns related to centralized trust and potential single points of failure, the Light-BHIA scheme incorporates decentralized trust mechanisms. Instead of relying on a single point for content verification, this mechanism distributes the responsibility across multiple nodes in the network. This

decentralization minimizes risks, enhances security, and fosters a more resilient and trustworthy system. Additionally, the Light-BHIA scheme is characterized by its lightweight design, specifically tailored for resource-constrained devices within ICNs. Unlike some existing BHIA schemes that may impose computational burdens, the lightweight nature of the Light-BHIA Scheme ensures efficient utilization of resource. This design consideration addresses practical challenges associated with deploying sophisticated cryptographic solutions on devices with limited processing power and memory. The Light-BHIA scheme strategically combines blockchain technology, homomorphic encryption, decentralized trust mechanisms, and a lightweight design to provide a secure, privacy-preserving, and efficient framework for content delivery within ICN. This integrated approach aims to overcome challenges related to content integrity, authentication, and user privacy, offering a comprehensive solution tailored to the evolving needs of ICNs

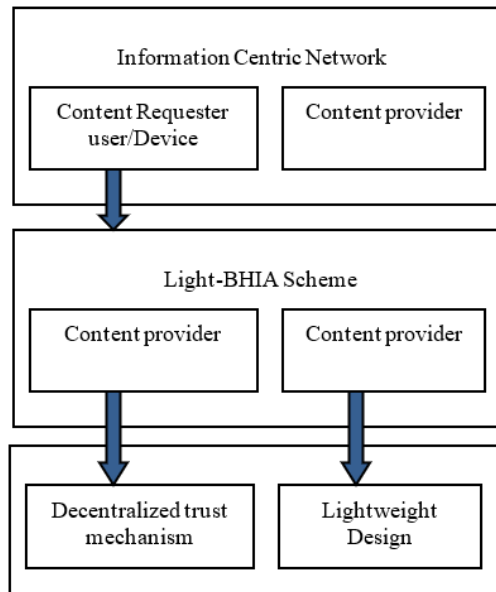


Figure 2. System model

2.6. Authentication scheme

The proposed Light-BHIA scheme addresses the challenges faced by ICNs in ensuring content integrity, authentication, and user privacy. In the contemporary landscape of ICNs, the need for secure and verifiable content delivery is paramount. The Light-BHIA scheme introduces a novel approach that strategically combines the transparency and immutability of blockchain, the privacy-preserving properties of homomorphic encryption, and decentralized trust mechanisms [37].

Authentication plays a pivotal role in ensuring the legitimacy and integrity of content within ICNs. In the Light-BHIA scheme, a permissioned blockchain is employed, utilizing efficient consensus mechanisms. This blockchain serves as a secure and transparent ledger, recording content transactions in a tamper-resistant manner. Content objects undergo encryption before distribution, and their corresponding hashes are stored on the blockchain. This process ensures that the history of content transactions remains unaltered, providing a foundation for robust authentication.

2.6.1. Mathematically, these steps involved homomorphic encryption

In the Light-BHIA scheme implemented with incremental cryptography notation using ndnSIM, the sender (S) initiates the process by preparing the original content object (M). This content undergoes hashing through a cryptographic hash function (H), generating a unique hash digest (h) to ensure its integrity throughout transmission and reception. Mathematically, this stage is represented as (1):

$$h = H(M) \quad (1)$$

Subsequently, the sender enhances tamper detection and integrity verification by incorporating a random nonce (r) during homomorphic signing. Through homomorphic addition ((+)), the hash digest (h) and the nonce (r) are combined to form a signed digest (s), expressed as (2):

$$s = h + r \quad (2)$$

To secure the integrity of the content during transmission, the sender utilizes Brakerski-Fan-Vercauteren (BFV) homomorphic encryption. Employing the receiver's public key (e_R), this process produces a homomorphic ciphertext (C). Mathematically, the encryption is denoted as (3):

$$C = \{Enc\}_{\{BFV\}(e_R, s)} \quad (3)$$

Simultaneously, the sender generates a digital signature ($\sigma - \text{sigma}$) for the original content object (M) using its private key (d_S). This signature ensures the authenticity and non-repudiation of the transmitted content:

$$\sigma = \{Sign\}(d_S, M) \quad (4)$$

During content transmission, the sender transmits both the homomorphic ciphertext (C) and the digital signature ($\sigma - \text{sigma}$) to the receiver. Upon reception, the receiver (R) proceeds with content verification, validating the digital signature ($\sigma - \text{sigma}$) using the sender's public key (e_S). The verification equation is expressed as (5):

$$\{Verify\}(e_S, \sigma, M) \quad (5)$$

Subsequently, the receiver decrypts the homomorphic ciphertext (C) using its private key (d_R), recovering the signed digest (s). This decryption process allows the receiver to access the signed digest for further verification:

$$s = \{Dec\}_{\{BFV\}(d_R, C)} \quad (6)$$

To ensure the integrity of the received content object (M'), the receiver computes its hash digest (h'). Following this, the receiver performs homomorphic subtraction ($(-)$) between the retrieved signed digest (s) and the newly computed hash (h'). Ideally, this operation results in the original nonce (r), providing enhanced granularity in content verification:

$$r = s - h' \quad (7)$$

Finally, the verification outcome is determined based on whether the result of the homomorphic subtraction ($(s - h')$) matches the expected random nonce (r). If the equality holds, it confirms the integrity of the content object (M') and validates its authenticity with enhanced granularity. The proposed Light-BHIA scheme, designed specifically for ICNs using ndnSIM, aims to tackle the challenges of content integrity, authentication, and user privacy. This scheme incorporates a series of mathematical equations to ensure the secure and efficient delivery of content within ICNs.

Blockchain integration plays a pivotal role in the Light-BHIA scheme, wherein hashed encrypted content is recorded onto the blockchain. This establishes a tamper-resistant ledger for content transactions, enhancing integrity and authentication within the network. Digital signatures are formulated based on the encrypted content and contextual attributes. These signatures provide cryptographic evidence of the sender's authenticity, ensuring the integrity and non-repudiation of content transactions. Additionally, message hashes are computed using cryptographic hash functions, further enhancing data integrity and authenticity. The scheme also includes mechanisms for signature validation and access control, to ensure only authorized users can access content. By evaluating check and scrutiny values based on transmission details, the scheme enhances user privacy and prevents unauthorized access to sensitive information.

Overall, the mathematical equations embedded within the Light-BHIA scheme serve to fortify content delivery in ICNs, leveraging blockchain technology, homomorphic encryption, and digital signatures to address the unique challenges of information-centric networks while safeguarding content integrity, authentication, and user privacy [38]. The proposed Light-BHIA scheme ensures content integrity and authenticity during transmission. It begins with content preparation, where the sender computes the hash digest (h) of the original content (M) and generates a signed digest (s) by adding a random nonce (r). The signed digest is then encrypted using Brakerski-Fan-Vercauteren (BFV) homomorphic encryption, producing a ciphertext (C), while the sender generates a digital signature ($\sigma - \text{sigma}$) for (M).

During transmission, both (C) and ($\sigma - \text{sigma}$) are sent to the receiver for verification. Upon reception, the receiver verifies ($\sigma - \text{sigma}$) using the sender's public key and decrypts (C) to retrieve (s).

The receiver then computes the hash digest (h') of the received content and performs homomorphic subtraction to verify the integrity of the content. If the result matches the expected nonce, the content's integrity and authenticity are confirmed.

The proposed Light-BHIA scheme introduces a lightweight design specifically tailored for ICNs, aiming to address the challenges of content integrity, authentication, and user privacy. By utilizing lightweight homomorphic encryption, the scheme reduces the computational burden on resource-constrained devices, enhancing its practicality for ICN deployments. This approach enables authorized recipients to perform integrity and authentication checks on encrypted content without decryption, preserving the confidentiality of the data [39].

Furthermore, the scheme introduces a standardized data format for content registration and verification, promoting interoperability across different BHIA implementations. This standardization resolves a critical limitation present in existing schemes lacking a uniform approach. Additionally, the scheme's compatibility with named data networking (NDN) aligns with ICNs' specific requirements, improving scalability and energy efficiency [40].

Figure 3 represents a cryptographic process using homomorphic encryption and digital signatures for secure content transmission. First, the content is prepared and signed with a homomorphic operation using Brakerski-Fan-Vercauteren (BFV) encryption. Then, the encrypted content is transmitted and upon reception, it is decrypted, and the signature is verified. The homomorphic verification checks the integrity of the content, and based on whether the result matches an expected nonce, the content is either accepted or rejected. This ensures both authentication and integrity during the transmission.

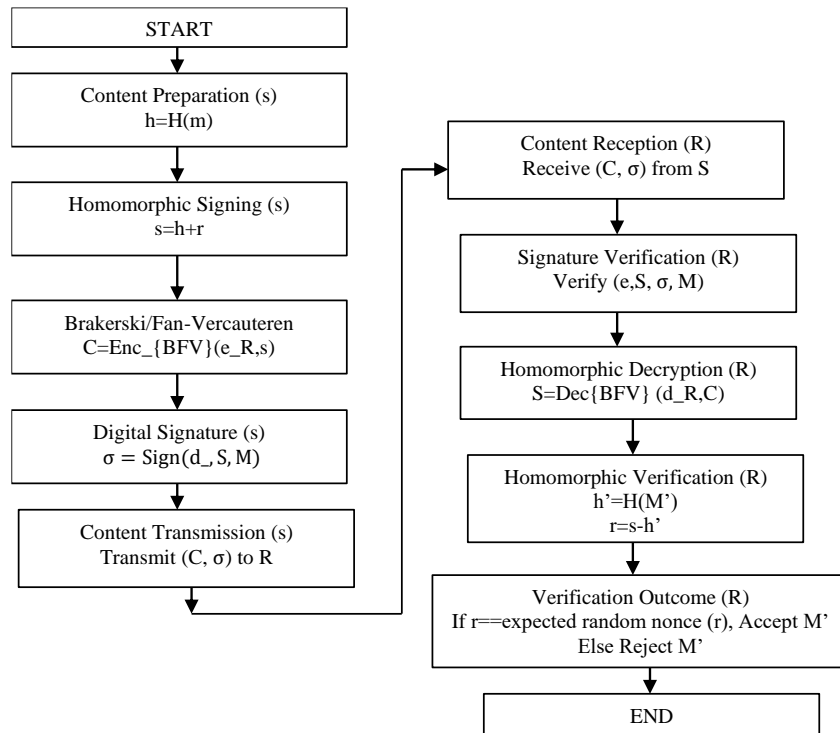


Figure 3. Light-BHIA ICN authentication flowchart

The authentication process in the Light-BHIA scheme encompasses various phases, ensuring secure and verifiable content delivery. Beginning with content request and encryption, where requests are initiated and content objects are encrypted before distribution, the process progresses to blockchain integration. Here, encrypted content transactions are documented in a permissioned blockchain, ensuring integrity and transparency through efficient consensus mechanisms and hash storage. Subsequently, the authorization check phase assesses the requester's authorization, enhanced by smart contract execution to enforce predefined rules. The process advances to homomorphic authentication, where computations on encrypted data ensure authentication checks without decryption, maintaining content confidentiality.

Decentralized trust mechanisms distribute authentication responsibilities across multiple nodes, minimizing risks associated with single points of failure. The introduction of a standardized data format

enhances interoperability, while compatibility with NDN improves scalability and energy efficiency. The entire authentication process is visually represented, including smart contract integration, verification process for new users, and certification generation for successful authorization [41].

In a simulated environment using ndnSIM with 30 nodes, the scheme's functionality is systematically orchestrated. Each node undergoes initialization, content request and encryption, blockchain integration, hash storage, authorization check with smart contract, homomorphic authentication, decentralized trust mechanisms, standardized data format application, Compatibility with NDN, and verification process for new users. This holistic approach provides a comprehensive understanding of the Light-BHIA scheme's functionality, incorporating mathematical representations, simulations, and real-world scenarios for secure and efficient content delivery in ICNs.

Algorithm 1 present outlines the implementation of the Light-BHIA scheme in ICNs using ndnSIM. It encompasses the steps of blockchain integration, verification, digital signature generation, and verification, ensuring secure and efficient content delivery while maintaining integrity and authenticity. Regarding ndnSIM implementation, while permissioned blockchain was explicitly specified, details regarding its integration with ndnSIM were not provided. However, it can be inferred that ndnSIM was utilized to simulate the behavior and interactions of the various nodes and components within the ICN, ensuring a comprehensive evaluation of the proposed scheme's performance under realistic network conditions.

Algorithm 1. LBHIA scheme

```

Input: Original content object M
Output: Enhanced content authentication and integrity
Begin
1. For each content requester
2. Send the request to the content provider
3. Content requester performs registration
4. Content Preparation (Sender, S):
   Compute hash digest:  $h=H(M)$ 
5. Homomorphic Signing (Sender, S):
   Generate random nonce:  $r$ 
   Compute signed digest:  $s=h+r$ 
6. Apply Brakerski-Fan-Vercauteren
   Perform Homomorphic Encryption (Sender, S):
   Encrypt signed digest:  $C=Enc_{\{BFV\}}(e_R, s)$ 
7. Digital Signature (Sender, S):
   Generate digital signature:  $\sigma=Sign(d_S, M)$ 
8. Content Transmission (Sender, S):
   Transmit  $(C, \sigma)$  to Receiver (R)
9. Content Verification (Receiver, R):
   Receive  $(C, \sigma)$ 
10. Signature Verification (Receiver, R):
   Verify signature:  $Verify(e_S, \sigma, M)$ 
11. Homomorphic Decryption (Receiver, R):
   Decrypt ciphertext:  $s=Dec_{\{BFV\}}(d_R, C)$ 
12. Homomorphic Verification (Receiver, R):
   Compute hash digest:  $h'=H(M')$ 
   Perform homomorphic subtraction:  $r=s - h'$ 
13.Verification Outcome:
   If  $r == 0$  then,
     "Content integrity and authenticity verified."
   Else
     "Verification failed, potential tampering or impersonation."
End

```

3. RESULTS AND DISCUSSION

Our proposed Light-BHIA scheme was implemented and evaluated using a permissioned blockchain platform known for its security, reliability, and scalability features [42]. The implementation comprised two primary components: smart contract algorithms responsible for registering transactions and retrieving data on the blockchain, and verification functions for cryptography calculations, excluding smart contracts. The experimental setup for evaluating our proposed Light-BHIA scheme was meticulously designed to provide comprehensive insights into its performance and capabilities. Leveraging the blockchain platform's security, reliability, and scalability, our implementation employed smart contract development. The experimentation environment featured a Linux OS configuration. To ensure a robust foundation, we conducted comparison test cases for each parameter. The communication link delay was intentionally set at 100 ms to simulate real-world network conditions and assess the scheme's performance under practical scenarios.

The meticulous experiment setup provided a reliable foundation for evaluating the proposed Light-BHIA scheme's efficiency and effectiveness in addressing the challenges posed by content integrity, authentication, and privacy within ICNs. While the permissioned blockchain platform was specified, ndnSIM implementation details were not explicitly mentioned. However, it can be inferred that the permissioned blockchain platform served as the backbone for the simulation environment, ensuring security and reliability in evaluating the Light-BHIA scheme's performance.

Figure 4 describes the results of registration delay based on the number of claims. The validation of the proposed LBHIA scheme is performed by comparing the results of the registration delay of existing named data networking-based data authentication (NDN-BDA) and decentralized public key infrastructure-zero knowledge proof (DPKI-ZKP). The time required to finish the registration phase (delay) is measured in milliseconds (ms). The delay of existing NDN-BDA is varied from 7,200 to 7,300 ms. Similarly, the delay of registration varied from 7,700 to 9,800 ms for existing DPKI-ZKP. Besides, the registration delay of the proposed LBHIA scheme is acquired as 7,500 to 9,700 ms.

Figure 5 depicts how the delay increases with the blockchain height and more consensus nodes, indicating that more time is needed to ensure consistency and reach a consensus. The x-axis takes blockchain height ranges from 0 to 400. With the increase in the blockchain height, delay is also increased. The overall certificate registration delay is varied from 5,000 to 11,400 ms. Node 4 gives a delay of 5,100 to 5,400 ms. Node 8 gives a delay as 7,100 to 7,500 ms whereas node 12 gives 11,000 to 11,400 ms of delay. It is found to be a higher delay in the registration phase. This observation highlights the impact of blockchain height and consensus node count on the registration phase delay.

The certificate registration phase delay of existing NDN-BDA can be observed in Figure 6. The delay is analyzed for three nodes such as node 4, node 8, and node 12. Based on the blockchain height, the certificate registration phase delay is measured. The certificate registration delay of NDN-BDA is varied in the ranges of 5,200 to 11,700 ms for three different nodes. In NDN-BDA, node 4 provides 5,200 to 5,700 ms of delay whereas node 8 provides 7,400 to 8,000 ms. Also, the 11,200 to 11,800 ms of delay is measured at node 12 and it is observed as the highest delay in NDN-BDA.

The certificate registration phase delay of existing DPKI-ZKP can be observed in Figure 7. The results of delay are measured for 3 nodes based on the blockchain height. Similar to the NDN-BDA, the results of DPKI-ZKP delay varied from 5,400 to 11,900 ms. Node 12 gives a higher delay than node 8 and node 4. For example, the 5,400 to 5,900 ms delay is achieved for node 4, 4,7500 to 8,000 ms of delay is achieved for node 8 whereas 11,300 to 11,900 ms of delay is attained for node 12.

The query, updating, and revoking delays of certificates were assessed with eight consensus nodes. Figure 8 demonstrates a rapid increase in query time for certificates as the blockchain height grows. This phenomenon is attributed to the larger data size of the distributed ledger, slowing down query traversal time. While the query delay is acknowledged, its optimization will be a focal point in future research. As compared to existing NDN-BDA and DPKI-ZKP, the proposed LBHIA achieved lesser query traversal time. Figure 8 displays the updating and revoking delays of the proposed LBHIA which are also influenced by the query delay. The delay is increased with the increase in the blockchain height. From Figure 9, the revoking delay is measured as 7,500 ms whereas the updating time of certificates is measured as 7,600 ms. Figure 10 shows the updating and revoking delays for certificates. Due to the influence of the query delay, the delays in terms of update and revocation were also longer.

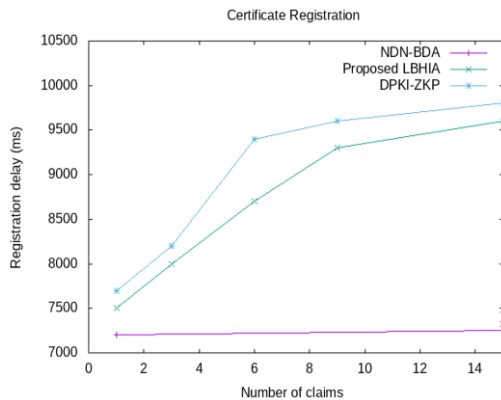


Figure 4. Registration phase delay comparison

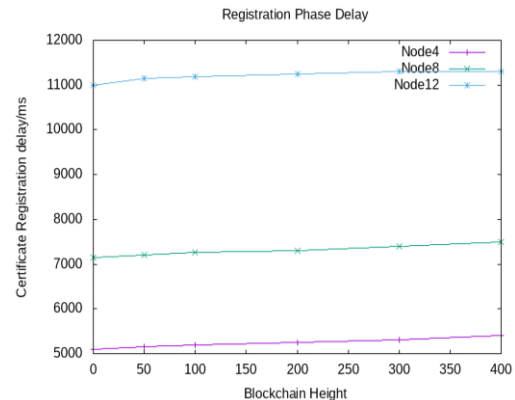


Figure 5. Registration phase delay with varying consensus nodes

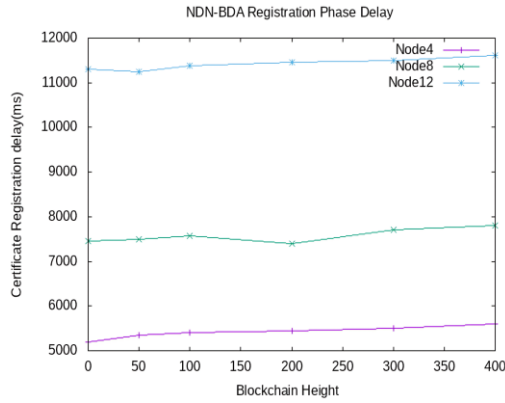


Figure 6. NDN-BDA registration phase delay

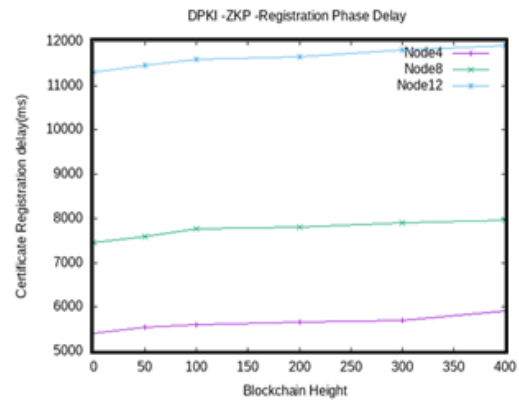


Figure 7. DPKI-ZKP-registration phase delay

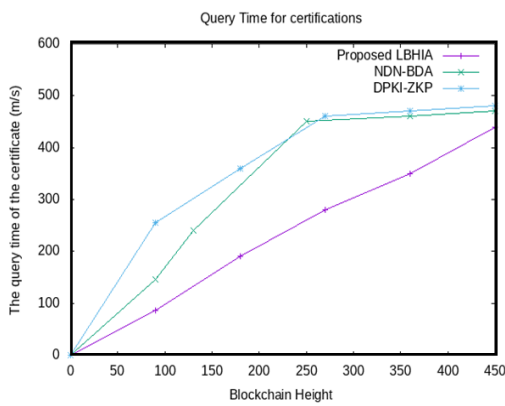


Figure 8. Certificate query time vs blockchain height

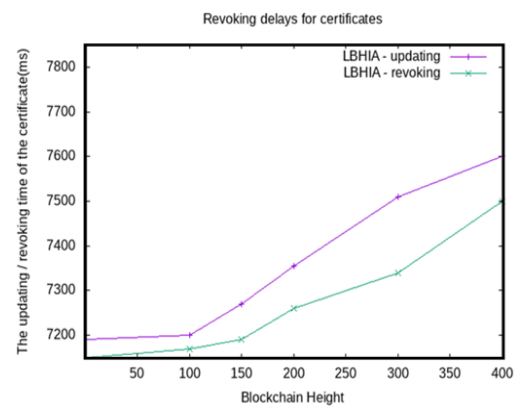


Figure 9. Revoking delays for certificates against blockchain height

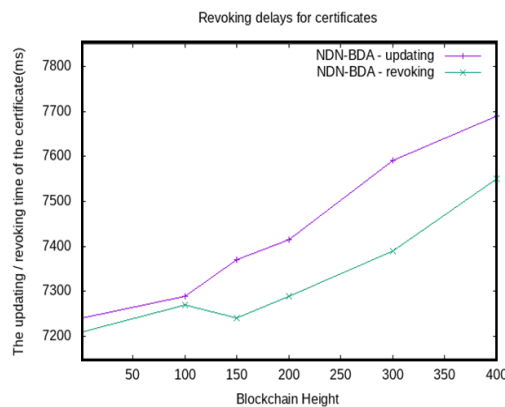


Figure 10. Updating/revoking delays for certificates

3.1. Findings and outcomes

From the results, it is analyzed that the proposed scheme has the capability of providing content authentication and integrity in ICNs by using a blockchain mechanism. Delay, centralized trust evaluation, and privacy preservation are problems in existing secure cryptography schemes such as NDN-BDA and DPKI-ZKP. The proposed method integrates homomorphic encryption, decentralized trust mechanisms, and blockchain technology for providing privacy preservation, centralized trust, and delay-minimized content sharing. From the comparison with the existing methods, NDN-BDA has limitations such as higher

verification time causing delays in certificate registration, higher query time owing to blockchain-based verification, and challenges raised between NDN and blockchain technology that concern the verification time. The DPKI-ZKP has a limitation of higher verification time, query time, and longer delay in updating and revoking certificates. These limitations are overcome by proposing a more efficient scheme in ICNs for content sharing. The proposed LBHIA reduced approximately 25% delay to the NDN-BDA and DPKI-ZKP. Despite LBHIA increases in the delay with the increase in the blockchain height, the incorporation of lightweight homomorphic encryption provided faster verification in ICNs. Thus, the experiments conducted on our proposed LBHIA scheme show its efficiency and effectiveness in addressing content integrity, authentication, and privacy concerns within ICNs. With this, higher security is achieved in ICN application areas in the future such as social networks, web applications, multimedia streaming, industrial IoT, and so on.

The proposed scheme stands out due to its lightweight design, which optimizes performance in environments where resources are limited. By integrating homomorphic encryption, the scheme ensures that data can be processed securely without revealing its contents, thus enhancing privacy and security in ICN systems. Additionally, the use of a permissioned blockchain framework supports efficient access control and data verification, which contributes to scalability and energy efficiency. Our results demonstrate that this approach surpasses traditional DPKI-ZKP and NDN-BDA in terms of security, speed, and resource management. These improvements open new possibilities for secure and practical content delivery across ICNs, supporting the network's evolving requirements.

Table 1 compares three ICN schemes Light-BHIA, NDN-BDA, and DPKI-ZKP, across several performance metrics. Light-BHIA demonstrates a 25% reduction in registration delays compared to the other two, particularly for multiple claim verifications, though delays increase with more consensus nodes and blockchain height. Both NDN-BDA and DPKI-ZKP show longer query times as blockchain height grows. Light-BHIA also benefits from lightweight homomorphic encryption for faster verification, while NDN-BDA and DPKI-ZKP face integration challenges, with DPKI-ZKP adding complexity due to zero-knowledge proof protocols.

Table 1. Comparison table of Light-BHIA scheme Vs NDNBDA Vs DPKI-ZKP scheme

Aspect	Light-BHIA Scheme	NDN-BDA	DPKI-ZKP
Registration phase delay	Approximately 25% reduction compared to NDN-BDA and DPKI-ZKP, especially noticeable with multiple claim verifications	Longer verification time, causing delays in certificate registration	Delays similar to the NDN-BDA scheme, potentially longer due to additional zero-knowledge proof verification
Registration phase with varying consensus nodes	Delay increases with blockchain height and more consensus nodes	-	-
Certificate query time vs blockchain height	The rapid increase in query time as blockchain height grows, attributed to larger data size	Longer query time due to blockchain-based verification	Longer query time due to zero-knowledge proof verification
Updating and revoking delays for certificates	Influenced by query delay; further optimization needed	Similar to the Light-BHIA Scheme	Longer updating and revoking delays due to additional zero-knowledge proof verification
Integrity and authentication verification	The integration of lightweight homomorphic encryption tailored for ICNs may offer faster verification	Integration challenges between NDN and blockchain technology may affect verification time	Verification time may depend on the efficiency of zero-knowledge proof protocols used for authentication

4. CONCLUSION

An innovative Light-BHIA scheme tailored specifically for ICNs to improve the security of content sharing. To address critical challenges related to content integrity, authentication, and user privacy within ICNs, blockchain technology, homomorphic encryption, and decentralized trust mechanisms were strategically integrated into the Light-BHIA scheme. The Light-BHIA scheme adopts a holistic approach, including a standardized data format for content registration and verification, compatibility with NDN, and decentralized trust mechanisms. This comprehensive solution positions the Light-BHIA scheme as a promising candidate to address the evolving needs of

ICNs effectively. The trustworthiness of content transmission within ICNs was increased with the integration of a blockchain-based model. Also, decentralized trust mechanisms were employed to solve the potential single points of failure. The experimental results reveal a significant 25% reduction in registration delay, particularly noticeable in scenarios involving multiple claim verifications. Leveraging a lightweight design and homomorphic encryption, the Light-BHIA scheme exhibits scalability, energy efficiency, and suitability for resource-constrained ICN environments. The utilization of a permissioned blockchain platform further alleviates scalability concerns, as seen in the experiments conducted with ndnSIM implementation.

A novel scheme for enhanced content integrity, authentication, and privacy ... (Aravinda Thejas Chandra)

Through experimental evaluation, our proposed scheme demonstrates remarkable efficiency and effectiveness, surpassing traditional DPKI-ZKP and NDN-BDA algorithms. Moreover, the experiments shed light on the influence of blockchain height and consensus node count on the registration phase delay, offering valuable insights for system optimization. Challenges associated with the growth of certificate query time as blockchain height increases underscore the necessity for ongoing research to optimize query delay in future iterations of the Light-BHIA scheme. In the future, research will concentrate on designing more scalable and multi-factor authentication mechanisms to improve the security of content transmission in ICNs.





REFERENCES

- [1] C. Gundogan, C. Amsuss, T. C. Schmidt, and M. Wahlisch, "Content object security in the internet of things: challenges, prospects, and emerging solutions," *IEEE Transactions on Network and Service Management*, vol. 19, no. 1, pp. 538–553, Mar. 2022, doi: 10.1109/TNSM.2021.3099902.
- [2] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing," *International Journal of Intelligent Networks*, vol. 3, pp. 16–30, 2022, doi: 10.1016/j.ijin.2022.04.001.
- [3] K. Xue, P. He, J. Yang, Q. Xia, and D. S. L. Wei, "SCD2: secure content delivery and deduplication with multiple content providers in information centric networking," *IEEE/ACM Transactions on Networking*, vol. 30, no. 4, pp. 1849–1864, Aug. 2022, doi: 10.1109/TNET.2022.3155110.
- [4] H. Xiong, Z. Zhou, L. Wang, Z. Zhao, X. Huang, and H. Zhang, "An anonymous authentication protocol with delegation and revocation for content delivery networks," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4118–4129, Sep. 2022, doi: 10.1109/JSYST.2021.3113728.
- [5] A. Bibi *et al.*, "TR-Block: a trustable content delivery approach in VANET through Blockchain," *IEEE Access*, vol. 12, pp. 60863–60875, 2024, doi: 10.1109/ACCESS.2024.3386461.
- [6] K. Xue *et al.*, "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, pp. 1761–1775, Jun. 2022, doi: 10.1109/TNSM.2021.3136547.
- [7] Q. Lyu *et al.*, "JRS: a joint regulating scheme for secretly shared content based on Blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2957–2971, Sep. 2022, doi: 10.1109/TNSM.2022.3175179.
- [8] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, "A proxy re-encryption approach to secure data sharing in the internet of things based on Blockchain," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685–1696, Mar. 2022, doi: 10.1109/JSYST.2021.3076759.
- [9] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5G-enabled vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1247–1259, Feb. 2022, doi: 10.1109/TITS.2020.3023797.
- [10] M. S. Mahmood and N. B. Al Dabagh, "Blockchain technology and internet of things: review, challenge and security concern," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 1, pp. 718–735, Feb. 2023, doi: 10.11591/ijece.v13i1.pp718-735.
- [11] S. Narayanappa, T. N. Anitha, P. Mishra, R. P. Herakal, and J. Kolar, "A trust based secure access control using authentication mechanism for interoperability in internet of things," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 2, pp. 2262–2273, 2024, doi: 10.11591/ijece.v14i2.pp2262-2273.
- [12] M. Parmar and P. Shah, "Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4422–4431, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4422-4431.
- [13] M. Fareed and A. A. Yassin, "A lightweight and secure multilayer authentication scheme for wireless body area networks in healthcare system," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1782–1794, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1782-1794.
- [14] R. Achary, C. J. Shelke, K. Marx, and A. Rajesh, "Security implementation on IoT using CoAP and elliptical curve cryptography," *Procedia Computer Science*, vol. 230, pp. 493–502, 2023, doi: 10.1016/j.procs.2023.12.105.
- [15] U. Ali *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for internet of things environment," *Internet of Things*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100923.
- [16] H. Szczepaniuk and E. K. Szczepaniuk, "Cryptographic evidence-based cybersecurity for smart healthcare systems," *Information Sciences*, vol. 649, Nov. 2023, doi: 10.1016/j.ins.2023.119633.
- [17] A. Z. Junejo, M. A. Hashmani, A. A. Alabdulatif, M. M. Memon, S. R. Jaffari, and M. N. B. Abdullah, "RZee: cryptographic and statistical model for adversary detection and filtration to preserve blockchain privacy," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 7885–7910, Nov. 2022, doi: 10.1016/j.jksuci.2022.07.007.
- [18] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: a novel approach using blockchain and quantum cryptography," *Internet of Things*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2023.101019.
- [19] D. Rosiyadi, A. I. Basuki, T. I. Ramdhani, H. Susanto, and Y. H. Siregar, "Approximation-based homomorphic encryption for secure and efficient blockchain-driven watermarking service," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4388–4400, 2023, doi: 10.11591/ijece.v13i4.pp4388-4400.
- [20] S. M. J. Rukmony and S. Gnanamony, "Rough set method-cloud internet of things: a two-degree verification scheme for security in cloud-internet of things," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 2233–2239, 2023, doi: 10.11591/ijece.v13i2.pp2233-2239.
- [21] K. Moldamurat, Y. Seitkulov, S. Atanov, M. Bakyt, and B. Yergaliyeva, "Enhancing cryptographic protection, authentication, and authorization in cellular networks: A comprehensive research study," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 1, pp. 479–487, 2024, doi: 10.11591/ijece.v14i1.pp479-487.
- [22] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data," *Computers & Security*, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102010.
- [23] F. Wang, J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong, "Blockchain-based lightweight message authentication for edge-assisted cross-domain industrial internet of things," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 1587–1604, Jul. 2024, doi: 10.1109/TDSC.2023.3285800.





- [24] T. Prantl *et al.*, "Performance Impact analysis of homomorphic encryption: a case study using linear regression as an example," in *Lecture Notes in Computer Science*, Singapore: Springer, 2023, pp. 284–298.
- [25] R. Raj and M. Ghosh, "A lightweight blockchain framework for secure transaction in resource constrained IoT devices," in *2023 5th International Conference on Recent Advances in Information Technology (RAIT)*, Mar. 2023, pp. 1–7, doi: 10.1109/RAIT57693.2023.10126898.
- [26] R. Salavi, M. M. Math, and U. P. Kulkarni, "A comprehensive survey of fully homomorphic encryption from its theory to applications," in *Cyber Security and Digital Forensics*, New Jersey, United States: Wiley, 2022, pp. 73–90.
- [27] A. Kharche, S. Badholia, and R. K. Upadhyay, "Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India," *Blockchain: Research and Applications*, vol. 5, no. 2, Jun. 2024, doi: 10.1016/j.bcra.2024.100188.
- [28] J. Quevedo and D. Corujo, "Selective content retrieval in information-centric networking," *Sensors*, vol. 22, no. 22, pp. 1–16, Nov. 2022, doi: 10.3390/s22228742.
- [29] M. A. Mohammed and H. B. A. Wahab, "Enhancing IoT data security with lightweight blockchain and Okamoto Uchiyama homomorphic encryption," *Computer Modeling in Engineering and Sciences*, vol. 138, no. 2, pp. 1731–1748, 2024, doi: 10.32604/cmescs.2023.030528.
- [30] Y. Lu, C. Wang, M. Yue, and Z. Wu, "Consumer-source authentication with conditional anonymity in information-centric networking," *Information Sciences*, vol. 624, pp. 378–394, May 2023, doi: 10.1016/j.ins.2022.12.051.
- [31] D. Du, W. Zhao, L. Wei, S. Lu, and X. Wu, "A lightweight homomorphic encryption federated learning based on Blockchain in IoV," in *2022 IEEE Smartworld, Ubiquitous Intelligence and Computing, Scalable Computing and Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous and Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, Dec. 2022, pp. 1001–1007, doi: 10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00148.
- [32] W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, "A review of homomorphic encryption for privacy-preserving biometrics," *Sensors*, vol. 23, no. 7, pp. 1–23, Mar. 2023, doi: 10.3390/s23073566.
- [33] P. P., M. M., S. K.P., and M. S. Sayeed, "An enhanced energy efficient lightweight cryptography method for various IoT devices," *ICT Express*, vol. 7, no. 4, pp. 487–492, Dec. 2021, doi: 10.1016/j.icte.2021.03.007.
- [34] H. H. Hlaing and H. Asaeda, "Ensuring content integrity and confidentiality in information-centric secure networks," in *2023 IEEE 20th Consumer Communications and Networking Conference (CCNC)*, Jan. 2023, pp. 810–816, doi: 10.1109/CCNC51644.2023.10060672.
- [35] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019, doi: 10.1109/JIOT.2019.2920987.
- [36] Q. Xia *et al.*, "PRIDN: a privacy preserving data sharing on named data networking," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 677–692, 2024, doi: 10.1109/TIFS.2023.3327660.
- [37] Q.-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. Bin Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6155–6176, Dec. 2023, doi: 10.1007/s40747-023-01058-8.
- [38] D. Doan Van and Q. Ai, "In-network caching in information-centric networks for different applications: A survey," *Cogent Engineering*, vol. 10, no. 1, pp. 1–21, Dec. 2023, doi: 10.1080/23311916.2023.2210000.
- [39] M.-J. Montpetit, C. Westphal, and D. Trossen, "Network coding meets information-centric networking: an architectural case for information dispersion through native network coding," in *Proceedings of the 1st ACM workshop on Emerging Name-Oriented Mobile Networking Design - Architecture, Algorithms, and Applications*, Jun. 2012, pp. 31–36, doi: 10.1145/2248361.2248370.
- [40] H. S. Shrishra and U. Boregowda, "An energy efficient and scalable endpoint linked green content caching for named data network based internet of things," *Results in Engineering*, vol. 13, Mar. 2022, doi: 10.1016/j.rineng.2022.100345.
- [41] Q. Xia, J. Gao, D. A. Worae, I. A. Obiri, and K. O. Asamoah, "Security overall in information-centric networks," in *Attribute-based Encryption (ABE)*, New Jersey, United States: Wiley, 2023, pp. 195–214.
- [42] S. Punathumkandi, V. M. Sundaram, and P. Panneer, "Interoperable permissioned-blockchain with sustainable performance," *Sustainability*, vol. 13, no. 20, pp. 1–12, Oct. 2021, doi: 10.3390/su132011132.

BIOGRAPHIES OF AUTHORS






Aravinda Thejas Chandra     received his B.E. degree in computer science and engineering from Kuvempu University, Shivamogga in 1996 and M.Tech. degree in computer science and engineering from Visvesvaraya Technological University, Belagavi in 2003. He is currently pursuing his Ph.D. from R.V. College of Engineering under Visvesvaraya Technological University, Belagavi. His area of interest includes network security, blockchain technology, IoT, cloud computing, and web technologies. He is presently working as associate professor at SJC Institute of Technology, Chickballapur, and he has 25 years of teaching experience. He is a Fellow of Institute of Engineers-FIE. He can be contacted at email: thejaschandra@gmail.com.






Rajashekara Murthy Shivarudraiah     holds a doctorate degree in natural language processing from Visvesvaraya Technological University, Belagavi. He has received his M.Tech. in computer science and engineering from Visvesvaraya Technological University, Belagavi, in 2001 and B.E. in computer science and engineering from Bangalore University, in 1998. He works as an associate professor in the Department of Information Science and Engineering, R.V. College of Engineering, Bengaluru and has 26 years of teaching experience. His area of interest includes NLP, network security, IoT, wireless communication. He is IEEE senior member, fellow, ISTE life member. He has published and reviewed many research papers in various journals and conferences. He has chaired many IEEE conference sessions and is also a BOE member in reputed autonomous universities, Bengaluru. He can be contacted at email: rajashekara.murthy@gmail.com.

A novel scheme for enhanced content integrity, authentication, and privacy ... (Aravinda Thejas Chandra)



Nagaraja Gadde    is a professor in the Department of Artificial Intelligence and Data Science, SJC Institute of Technology, Chickaballpur, Affiliated to Vishveswaraya Technological University, Belagavi, India. He completed B.E. in computer science and engineering, M.Tech. and Ph.D. in computer science and engineering. His area of interest includes wireless networks. He has more than 23 years of academic experience, He has authored research publications in reputed international journals and conference with good number of citations in Scopus indexed journals. He can be contacted at email: nagarajgadde11@gmail.com.



Ravi Kumar Begur Nagarajappa    currently working as an assistant professor in Department of ISE at BMS Institute of Technology and Management, Bangalore. He Completed Ph.D. in computer and information sciences at VTU in 2023, M.Tech. in CSE in 2013 and B.E. in CSE in 2008. He has teaching experience of 14 years, research experience of 6 years and 2 year industry experience. He has 15 publications in international conferences and reputed journals. His research interests are in the area of software engineering, artificial intelligence and machine learning. email: ravikumarn@bmsit.in.