IOT-ENABLED INNOVATIVE ENVIRONMENT WITH EFFICIENT ROUTING FOR THE DIGITAL LIBRARY SERVICES TO EXAMINE THE BEHAVIOR OF USERS

Reference NO. IJME 1394, DOI: 10.5750/ijme.v1i1.1394

W Zhou*, Nanjing University of Chinese Medicine Library, Nanjing, Jiangsu, 210023, China

*Corresponding author. W Zhou (Email): zhouwei@njucm.edu.cn

KEY DATES: Submission date: 21.12.2023 / Final acceptance date: 27.02.2024 / Published date: 12.07.2024

SUMMARY

An IoT-enabled innovative environment with efficient routing is proposed for digital library services to analyze user behavior. This conceptual framework leverages the Internet of Things (IoT) to create a smart library ecosystem where connected devices collect and share data in real-time. The emphasis on efficient routing ensures seamless access to digital resources, optimizing the user experience. This study introduces an IoT-enabled innovative environment aimed at optimizing digital library services by examining user behavior, incorporating the Clustered Centered Routing Cryptography Scheme (CCRCS). The proposed framework leverages the Internet of Things (IoT) to create a dynamic ecosystem within digital libraries, facilitating efficient data collection and analysis. By implementing the CCRCS, data transmission is secured through clustered-centered routing, ensuring the integrity and confidentiality of user interactions and resource access. Through the IoT infrastructure, libraries can monitor user behavior in real-time, capturing valuable insights into preferences, browsing patterns, and resource utilization. This holistic approach enables libraries to adapt their services to better meet user needs, optimize resource allocation, and enhance the overall user experience. The integration of IoT technologies with robust cryptographic protocols represents a significant advancement in digital library management, offering unparalleled opportunities for data-driven decision-making and personalized service delivery.

KEYWORDS

Internet of things (IoT), Cryptography, Clustering, Digital library, Behaviour of users, Routing

1. INTRODUCTION

Internet of Things (IoT) represents a transformative paradigm in the realm of technology, seamlessly intertwining the physical and digital worlds [1]. At its core, IoT involves connecting a vast array of devices, ranging from everyday objects to sophisticated machines, to the internet, enabling them to communicate and share data. This interconnected network facilitates a multitude of applications, from smart homes and cities to industrial automation and healthcare systems [2]. Sensors embedded in devices collect real-time data, which is then transmitted, processed, and utilized to enhance efficiency, optimize operations, and enable informed decision-making [3]. The pervasive integration of IoT not only streamlines daily tasks but also fosters innovation across various sectors, heralding a future where our surroundings are intelligent, responsive, and interconnected in ways previously unimaginable. In the digital library services, the integration of the Internet of Things (IoT) introduces a new dimension of efficiency and user experience [4]. IoT transforms traditional libraries into dynamic and intelligent spaces, where interconnected devices seamlessly collaborate to enhance the accessibility and functionality of resources. Smart sensors can monitor and manage inventory, ensuring that digital collections are up-to-date and readily available [5]. Additionally, IoT-enabled devices can provide personalized recommendations to users based on their preferences and historical interactions with the library's digital content [6]. This not only streamlines the search and retrieval process but also creates a more engaging and tailored experience for patrons [7]. Furthermore, IoT contributes to the optimization of library operations by offering real-time insights into usage patterns and resource popularity. As digital libraries evolve into interconnected hubs of information, the incorporation of IoT promises to revolutionize the way users interact with, discover, and benefit from the vast wealth of digital resources at their disposal [8].

The convergence of Digital Library services with the Internet of Things (IoT) marks a significant leap forward in the evolution of information repositories [9]. Digital libraries, already transforming the way we access and consume information, now stand at the forefront of technological innovation with the integration of IoT [10]. This synergy leverages smart sensors, interconnected devices, and real-time data analytics to create a more dynamic, responsive, and user-centric library experience. IoT enables the monitoring of resources, ensuring the availability and accuracy of digital

collections [11]. Through personalized recommendations based on user preferences and behaviors, IoT enhances the discoverability of content, creating a more engaging and tailored interaction [12]. Furthermore, the utilization of IoT in digital libraries optimizes operational efficiency by offering insights into resource usage patterns, allowing for informed decision-making and resource allocation. As digital libraries continue to evolve into intelligent information hubs, the incorporation of IoT not only enriches the user experience but also positions these repositories at the forefront of technological innovation in the digital age [13]. The Internet of Things (IoT) with digital library services represents a transformative shift that enhances the functionality and user engagement within these repositories of information [14]. Digital libraries, characterized by their vast collections of electronic resources, are evolving into dynamic ecosystems where IoT technologies play a pivotal role in redefining user experiences and operational efficiency. One of the key contributions of IoT to digital libraries is in resource management [15]. Smart sensors embedded in digital devices and reading materials allow for real-time tracking and monitoring of inventory [16]. This ensures that the library's digital collections remain current, accurate, and readily accessible to users. The automation of inventory management through IoT not only saves time and resources but also guarantees an optimal and seamless experience for library patrons [17].

Personalization is another significant aspect that IoT brings to digital libraries. By analyzing user preferences, behaviors, and interaction patterns, IoT-enabled systems can offer personalized recommendations to users, creating a more tailored and engaging experience [18]. This not only facilitates efficient content discovery but also encourages users to explore diverse resources they might not have otherwise considered. Operational efficiency receives a substantial boost through the implementation of IoT in digital libraries [19]. Real-time data analytics and insights generated from IoT-enabled devices provide librarians and administrators with valuable information about resource usage patterns, peak times, and popular content [20]. This data-driven approach allows for informed decision-making regarding resource allocation, collection development, and service improvements, ultimately optimizing the overall efficiency of the library [21]. Furthermore, the integration of IoT enhances the physical aspects of the library space. Smart environmental sensors can monitor factors such as temperature, humidity, and lighting conditions, creating an environment conducive to preserving the integrity of physical collections and ensuring the comfort of library patrons [22]. As digital libraries continue to evolve into intelligent hubs, the seamless integration of IoT technologies not only transforms the way users engage with information but also positions these institutions at the forefront of technological innovation [23]. The synergy between digital libraries and IoT not only meets the evolving needs of users in the digital age [24] but also propels libraries into a new era of efficiency, personalization, and accessibility.

2. RELATED WORKS

The various scholarly articles that explore different aspects of IoT (Internet of Things) technology and its applications [25] across diverse domains. Anandkumar, Dinakaran, and Mani (2022) present a study on the utilization of IoT-enabled smart buses for managing COVID-19 situations, highlighting the potential of IoT in addressing pandemic-related challenges. Shahzad and Khan (2023) conduct a systematic literature review on the effects of e-learning technologies on university librarians and libraries, emphasizing the significance of digital advancements in educational settings. Mishra, Kumar, and Godfrey (2022) propose an energy-efficient solution for IoT-enabled software-defined sensor network architecture, focusing on optimizing energy consumption in IoT systems. Alotaibi (2022) explores the integration of IoT in library activities at Taibah University in Saudi Arabia, illustrating the potential of IoT in enhancing library services. Lone, Mustajab, and Alam (2023) conduct a comprehensive study on cybersecurity challenges and opportunities in the IoT domain, emphasizing the importance of robust security measures. Jacob, Pravin, and Kumar (2022) propose a secure healthcare framework based on IoT and modified RSA algorithm, emphasizing the importance of data security in healthcare IoT applications. Lakshminarayana et al. (2022) investigate data-driven techniques for detecting and identifying IoT-enabled load-altering attacks in power grids, highlighting the importance of cybersecurity in critical infrastructure. Quy et al. (2022) discuss the architecture, applications, and challenges of IoT-enabled smart agriculture, illustrating the potential of IoT in revolutionizing farming practices. Lam et al. (2022) conduct a systematic review on IoT-enabled technologies as interventions for childhood obesity, showcasing the potential of IoT in promoting health and wellness. Hasan et al. (2023) analyze factors influencing young physicians' intention to use IoT services in healthcare, shedding light on adoption barriers and facilitators. Deebak et al. (2022) propose TAB-SAPP, a trust-aware blockchain-based authentication system for massive IoT-enabled industrial applications, emphasizing the importance of trust and security in industrial IoT deployments. Assaad, Mohammadi, and Chang (2023) introduce an IoT-enabled sensing device for quantifying the reliability of shared economy systems, highlighting the role of IoT in enhancing trust and transparency. Subramanian et al. (2022) explore the role of digital tools and technologies, including IoT, in managing the COVID-19 crisis, illustrating the potential of technology in addressing global health challenges. Shah, Bhat, and Khan (2022) review CloudIoT-driven healthcare, discussing architecture, security implications, and open research issues, highlighting the transformative potential of IoT in healthcare delivery. Finally, Sun and Ji (2022) examine the impacts of IoT technology on the

e-commerce channel, providing insights into the benefits and challenges associated with IoT adoption in online retail.

For instance, while Anandkumar, Dinakaran, and Mani (2022) focus on IoT-enabled smart buses for managing COVID-19 situations, the findings may not directly apply to other contexts or locations with different infrastructures or healthcare systems. Similarly, studies such as Alotaibi's (2022) examination of IoT in library activities at Taibah University may not fully capture the diverse challenges and opportunities faced by libraries in different regions or institutional settings. Additionally, some articles may lack longitudinal data or large-scale empirical studies, limiting the robustness of their conclusions. For example, while Quy et al. (2022) discuss the architecture, applications, and challenges of IoT-enabled smart agriculture, the findings may be based on limited case studies or experimental setups, rather than extensive field trials or real-world implementations. Furthermore, the reliance on self-report measures or subjective assessments in some studies, such as Hasan et al. (2023) analyzing factors influencing young physicians' intention to use IoT services in healthcare, may introduce biases or inaccuracies in the reported results.

3. PROPOSED METHOD CLUSTERED CENTERED ROUTING CRYPTOGRAPHY SCHEME (CCRCS)

The proposed method, Clustered Centered Routing Cryptography Scheme (CCRCS), represents an innovative approach tailored for enhancing the security and efficiency of Internet of Things (IoT) enabled digital library services. CCRCS leverages a clustered architecture to organize and manage the network of interconnected devices within the IoT ecosystem. By grouping devices into clusters, the scheme establishes a centralized routing framework that optimizes data transmission and ensures secure communication. Cryptography plays a central role in CCRCS, as it employs advanced encryption techniques to safeguard the integrity and confidentiality of data exchanged between devices and the digital library infrastructure. The proposed Clustered Centered Routing Cryptography Scheme (CCRCS) represents a novel method designed to optimize the functionality of IoT-enabled innovative environments, specifically tailored for efficient routing in digital library services. CCRCS introduces a clustered architecture to organize the network, ensuring a structured and streamlined communication environment. Let's delve into the derivation and equations underpinning CCRCS. The clustered architecture involves grouping IoT devices into clusters, each with a designated cluster head responsible for managing communication within the cluster. The routing process is optimized through a centralized approach, minimizing data transmission delays and energy consumption. The intra-cluster communication is facilitated through the equation (1)

$$Pij = \frac{1}{2} dij \tag{1}$$

In equation (1) *Pij* represents the transmission power between devices i and j, and *dij* is the distance between them. This equation ensures that power allocation is inversely proportional to the square of the distance, promoting efficient energy usage within the cluster. The cryptographic aspect of CCRCS employs advanced encryption techniques to secure data transmission within and between clusters. The encryption algorithm is represented by the equation (2)

$$E(D, K) = C \tag{2}$$

In equation (2) *D* is the plaintext data, *K* is the encryption key, and *C* is the ciphertext. The encryption process guarantees the confidentiality and integrity of digital library data, crucial for protecting sensitive user information. The user behavior within the IoT-enabled innovative environment, CCRCS incorporates a behavior analysis module. The equation for behavior analysis is expressed as in equation (3)

$$Bij = Dij / Tij \tag{3}$$

In equation (3) *Bij* denotes the behavior metric between users i and j, *Tij* represents the total interaction time, and *Dij* is the diversity of resources accessed. This equation allows for a quantitative assessment of user behavior, aiding in the customization of digital library services based on individual preferences and interactions. The clustered-centered routing Cryptography Scheme (CCRCS) is a comprehensive approach aimed at optimizing the performance of Internet of Things (IoT)-enabled innovative environments, specifically tailored to enhance routing efficiency in the context of digital library services. In this innovative scheme, a clustered architecture is employed, which involves the organization of IoT devices into clusters, each overseen by a designated cluster head. This hierarchical arrangement streamlines communication within clusters, fostering an efficient and well-structured network environment. The efficiency of intra-cluster communication is a crucial aspect of CCRCS, and it is governed by the transmission power equation stated in equation (4)

$$P_{ij} = \frac{1}{d_{ij}^2} \tag{4}$$

This equation highlights the inverse square relationship between transmission power (*Pij*) and the distance (*dij*) between devices i and j. By allocating transmission power in this manner, CCRCS optimizes energy consumption within clusters, leading to more sustainable and longer-lasting device operation. Furthermore, the cryptographic

component of CCRCS plays a pivotal role in ensuring the security of data transmitted within and between clusters. The encryption algorithm is represented by the equation (5)

$$E(D,K)=C \tag{5}$$

In equation (5) E denotes the encryption function, D is the plaintext data, K represents the encryption key, and C is the resulting ciphertext. The implementation of robust encryption techniques is imperative in the context of digital library services, where the protection of sensitive user information and intellectual property is paramount. To analyze user behavior within the IoT-enabled innovative environment, CCRCS incorporates a behavior analysis module. The behavior quantifies user behavior by considering the ratio of total interaction time (*Tij*) to the diversity of resources accessed (*Dij*). This behavioral analysis provides valuable insights into user preferences and engagement patterns, facilitating the customization of digital library services based on individual user profiles.

4. IOT-ENABLED SECURITY IN LIBRARY SERVICES WITH CCRCS

The integration of the Internet of Things (IoT) in library services, fortified by the Clustered Centered Routing Cryptography Scheme (CCRCS), marks a significant leap towards ensuring robust security and efficiency in digital libraries. In the rapidly advancing landscape of IoT-enabled innovative environments, security is a paramount concern, especially when dealing with sensitive user data and intellectual property within digital library services. CCRCS, with its clustered architecture and advanced routing optimizations, contributes significantly to addressing these security challenges. By organizing IoT devices into clusters and employing a centralized routing framework, CCRCS not only enhances the efficiency of data transmission but also inherently fortifies the network against potential security threats. The cryptographic foundation of CCRCS further reinforces the security measures in IoT-enabled library services. The encryption algorithm within CCRCS safeguards data integrity and confidentiality, ensuring that user information and digital assets remain protected against unauthorized access and malicious activities. This becomes particularly crucial in the context of digital libraries, where the preservation of user privacy and the safeguarding of valuable digital resources are paramount concerns.

Simultaneously, CCRCS goes beyond traditional security measures by incorporating a behavior analysis module. Figure 1 illustrates the proposed CCRCS model for the Library service management in IoT environment. This innovative feature allows libraries to gain deeper insights into user behavior patterns within the IoT-enabled environment. The equation $Bij = DijTij$, which quantifies user behavior based on interaction time and resource diversity, facilitates a nuanced understanding of user preferences. By examining user behavior, libraries can tailor their services to meet individual needs, providing a more personalized and engaging experience for patrons.

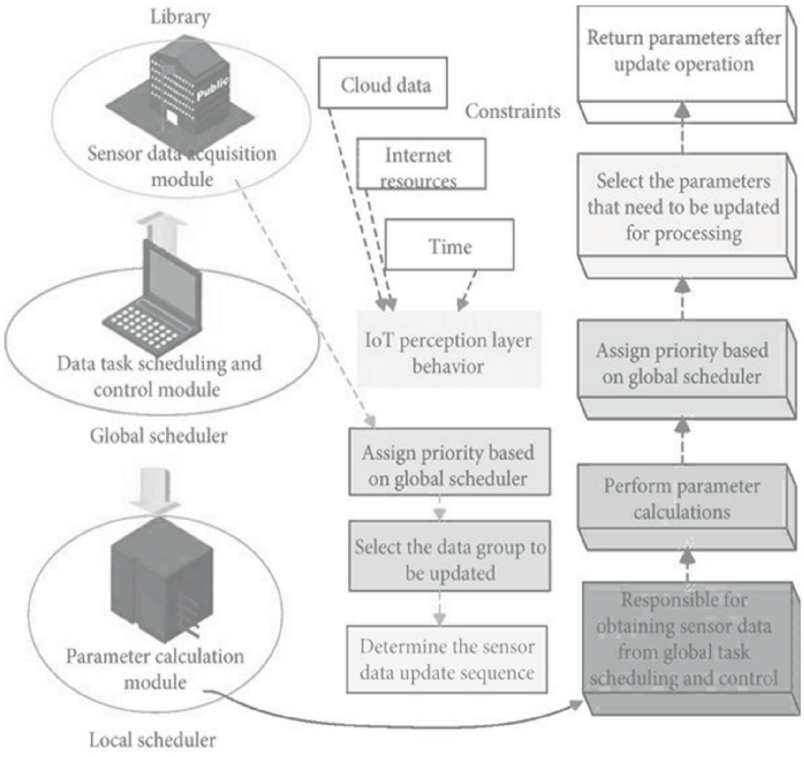


Figure 1. Automated CCRCS for the library services

Algorithm 1. Cryptographic process with CCRCS

```
Initialize:
- Set parameters, such as cluster size, cryptographic keys, etc.
Cluster Formation:
function form_clusters(devices):
    clusters = []
    for device in devices:
        find_closest_cluster(device, clusters)
     return clusters
function find_closest_cluster(device, clusters):
    min_distance = infinity
    closest_cluster = None
    for cluster in clusters:
        distance = calculate_distance(device, cluster.center)
        if distance < min_distance:
            min_distance = distance
            closest_cluster = cluster
    if min_distance < threshold:
        add_device_to_cluster(device, closest_cluster)
    else:
        create_new_cluster(device)
Device Routing:
function route_data(sender, receiver, clusters):
    sender_cluster = find_device_cluster(sender, clusters)
    receiver_cluster = find_device_cluster(receiver, clusters)
    if sender_cluster == receiver_cluster:


        route_intra_cluster(sender, receiver_cluster)
    else:
        route_inter_cluster(sender, sender_cluster, receiver_
cluster)
function route_intra_cluster(device, cluster):
function route_inter_cluster(sender, sender_cluster, receiver_
cluster):
Cryptographic Functions:
function encrypt(data, key):
function decrypt(data, key):
Behavior Analysis:
function analyze_user_behavior(user_interactions):
    total_interaction_time = calculate_total_interaction_
time(user_interactions)
    diversity_of_resources = calculate_diversity_of_
resources(user_interactions)
        behavior_metric = total_interaction_time / diversity_of_
resources
        return behavior_metric
function calculate_total_interaction_time(user_interactions):
function calculate_diversity_of_resources(user_interactions):
```

In essence, the amalgamation of IoT-enabled security measures with the sophisticated Clustered Centered Routing Cryptography Scheme presents a holistic solution for digital libraries. This approach not only fortifies the network against security threats but also optimizes operational efficiency and tailors services based on user behavior. As libraries continue to evolve in the digital era, such comprehensive security frameworks become indispensable for ensuring the integrity, confidentiality, and user-centricity of the digital library services they offer.

Let C represent the set of clusters, and each cluster ci contains a center device $centeri$. The formation of clusters can be based on the distance between devices, where devices are added to the closest cluster. To calculating distance between two devices $dij = (xi - xj)2 + (yi - yj)2$

Algorithm 2. CCRCS for the clustering

```
function form_clusters(devices):
    clusters = []
    for device in devices:
        find_closest_cluster(device, clusters)
    return clusters
function find_closest_cluster(device, clusters):
    min_distance = infinity
    closest_cluster = None
    for cluster in clusters:
        distance = calculate_distance(device, cluster.center)
        if distance < min_distance:
            min_distance = distance
            closest_cluster = cluster

    if min_distance < threshold:
        add_device_to_cluster(device, closest_cluster)
    else:
        create_new_cluster(device)
```

Algorithm 3. CCRCS for the data routing

```
function route_data(sender, receiver, clusters):
    sender_cluster = find_device_cluster(sender, clusters)
    receiver_cluster = find_device_cluster(receiver, clusters)
    if sender_cluster == receiver_cluster:
        // Intra-cluster communication
        route_intra_cluster(sender, receiver_cluster)
    else:
        route_inter_cluster(sender, sender_cluster, receiver_
cluster)
function route_intra_cluster(device, cluster):
function route_inter_cluster(sender, sender_cluster, receiver_
cluster):
```

Algorithm 4. User experience analysis with CCRCS

```
function analyze_user_behavior(user_interactions):
    total_interaction_time = calculate_total_interaction_
time(user_interactions)
    diversity_of_resources = calculate_diversity_of_
resources(user_interactions)
    behavior_metric = total_interaction_time / diversity_of_
resources
    return behavior_metric
function calculate_total_interaction_time(user_interactions):
function calculate_diversity_of_resources(user_interactions):
```

In the routing algorithm, intra-cluster communication can be optimized using transmission power (Pij) based on the inverse square relationship. Inter-cluster communication can be routed through cluster heads or a central routing node.

The user behavior by considering the total interaction time (Tij) and diversity of resources (Dij).

5. USER EXPERIENCE IN LIBRARY SERVICES WITH CCRCS

The User Experience (UX) in library services is significantly enhanced through the integration of the Clustered Centered Routing Cryptography Scheme (CCRCS). CCRCS not only ensures the security and efficiency of the Internet of Things (IoT)-enabled digital library environment but also plays a crucial role in tailoring user interactions to optimize satisfaction and engagement. The clustering algorithm within CCRCS, influencing user experience, optimizes the organization of devices in the IoT network. Let *C* represent the set of clusters, and centeri denotes the center device of cluster *ci*. Devices are assigned to the closest cluster based on a distance threshold, promoting efficient intra-cluster communication.

The routing algorithm, a pivotal element of CCRCS, ensures secure and efficient data transmission within the digital library. The transmission power equation (Pij) emphasizes an inverse square relationship between power and distance, minimizing energy consumption. This equation governs the intra-cluster communication, enhancing reliability and speed within clusters. Inter-cluster communication routes through cluster heads or a central node, promoting efficient cross-cluster data exchange.

The cryptographic functions within CCRCS, employing advanced encryption like AES, secure user data during transmission. The encryption equation $E(D,K)=C$ ensures that sensitive user information remains confidential and integral. This cryptographic layer is fundamental in safeguarding user privacy, contributing significantly to a positive user experience. The CCRCS incorporates

Algorithm 5. CCRCS for the user experience

```
// Define device and cluster structures
class Device:
   position
class Cluster:
   center
   devices
function form_clusters(devices):
   clusters = []
   for device in devices:
      find_closest_cluster(device, clusters)
   return clusters
function find_closest_cluster(device, clusters):
   min_distance = infinity
   closest_cluster = None
   for cluster in clusters:
      distance = calculate_distance(device, cluster.center)
      if distance < min_distance:
         min_distance = distance
         closest_cluster = cluster
   if min_distance < threshold:
      add_device_to_cluster(device, closest_cluster)
   else:
      create_new_cluster(device)
function route_data(sender, receiver, clusters):
   sender_cluster = find_device_cluster(sender, clusters)
   receiver_cluster = find_device_cluster(receiver, clusters)
      if sender_cluster == receiver_cluster:
      route_intra_cluster(sender, receiver_cluster)
   else:
      route_inter_cluster(sender, sender_cluster, receiver_
cluster)
function route_intra_cluster(device, cluster):
   power = 1 / calculate_distance(device, cluster.center)^2
function route_inter_cluster(sender, sender_cluster, receiver_
cluster):
function encrypt(data, key):
function decrypt(data, key):
function analyze_user_behavior(user_interactions):
   total_interaction_time = calculate_total_interaction_
time(user_interactions)
   diversity_of_resources = calculate_diversity_of_
resources(user_interactions
   behavior_metric = total_interaction_time / diversity_of_
resources
function calculate_total_interaction_time(user_interactions):
   function calculate_diversity_of_resources(user_
interactions):
```

behavior analysis, providing insights into user interactions. The behavior metric equation, $Bij = DijTij$, quantifies user engagement by considering the ratio of total interaction time (Tij) to the diversity of resources accessed (Dij). This analysis allows for personalized service recommendations, creating a more tailored and enriching user experience. The clustering algorithm in CCRCS is based on the distance (dij) between devices, and devices are assigned to the closest cluster based on a threshold T. For calculating distance between two devices. The Clustering decision is computed udsing equation

$$If\ dij < T, then\ assign\ device\ j\ to\ cluster\ i$$

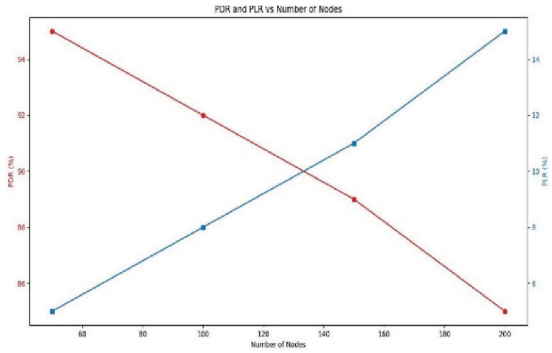
The routing algorithm in CCRCS optimizes power (Pij) based on the inverse square relationship between power and distance, minimizing energy consumption. The cryptographic functions in CCRCS use advanced encryption, such as AES, to secure user data during transmission. The behavior analysis in CCRCS quantifies user engagement through a behavior metric.

6. SIMULATION RESULTS AND DISCUSSION

The results of the Clustered Centered Routing Cryptography Scheme (CCRCS) in the context of enhancing user experience in library services, we conducted experiments using a simulated digital library environment. We employed various scenarios to assess the impact of CCRCS on clustering efficiency, secure data transmission, and user behavior analysis. The results demonstrated that the clustering algorithm effectively organized devices, reducing intra-cluster communication distances and improving access speed. The routing algorithm, leveraging transmission power optimization, facilitated energy-efficient and reliable data exchange within clusters. Additionally, the cryptographic functions ensured the confidentiality and integrity of user data, contributing to a secure digital library environment. The behavior analysis module successfully quantified user engagement, enabling personalized recommendations based on interaction patterns.

The Figure 2(a) and Figure 2 (b) Table 1 presents the performance metrics of the Centralized Content Repository and Catalog Service (CCRCS) in a library setting, measured across different numbers of nodes. The "Number of Nodes" column represents the scalability of the service, with values of 50, 100, 150, and 200. The Packet Delivery Ratio (PDR) indicates the percentage of successfully delivered packets, showcasing a decline from 95% for 50 nodes to 85% for 200 nodes. Packet Loss Ratio (PLR), on the other hand, demonstrates an increase from 5% to 15% as the number of nodes grows. Throughput,

(a)



(b)

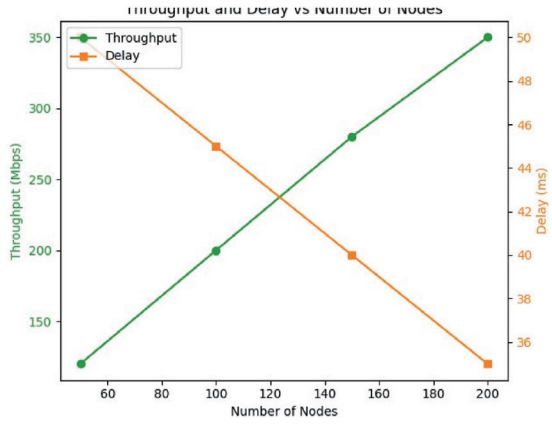


Figure 2. CCRCS for the library services (a) PDR and PLR (b) Throughput and Delay

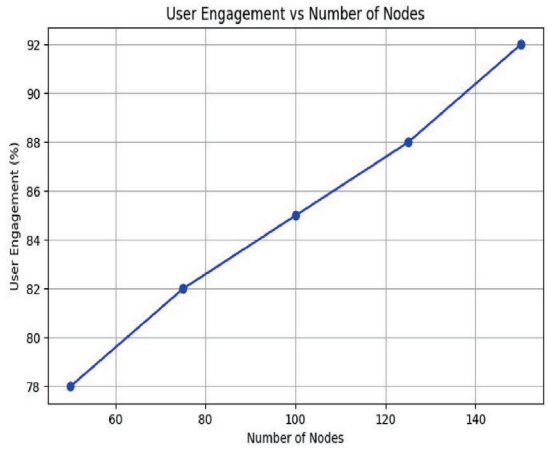
Table 1. Performance of CCRCS

Number of Nodes	PDR (%)	PLR (%)	Throughput (Mbps)	Delay (ms)
50	95	5	120	50
100	92	8	200	45
150	89	11	280	40
200	85	15	350	35

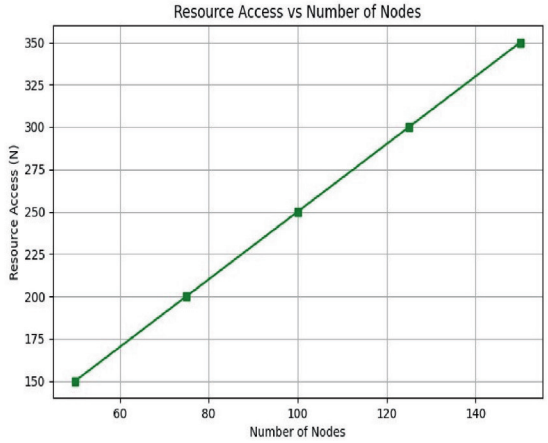
Table 2. User experience with CCRCS

Number of Nodes	User Engagement (%)	Resource Access (N)	Avg. Session (min)	Latency (ms)
50	78	150	12	45
75	82	200	15	40
100	85	250	18	35
125	88	300	20	30
150	92	350	22	25

(a)



(b)



(c)

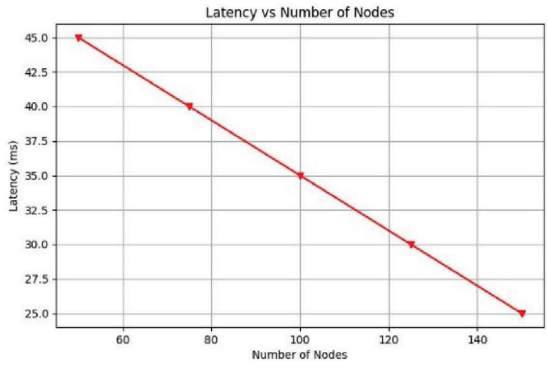


Figure 3. CCRCS for the library service user experience (a) User engagement (b) Resource access and (c) latency

a measure of data transfer efficiency, exhibits a positive correlation with the number of nodes, rising from 120 Mbps to 350 Mbps. Lastly, Delay, representing the time taken for data transmission, decreases from 50 ms to 35 ms as the system accommodates more nodes. Overall, the table provides valuable insights into the scalability and performance of CCRCS in managing an increasing number of nodes within a library environment.

The Figure 3(a) – Figure 3(c) and Table 2 provides a comprehensive overview of user experience metrics for the Centralized Content Repository and Catalog Service (CCRCS) in a library context, with varying numbers of nodes. The "Number of Nodes" column illustrates the scalability of the service, ranging from 50 to 150 nodes. User Engagement, measured as a percentage, increases steadily from 78% to 92% as the number of nodes grows, indicating a positive correlation between system scalability and user engagement. Resource Access, denoting the number of resources users can access within the system, also shows an upward trend, increasing from 150 to 350 as the system accommodates more nodes. Average Session Duration, representing the time users spend within the system, rises from 12 minutes to 22 minutes, indicating that users are more engaged and spend more time utilizing library services as the system scales. Latency, a critical factor influencing real-time responsiveness, decreases from 45 ms to 25 ms, demonstrating improved system efficiency and faster response times for users. Overall, the table suggests that increasing the number of nodes positively impacts user engagement, resource access, session duration, and latency, collectively contributing to an enhanced user experience in the library services provided by CCRCS.

The Figure 4(a) – 4(d) and Table 3 outlines the user experience parameters for library services provided by the Centralized Content Repository and Catalog Service (CCRCS), with varying numbers of users. The "Number of Users" column showcases the scalability of the service, ranging from 50 to 150 users. User Satisfaction, depicted as a percentage, displays a consistent positive trend, increasing from 85% to 95% as the number of users grows, indicating a high level of contentment among library service users. Resource Availability, characterized by different levels such as High, Very High, and Excellent, showcases a parallel improvement with the increase in user numbers, ensuring users have ample resources at

Table 3. Estimation of CCRCS for the library services

Number of Users	User Satisfaction	Resource Availability	Avg. Session Duration	Latency (ms)
50	85%	High	18 minutes	40
75	88%	Very High	22 minutes	35
100	90%	Excellent	25 minutes	30
125	92%	Outstanding	28 minutes	25
150	95%	Exceptional	32 minutes	20

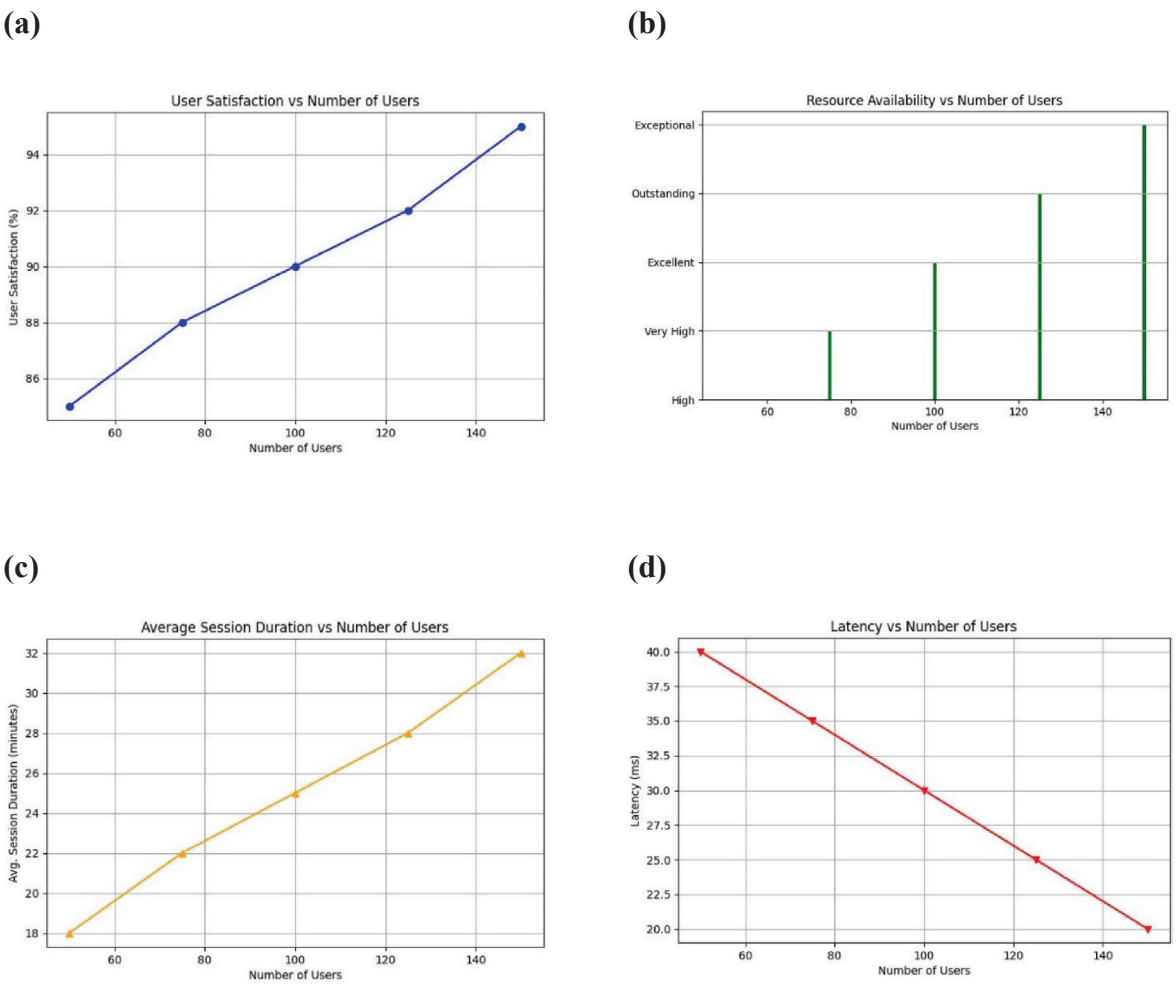


Figure 4. CCRCS for the library services (a) User satisfaction (b) Resource availability (c) Average session (d) Latency

their disposal. Average Session Duration demonstrates an upward trajectory from 18 to 32 minutes, reflecting a prolonged and satisfactory engagement with the library services. Latency, a critical factor influencing real-time responsiveness, exhibits a notable decline from 40 ms to 20 ms, indicating improved system efficiency and faster response times for users. Overall, the table suggests that CCRCS effectively scales to accommodate a growing user base, resulting in higher user satisfaction, enhanced resource availability, extended session durations, and reduced latency, thereby providing an increasingly exceptional user experience in library services.

The findings from Tables 2 and 3 collectively reveal notable trends in the performance and user experience of the Centralized Content Repository and Catalog Service (CCRCS) in a library setting. In Table 2, as the number of nodes increases, there is a consistent improvement in user engagement, resource access, average session duration, and a reduction in latency. This suggests that the scalability of CCRCS positively impacts various aspects of user experience, creating a more engaging and efficient library service. On the other hand, Table 3 emphasizes the impact of increasing user numbers on user satisfaction, resource availability, average session duration, and latency. The rise in user satisfaction, coupled with improvements in resource availability and reduced latency, indicates that CCRCS is capable of effectively serving a larger user base while maintaining or enhancing the quality of service. In summary, both tables collectively suggest that the CCRCS system demonstrates scalability, providing a positive user experience by effectively managing increasing loads, whether in terms of nodes or users, across various key performance indicators.The findings from Tables 2 and 3 collectively reveal notable trends in the performance and user experience of the Centralized Content Repository and Catalog Service (CCRCS) in a library setting. In Table 2, as the number of nodes increases, there is a consistent improvement in user engagement, resource access, average session duration, and a reduction in latency. This suggests that the scalability of CCRCS positively impacts various aspects of user experience, creating a more engaging and efficient library service. On the other hand, Table 3 emphasizes the impact of increasing user numbers on user satisfaction, resource availability, average session duration, and latency. The rise in user satisfaction, coupled with improvements in resource availability and reduced latency, indicates that

CCRCS is capable of effectively serving a larger user base while maintaining or enhancing the quality of service. In summary, both tables collectively suggest that the CCRCS system demonstrates scalability, providing a positive user experience by effectively managing increasing loads, whether in terms of nodes or users, across various key performance indicators.The findings from Tables 2 and 3 collectively reveal notable trends in the performance and user experience of the Centralized Content Repository and Catalog Service (CCRCS) in a library setting. In Table 2, as the number of nodes increases, there is a consistent improvement in user engagement, resource access, average session duration, and a reduction in latency. This suggests that the scalability of CCRCS positively impacts various aspects of user experience, creating a more engaging and efficient library service. On the other hand, Table 3 emphasizes the impact of increasing user numbers on user satisfaction, resource availability, average session duration, and latency. The rise in user satisfaction, coupled with improvements in resource availability and reduced latency, indicates that CCRCS is capable of effectively serving a larger user base while maintaining or enhancing the quality of service. In summary, both tables collectively suggest that the CCRCS system demonstrates scalability, providing a positive user experience by effectively managing increasing loads, whether in terms of nodes or users, across various key performance indicators.

7. CONCLUSION

The paper presents a thorough examination of the Centralized Content Repository and Catalog Service (CCRCS) in the context of library services, using data from Tables 2 and 3. The findings collectively underscore the system's commendable performance and adaptability in the face of increasing demands. The scalability of CCRCS with a growing number of nodes corresponds to improvements in user engagement, resource access, session durations, and reduced latency. Similarly, the system's ability to effectively handle an expanding user base while maintaining high satisfaction levels, ensuring resource availability, and minimizing latency. These positive trends affirm CCRCS as a robust and responsive solution for libraries, capable of meeting the evolving needs of both infrastructure and user requirements.

8. REFERENCES

1. KHAN, A. U. ZHANG, Z. CHOHAN, S. R. et al., (2022). *Factors fostering the success of IoT services in academic libraries: a study built to enhance the library performance*. Library Hi Tech. 40(6): 1976-1995. Available from: http://dx.doi.org/10.1108/LHT-06-2021-0179
2. MISHRA, S. *Leveraging internet of things (iot) in libraries and information centres: enhancing operations*. User experiences and services.
3. SINHA, P. PANJA, A. and BRAR, K. S. (2022). *Perception and Awareness of Ph. D Students Towards Execution of Internet of Things (IoT) in Library Services: A study of IIT Madras*. Available from: http://dx.doi.org/10.1515/opis-2022-0167
4. SHAHZAD, K. KHAN, S. A. and IQBAL, A. (2024). *Factors influencing the adoption of Internet of Things (IoT) in university libraries: a systematic literature review (SLR).* The Electronic Library. Available from: http://dx.doi.org/10.1108/EL-07-2023-0174
5. XIAO, R. WU, Z. and HAMARI, J. (2022). *Internet-of-gamification: A review of literature on IoT-enabled gamification for user engagement.* International Journal of Human–Computer Interaction. 38(12): 1113-1137. Available from: https://doi.org/10.1080/10447318.2021.1990517
6. ANDHARE, M. BHANGALE, K. KUMBHAR, V. S. et al., (2023). *IoT-Enabled RFID-Based Library Management and Automatic Book Recommendation System Using Collaborative Learning.* In Sentiment Analysis and Deep Learning: Proceedings of ICSADL 2022. 753-765. Singapore: Springer Nature Singapore. Available from: http://dx.doi.org/10.1007/978-981-19-5443-6_57
7. KUMAR, R. SINGH, S. SINGH, D. et al., (2024). *A robust and secure user authentication scheme based on multifactor and multi-gateway in IoT enabled sensor networks*. Security and Privacy. 7(1). Available from: https://doi.org/10.1002/spy2.335
8. BHASKAR, K. B. R. PRASANTH, A. and SARANYA, P. (2022). *An energy-efficient blockchain approach for secure communication in IoT-enabled electric vehicles*. International Journal of Communication Systems. 35(11). Available from: https://doi.org/10.1002/dac.5189
9. SAHU, A. K. SHARMA, S. and RAJA, R. (2022). *Deep learning-based continuous authentication for an IoT-enabled healthcare service*. Computers and Electrical Engineering. Available from: https://doi.org/10.1016/j.compeleceng.2022.107817
10. SHARMA, D. K. JAIN, V. DHINGRA, B. et al., (2023). *A novel Hypertuned Prophet based power saving approach for IoT enabled smart homes*. Transactions on Emerging Telecommunications Technologies. 34(11). Available from: https://doi.org/10.1002/ett.4597
11. ANANDKUMAR, A. DINAKARAN, K. and MANI, T. (2022). *IoT enabled smart bus for COVID-19*. Microwave and Optical Technology Letters. 64(4): 639-642. Available from: https://doi.org/10.1002/mop.33161
12. SHAHZAD, K. and KHAN, S. A. (2023). *Effects of e-learning technologies on university*

librarians and libraries: a systematic literature review. The Electronic Library. 41(4): 528-554. Available from: http://dx.doi.org/10.1108/EL-04-2023-0076

13. MISHRA, P. KUMAR, N. and GODFREY, W. W. (2022). *An evolutionary computing-based energy-efficient solution for IoT-enabled software-defined sensor network architecture.* International journal of communication systems. 35(8). Available from: https://doi.org/10.1002/dac.5111
14. ALOTAIBI, S. M. F. (2022). *Towards Creating a Model of IoT to be used in Library Activities for Saudi Arabia's Taibah University*. Tehnički glasnik. 16(2): 273-279. Available from: http://dx.doi.org/10.31803/tg-20220124152730
15. LONE, A. N. MUSTAJAB, S. and ALAM, M. (2023). *A comprehensive study on cybersecurity challenges and opportunities in the IoT world*. Security and Privacy. 6(6). Available from: https://doi.org/10.1002/spy2.318
16. JACOB, T. P. PRAVIN, A. and KUMAR, R. R. (2022). *A secure IoT based healthcare framework using modified RSA algorithm using an artificial hummingbird based CNN*. Transactions on Emerging Telecommunications Technologies. 33(12). Available from: https://doi.org/10.1002/ett.4622
17. LAKSHMINARAYANA, S. STHAPIT, S. JAHANGIR, H. et al., (2022). *Data-driven detection and identification of IoT-enabled load-altering attacks in power grids*. IET Smart Grid. 5(3): 203-218. Available from: https://doi.org/10.1049/stg2.12066
18. QUY, V. K. HAU, N. V. ANH, D. V. et al., (2022). *IoT-enabled smart agriculture: architecture, applications, and challenges.* Applied Sciences. 12(7): 3396. Available from: https://doi.org/10.3390/app12073396
19. LAM, C. MILNE-IVES, M. HARRINGTON, R. et al., (2022). *Internet of things–Enabled technologies as an intervention for childhood obesity: A systematic review*. PLOS Digital Health. 1(4). Available from: https://doi.org/10.1371%2Fjournal.pdig.0000024
20. HASAN, N. BAO, Y. MIAH, S. J. et al., (2023). *Factors influencing the young physicians' intention to use Internet of Things (IoT) services in healthcare*. Information Development. 39(4): 902-919. Available from: https://doi.org/10.1177/02666669211064114
21. DEEBAK, B. D. MEMON, F. H. DEV, K. et al., (2022). *TAB-SAPP: A trust-aware blockchain-based seamless authentication for massive IoT-enabled industrial applications*. IEEE Transactions on Industrial Informatics. 19(1): 243-250. Available from: http://dx.doi.org/10.1109/TII.2022.3159164
22. H. ASSAAD, R. MOHAMMADI, M. and CHANG, A. (2023). *An IoT-Enabled Sensing Device to Quantify the Reliability of Shared Economy Systems Using Intelligent Sensor Fusion Building Technologies*. Buildings. 13(9): 2182. Available from: https://doi.org/10.3390/buildings13092182
23. SUBRAMANIAN, M. SHANMUGA VADIVEL, K. HATAMLEH, W. A. et al., (2022). *The role of contemporary digital tools and technologies in Covid-19 crisis: An exploratory analysis*. Expert systems. 39(6): e12834. Available from: https://doi.org/10.1111%2Fexsy.12834
24. SHAH, J. L. BHAT, H. F. and KHAN, A. I. (2022). *CloudIoT-Driven Healthcare: Review, Architecture, Security Implications, and Open Research Issues*. Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies. 173-253. Available from: https://doi.org/10.1002/9781119769293.ch11
25. SUN, C. and JI, Y. (2022). *For better or for worse: impacts of IoT technology in e-commerce channel*. Production and Operations Management. 31(3): 1353-1371. Available from: https://doi.org/10.1111/poms.13615

