Museum Design and Simulation Research Based on Embedded Systems and Symmetric Encryption Privacy Protection

Si Li
School of Information Engineering
Liaoning Institute of Science and Engineering, China
lisi0928@hotmail.com

Hui Dai
Academic Affairs Office
Liaoning Institute of Science and Engineering, China
daihui_dh@hotmail.com

Xiaoyuan Li
College of Fine Arts and Designn
Guangdong Vocational College of Arts, China
Xiaoyuan_Li20@outlook.com

Yihua Wu
College of Fine Arts and Design
Guangdong Vocational College of Arts, China
WuYihua_wyh@outlook.com

Abstract: *Museum design plays an important role in preserving the cultural heritage information. The museum has been designed by considering various factors such as layout, technique, and accessibility because it must be user-friendly and secure. The museum holds various sensitive information that may be accessed by unauthorized users, which leads to privacy, confidentiality and integrity issues. The existing cryptographic techniques are vulnerable to the long-term sustainability requirement to protect and create access control issues. A novel lightweight symmetric encryption technique, termed Symmetric and Lightweight Encryption Methodology (SLEM), is introduced to secure data in embedded museum environments. The study uses the ChaCha20 encryption algorithm with Role-Based Access Control (RBAC) to provide security to sensitive data. During this process, nonce and keystream blocks are utilized to get the cipher text, which ensures the security of the data. In addition, lightweight encryption and end-to-end encryption processes are integrated with chacha20 to improve overall data privacy. Then, the microcontroller is embedded with the encryption procedure, simplifying the encryption and decryption delay. Then, the system efficiency is evaluated using experimental results.*

Keywords: *Museum design, ChaCha20 encryption, lightweight encryption, end-to-end encryption, keystream block, data privacy, security and confidentiality.*

Received March 04, 2025; accepted December 18, 2025
https://doi.org/10.34028/iajit/23/4/10

1. Introduction

Museum design [21] is essential in creating innovative and educational visitor experiences. The design includes several factors: exhibition layout, foot traffic facilities, technologies, and accessibilities. Among the various aspects, the exhibition is the most crucial factor in which designers and curators [3] cooperate to interpret and present the collections in the museum. The museum design has various themes, text panels, and lighting settings to improve the overall appearance. The design of a museum's architecture determines the fundamental arrangement and atmosphere of the area. The building design [9] incorporates lines of view, light management, and layout optimization to enhance the visitor experience. The embedded systems [7] are highly utilized in this modern museum design because they give the optimal solution for sensitive artefacts. The microcontroller embedded systems [15] create innovative systems consisting of motion sensors, touch screens and optimal input devices like visual and audio components. In addition, embedded systems are applied in concepts related to connectivity, automation, monitoring, accessibility, power management and location awareness in museum design [14]. Museums utilize integrated technology to create immersive exhibit experiences that inspire and educate visitors also optimize museum operations.

Museums must maintain their visitors' confidentiality [4] and the data about their collections. As public institutions, museums gather personal data from visitors, including names, contact information, and ticket transactions. Museums also own databases that store confidential information on objects, benefactors, origin, and insurance appraisals. Enforcing privacy [11] safeguards is essential to safeguard sensitive data and deter unlawful access or monitoring. Incorporating strong encryption, stringent access restrictions, and comprehensive cybersecurity protections [17] is vital in museum design to establish visitor confidence, comply with laws, and mitigate liability. Visitors anticipate their privacy will be honoured, particularly as museums integrate additional digital interaction technologies. By prioritizing privacy from the outset of the design process, museums may establish environments centred around teaching and community while protecting

sensitive information and individual rights. Implementing a robust privacy protection system [18] indicates a museum's dedication to ethical data management. To ensure that privacy policies are not only conceptual but also enforceable in technical systems, encryption mechanisms become essential tools in upholding data confidentiality and integrity. Designers must consider several restrictions when integrating encryption [24] into museum exhibitions and systems, especially when balancing user experience with security requirements. Several encryption schemes require significant computer resources, resulting in undesirable delays for real-time interactive displays. Embedded devices with limited resources may not have the processor power and memory capacity to handle complicated cryptographic operations. In resource-constrained environments such as museums, generating, distributing, and storing cryptographic keys presents technical challenges due to limited computational and memory capacities [20]. Furthermore, it is essential to note that the current procedures, which are considered immune to decryption, may eventually be vulnerable to future cryptanalysis or quantum algorithms during the duration of a museum system. Encrypting the actual material while leaving the metadata exposed reveals crucial patterns. Hence, it is imperative for museum designers to thoroughly evaluate encryption alternatives based on their performance, usability, and long-term sustainability requirements to safeguard exhibit interaction, collecting data, and visitor privacy [10]. Achieving optimal equilibrium among security, accessibility, and practicality is crucial. Museums must guarantee that implementing encryption technologies promotes confidence among visitors and stakeholders while avoiding any detrimental influence on their experiences towards the system's capacity [5].

This paper proposes a novel Symmetric and Lightweight Encryption Methodology (SLEM), specifically designed by the authors for real-time, low-latency data protection in embedded museum systems. By implementing selective, symmetric, and lightweight encryption, museums can efficiently and effectively preserve sensitive data while still enabling interactive exhibitions in a scalable manner. The symmetric ChaCha20 encryption algorithm provides significantly higher data transfer rates than asymmetric encryption, meeting the demands of real-time multimedia networks. Lightweight ciphers are specifically designed to operate efficiently on resource-constrained devices such as embedded systems and Internet of Things (IoT) platforms commonly utilized in modern museum applications [13]. Their simple designs facilitate integration, especially on endpoints with limited resources. Certain lightweight cryptosystems also offer resistance against prospective quantum computing threats. These solutions enhance power efficiency while reducing the hazards of vendor lock-in through improved interoperability. Significantly, lightweight symmetric encryption enables museums to enhance user involvement through immersive exhibitions while safeguarding privacy across various digital interaction platforms. The feasibility of integrating extensive encryption into museum architecture is made possible by the accessibility, efficiency, and simplicity of these approaches on a large scale. Then the overall objective of this work is listed as follows.

- To develop a simulation-based framework that integrates embedded systems into modern museum infrastructures for secure and efficient data management.
- To implement and evaluate the ChaCha20 cipher as a lightweight symmetric encryption algorithm suitable for real-time data protection in resource-constrained museum devices.
- To ensure privacy preservation and low-latency performance by optimizing the cryptographic workflow within interactive museum environments.

The rest of this paper is organized as follows. The second part presents a comprehensive literature review and outlines the research methods. Section 3 discusses the research plan, methods used, and data processing. Section 4 talks about what the analysis found. Section 5 has the conclusion and plans for the future.

2. Related Work

Shang and Li [19] applied the Heuristic Data Management and Protection Approach (HDMP) to manage digital Chinese cultural information. This study addresses reliability and robustness issues while protecting cultural information. Cultural heritage information is processed using heuristic operations that ensure protection and promising results.

Zhao *et al*. [25] recommended a Blockchain Encryption Interaction Approach (BEIA) to manage the museum collections. The gathered digital museum information is included in the Museum Art Exchange Protocol (MAXP) to eliminate illegal fundraising, fraud and smuggling. The SM2 elliptic curve and Diffie-Hellman algorithm are applied on the sender side to encrypt the information. The encrypted information is stored in the third-party service provider, and the decryption is performed using blockchain approaches that ensure data privacy. Details from the Natural History Beijing Museum and Planetarium were used to evaluate the system efficiency during the analysis. The blockchain approach ensures security feasibly. The secured digital collection in the museums provides significant promotions to the heritages.

Wang *et al*. [23] protected museum digital property rights using blockchain technology. This work uses the digital authorization mechanism to protect the museum records from unauthorized users. The protection mechanism works with the business model and signature time stamp to ensure traceability,

decentralization and verifiability issues. In addition, the blockchain mechanism promotes data security rights and addresses financial problems successfully.

Vayadande *et al*. [22] recommended cryptography techniques to manage museum and monument ticketless booking system security. The system intends to address the scalability, ticket and physical token-related issues and ensures integrity, authentication and confidentiality. The Advance Encryption Standard (AES) 256 encryption algorithm achieves the objectives. Blockchain and digital certificates are applied to manage the anti-tempering and authentication during this process. The developed solution effectively tackles significant scalability, security, and efficiency constraints compared to conventional manual methods.

Jingwen and Lin [12] explored ethical dilemmas that arise from processing large-scale data collected from museum visitors. It emphasizes issues such as vulnerabilities of privacy and the need for informed consent in the context of substantial gathering of personal data. The authors contend that implementing appropriate data governance is necessary to protect the rights of visitors. Big data applications advocate for transparent regulations, consent processes, and accountability. Collectively, the literature provides a helpful viewpoint on the ethical management of visitor information at museums.

The study of Ferrato *et al*. [6] investigated the utilization of deep learning techniques to collect museum visitor data in private. A You Only Look Once (YOLO)-based approach monitors and analyses visitors, capturing data on their whereabouts, groupings, and the amount of time they occupy in a specific area. The system was evaluated in a museum and demonstrated a monitoring accuracy of over 90% using computer vision analysis. This exemplifies the capacity of deep learning to gather geographical, temporal, and social data to guide museum activities. The inconspicuous method surpasses the constraints of intrusive sensing for behavioural research.

Hu *et al*. [8] introduced a 3D virtual simulation system to offer museum previews and online experiences. A case study on the Palace Museum is implemented utilizing Unity3D, and the technology uses advanced techniques to recreate architectural structures, objects, and environments, capturing intricate details of textures and lighting. The questionnaire findings indicate user satisfaction and enthusiasm for the 3D virtual museum. The study demonstrates the potential for improving museum tourism through interactive visualization techniques.

Acheampong *et al*. [2] proposed a cryptographic solution to secure virtual assets in immersive environments using digital signatures and hash algorithms. The system uses Rivest-Shamir-Adleman (RSA-2048) for signing and SHA-256 hashing to prevent tampering and forgery. The signing process is efficient, with a minimal memory footprint and near-instantaneous verification times. The system also detects unauthorized modifications with a 100% detection rate. Although RSA may be vulnerable to quantum computing, its modular design ensures crypto-agility, allowing for the integration of quantum-resistant algorithms.

Abed *et al*. [1] stated that sensor-equipped smart devices drove the development of Cyber-Physical-Social Systems (CPSSs) to study CPS-human interaction. Virtual, physical, and social spaces make up CPSSs. An implementation of CPSSs, the metaverse includes computer systems, Artificial Intelligence (AI), computer vision, image processing, mixed reality, augmented reality, extended reality, physical systems, controlled objects, and human interaction. Weak security and heavy calculation plague CPSS identification. New Secure Lightweight Authentication protocol in CPSSs (SLACPSSs) offers secure communication between platform servers and users and avatar interactions. The code is lightweight and secure, according to security analysis. Table 1 is the summary of related work in museum data protection and smart system.

Table 1. Summary of related work in museum data protection and smart systems.

Authors	Objective	Findings	Research gap
Shang and Li [19]	Protect chinese cultural information	Ensured robustness and reliability in cultural heritage data protection	No integration with real-time embedded or encryption systems
Zhao *et al*. [25]	Secure digital museum collections	Achieved secure collection access and data privacy via decentralized encryption	High computational overhead; lacks focus on lightweight devices
Wang *et al*. [23]	Safeguard digital property rights in museums	Enabled traceability and verification while addressing financial data issues	Not targeted for embedded systems or real-time encryption scenarios
Vayadande *et al*. [22]	Secure museum ticketless systems	Ensured authentication and integrity in e-ticket systems	Lacks integration with embedded museum infrastructures
Jingwen and Lin [12]	Address ethical issues in museum visitor data	Emphasized importance of consent and transparent data policies	Does not address secure system-level implementations
Ferrato *et al*. [6]	Privately collect visitor behavioral data	Achieved over 90% accuracy in unobtrusive monitoring	No integrated privacy-preserving encryption or secure data storage used
Hu *et al*. [8]	Offer virtual museum experience	Demonstrated user satisfaction and potential for virtual tourism	No emphasis on secure data storage, transmission, or user privacy

While previous studies have primarily addressed museum data protection through blockchain, cryptographic ticketing systems, or virtual environments, none have integrated symmetric

lightweight encryption with embedded system design for real-time museum data privacy. Unlike existing approaches that focus on centralized architectures or computationally intensive encryption, our proposed methodology emphasizes low-latency, energy-efficient security tailored for embedded museum infrastructures-filling a crucial gap in both performance and applicability.

3. Symmetric and Lightweight Encryption Methodology (SLEM) for Secure Musume Design

The primary objective of SLEM is to provide a comprehensive encryption framework specifically designed to satisfy the performance, privacy, and data protection requirements of digital museum systems. The SLEM approach utilizing high-speed ChaCha20 encryption to safeguard sensitive collection databases and cultural objects. Efficient ciphers designed for embedded devices and IoT enable widespread encryption without affecting usability or causing delays. SLEM employs a strategic approach by targeting essential data, such as visitors' personal information and valuable collections, instead of applying encryption across the board. Furthermore, it incorporates permission processes and promotes transparency about data practices to establish confidence among visitors. Hardware acceleration, compatible standards, and simplified integration make implementing comprehensive and effective encryption throughout an entire museum easier. A Hardware Security Module (HSM) is a dedicated physical device that securely stores cryptographic keys and performs encryption operations.Then, the overall working process is illustrated in Figure 1.

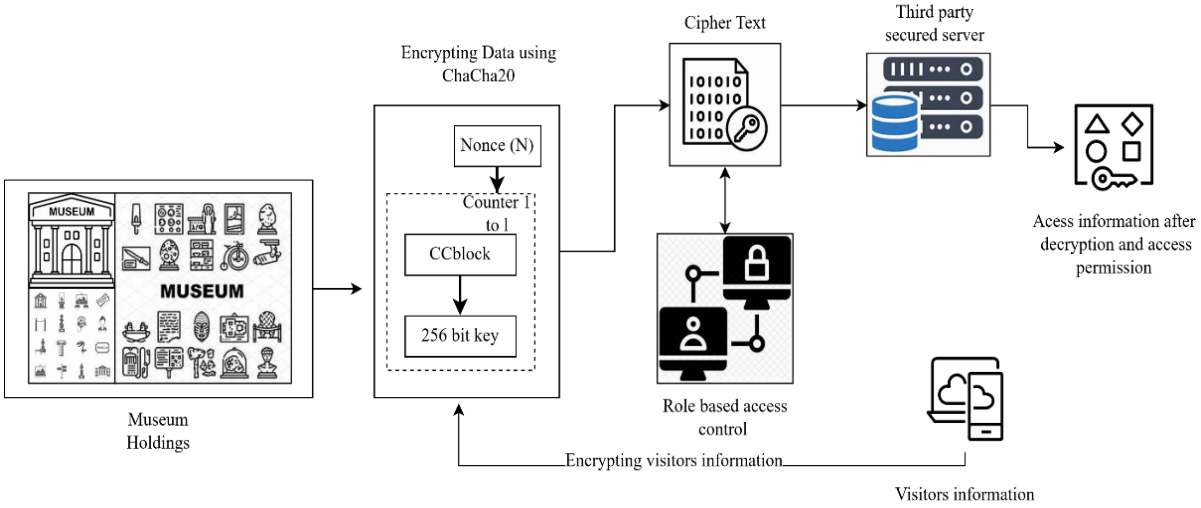


Figure 1. Overall working structure of SLEM-based museum design.

3.1. Protect Sensitive Museum Data Using the Symmetric Encryption Algorithm

The museum consists of several comprehensive pieces of information such as item name, inventory numbers, origin, acquisition data, condition, artefact dimensions, material information, monetary details and associated documents. This information is important for managing and documenting museum collections. Museum data can be intercepted by unauthorized entities during transmission, which may lead to serious privacy and confidentiality breaches. Therefore, museum holding should be encrypted to manage their originality; in this study, the chacha20 encryption algorithm is utilized. ChaCha20 should serve as the primary symmetric encryption technique for protecting sensitive collected data at rest and in transit. ChaCha20 was chosen because of its fast speed, compact code footprint, suitability for embedded devices, and resistance to cryptanalysis attempts. Databases in museum management systems that hold item records, provenance, values, insurance information, and other secret data should be fully encrypted with ChaCha20 and 256-bit keys.

Transport Layer Security (TLS) using ChaCha20 cipher suites for encrypting data in motion while establishing network connections to collection databases. TLS will be utilized via Application Programming Interface (API) access and web interfaces. All data stored on the servers and storage that has been encrypted using ChaCha20 at the filesystem level. Dedicated cryptographic accelerator cards will accelerate cryptographic workloads on servers. Mobile collection management applications will keep data that has been synchronized locally in application sandboxes that are encrypted and secured by device Trusted Platform Module (TPM).The TPM is a dedicated security chip embedded in computing devices to securely store cryptographic keys, digital certificates, passwords, and other sensitive data. It ensures hardware-based protection, enabling functions like secure boot, measured system integrity, and data encryption by preventing unauthorized access or tampering-even if the operating system is compromised.The process of synchronizing

communications with core databases will involve encrypting the data from the beginning to the conclusion. The encrypted data was accessed using the multi-factor authentication access control. Granular role-based access will restrict data visibility to only those people requiring it for their work obligations. Auditing capabilities will log all access attempts and actions under authenticated sessions for accountability. Encryption keys must be produced, cycled, and backed up in a safe manner using a robust cryptoprocessor. Consider *P* is the museum details (plain text) that has *n* length in bytes. The encryption algorithm takes 256-bit key *K*, 32-bit block counter *i* and 96-bit nonce *N*. Initially, the key stream block (K_i) is generated with the help of the Chacha20 key schedule, is defined as K_i=chacha20 (*k, N, i*). The generated K_i is Exclusive OR (XOR) with *P* (plain text) to create the cipher text *C* which is defined in Equation (1).

$$C_i = P_i \oplus K_i \; ; i = 1 \; to \; n/64 \tag{1}$$

In Equation (1), the cipher text C_i is derived from the XOR operation ($\oplus$) of P_i and K_i; the entire C_i is denoted as $C = C_1 \| C_2 \| \ldots \ldots C_n/64$. The use of a nonce *N* guarantees that each message is associated with a distinct keystream, even while using the same key *K*. Then the decryption process inverse this by getting a similar keystream block K_i using the *N* (same nonce) and counters *i*. Finally, the XORing process is performed to attain the plaintext $P_i = C_i \oplus K_i$. According to the discussion, the encryption and decryption of ChaCha20 is derived in Equation (2)

$$\begin{cases} C = ChaCha20(K, N) \oplus P \\ P = ChaCha20\ (K, N) \oplus C \end{cases} \tag{2}$$

According to the above process, ChaCha20 encrypts the data and stores it in the Hardware Security Module (HSM). For every museum record in the collections, random 96-bit nonce values, which are unique in characteristics, are generated. Then, plaintexts like artefact names, provenance, and descriptions are divided into 64 blocks. ChaCha20 is started using a 256-bit key, a 96-bit nonce for each record, and a block counter that begins at 1. The result is a block of keystream. The keystream block is combined with the initial 64 bytes of plaintext by an XOR operation to generate the initial ciphertext block. The counter is increased, and ChaCha20 creates a new keystream block. This block is then combined with the following 64 bytes of plaintext using the XOR operation. This process persists until all blocks of plaintext are encrypted. The resultant ciphertext blocks are combined to create the whole encrypted record, which is then saved in the database. To decode the record, it is necessary to have the identical nonce and key. The keystream is regenerated by utilizing the nonce and then combined with the ciphertext through the process of XOR to get the original plaintext data. Then, the working structure of the ChaCha20 encryption algorithm is described in Figure 2.

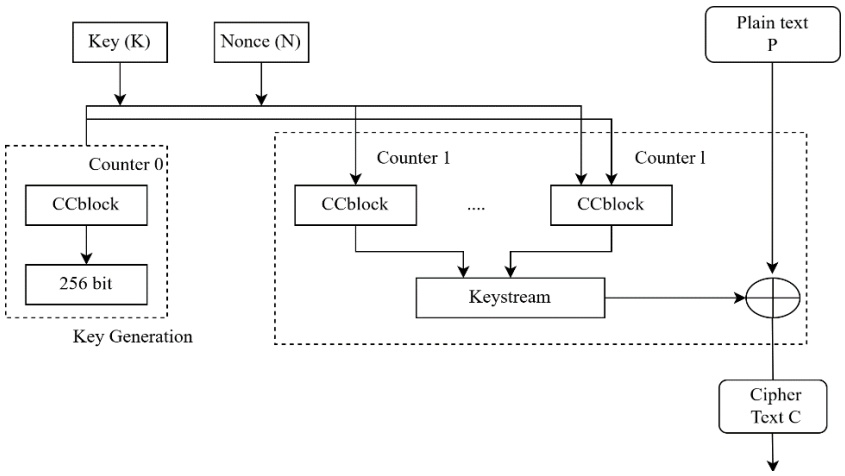


Figure 2. Process of ChaCha20 encryption.

Every object in the collection possesses a distinct nonce, whereas the entire database employs the same key. This enables the implementation of effective encryption and decryption processes while ensuring the security of each record. Then, the pseudocode for the chacha20 encryption algorithm is shown in Algorithm 1and 2.

Algorithm 1: ChaCha20-based Encryption for Museum Artifact Data.

Input:
K ← 256-bit Secret Key
N ← 96-bit Nonce
P ← Plaintext Artifact Data

Output:
C_i ← Encrypted Data Blocks

1: C ← ∅ ; counter ← 1
2: while P ≠ ∅ do
3: K_i ← ChaCha20(K, N, counter)
4: block ← P[0:64]
5: C_i ← block ⊕ K_i
6: C ← C ∪ C_i
7: P ← P[64:]
8: counter ← counter + 1
9: Save (C, N, artifact_metadata)

Algorithm 1 secures museum artifact data using the ChaCha20 stream cipher. It takes as input a 256-bit secret key (K), a 96-bit nonce (N), and the plaintext artifact data (P). In each iteration, the algorithm generates a 64-byte keystream block K_i using the ChaCha20 function, which is then XORed with a 64-byte segment of the plaintext to produce the ciphertext block C_i. This process repeats until all plaintext is encrypted. Finally, the ciphertext, nonce, and artifact metadata are saved for secure storage or transmission.

Algorithm 2: ChaCha20-based Decryption for Museum Artifact Data.

Input:
K ← 256-bit Secret Key
N ← 96-bit Nonce
C ← Encrypted Data Blocks

Output:
P ← Decrypted Artifact Data

1: P ← ∅; counter ← 1
2: while C ≠ ∅ do
3: Ki← ChaCha20(K, N, counter)
4: block ← C[0:64]
5: Pi ← block ⊕ Ki
6: P ← P ∪ Pi
7: C ← C[64:]
8: counter ← counter + 1
9: Save (artifact, P)

Algorithm (2), decryption process reverses the encryption using the same key and nonce. For each ciphertext block, it regenerates the same keystream block Kiusing ChaCha20 and XORs it with the encrypted block to recover the original plaintext segment P_i. The decrypted segments are combined to reconstruct the full artifact data, which is then saved along with its metadata.

According to the pseudocode, the museum details are encrypted and stored in the database, which ensures the security of the sensitive data. In addition, granular RBAC is applied to the process of managing sensitive data. Implementing a detailed Role-Based Access Control (RBAC) system offers an efficient method for museums to regulate the management of sensitive collection data and limit access to their systems. RBAC links permissions to certain roles, such as curator or conservator, rather than individual users. By carefully assigning roles that align with specific job responsibilities, individuals may be given precise access to only the necessary data sets and functionalities. Registrars may necessitate access to records and loans, except insurance assessments. For highly sensitive positions, it may be required to implement additional security measures such as multi-factor authentication. Thoroughly documenting and reviewing job definitions guarantees the proper separation of data and limited access privileges. Users are granted access based on their designated responsibilities, which simplifies access management when staff changes occur. Thorough activity tracking and auditing ensure accountability. The granular RBAC ensures the protection of important museum systems and data by matching access with institutional roles and responsibilities. Continual governance mitigates the risks of excessive permissions or internal security breaches. In the equation $K_i = chacha20\ (k, N, i)$, k denotes the 256-bit secret key used for encryption. It is a critical input to the ChaCha20 algorithm and must be kept secure.

Let's assume, in museum design, that several users are accessible to process the museum holdings and other information. During this process, several sensitive information may abused by the intemediator. Therefore, RBAC is utilized to restrict and limit access to sensitive information on museum holdings. In the museum, there are sets of roles R in which every role r requires permission p to access the information. The set of roles R is defined using Equation (3).

$$\left.\begin{array}{c} R = \{r_1, r_2 \ldots . r_n\} \\ r_1 = \{p_{11}, p_{12}, \ldots . . p_{1m}\} \\ r_2 = \{p_{21}, p_{22}, \ldots . . p_{2k}\} \\ \ldots \ldots . \\ r_n = \{p_{n1}, p_{n2}, \ldots . . p_{nj}\} \end{array}\right\} \quad (3)$$

After defining the roles, user A is assigned to the subset of roles R_u where, $R_u \subseteq R$. The permissions available to user u are the collective set of permissions derived from the roles in R_u. Then $p_u = \cup\ for\ all\ r_m\ in\ R_u$. After assigning the roles, the authorization function A is computed for every user u with respective resources. In Equation (4), the symbol $\boldsymbol{s}$ represents the symmetric key generated by the SLEM algorithm, which is used in conjunction with the user identifier u to form the access tuple $A=(u, s)$. This definition has now been explicitly added in the revised manuscript to eliminate ambiguity.

The authorization is defined using Equation (4)

$$A = (u, s) = \begin{cases} 1 & if\ permission\ for\ s\ in\ p_u \\ 0, & otherwise \end{cases} \quad (4)$$

Let the museum have two roles $R\{Curator, registrar\}$.The curator role has permission to update and read the objects or artefacts that are defined as $curator = \{r_{artifacts}, u_{artifacts}\}$. The registrar only has read permission $Registrar = \{r_{artifacts}\}$. Now the design has user A assigned to the $Au = \{curator\}$, and the authorization function is defined using Equation (5)

$$\left.\begin{array}{c} Au(A, r_{artifacts}) = allows\ (A\ has\ permission\ via\ role) \\ Au(A, u_{artifacts}) = allows\ (A\ has\ permission\ via\ role) \\ Au(A, de_{artifacts}) = deny\ (A\ does\ not\ have\ permission) \end{array}\right\} \quad (5)$$

Similarly, the museum has another user, B and the registrar role is assigned $Bu = \{registrar\}$, and the authorization function is defined using Equation (6)

$$\left.\begin{array}{c} Bu(Br_{artifacts}) = allows\ (B\ has\ permission\ via\ role) \\ Bu(B, u_{artifacts}) = deny(B\ does\ not\ have\ permission\ via\ role) \\ Bu(B, de_{artifacts}) = deny\ (B\ does\ not\ have\ permission \end{array}\right\} \quad (6)$$

The authorization function ensures access control over the museum's data and systems by verifying a user's rights linked to their allocated responsibilities. This

enables the implementation of a least privilege access system that is specifically designed for the operations of a museum. In order to protect confidential visitor data, museums should use end-to-end encrypted communication channels utilizing the ChaCha20 stream cipher for any service that gathers personal information. ChaCha20 offers rapid software encryption that is highly suitable for protecting visitor data during transmission and storage. It is necessary to encrypt any personally identifiable information that is submitted to online ticket forms, reservation systems, contribution sites, etc., using the ChaCha20 encryption method before securely transmitting it via TLS connections. Mobile applications used by visitors should use end-to-end ChaCha20 encryption to ensure that data is anonymized and protected from the network provider. A nonce and key exchange enables the establishment of a distinct ChaCha20 encrypted session between the device of each visitor and the museum servers. Visitors' mobile devices have hardware-protected enclaves that segregate private keys. Backend services employ load balancers to decrypt and subsequently re-encrypt data before it is sent to internal servers responsible for storing encrypted data. Implementing ChaCha20 encryption in an end-to-end system allows museums to guarantee visitors that their data and actions will remain confidential within the museum's network. This all-encompassing strategy ensures that confidential information is hidden from the network and remains unidentified throughout transmission.

In order to ensure the smooth and immediate responsiveness of museum exhibitions, it is necessary to incorporate the ChaCha20 lightweight encryption algorithm into the endpoint controllers of the exhibits. ChaCha20 is specifically designed to achieve efficient execution in software on various embedded devices, such as Raspberry Pis and microcontrollers commonly seen in museum exhibitions. The stream cipher operation enables the efficient and immediate encryption of audio, video, and control logic streams on show computers that have limited resources. ChaCha20 would be executed directly on the show endpoint hardware rather than on the main application Central Processing Units (CPUs). Basic (APIs) reduce the level of difficulty in integrating systems compared to conventional encryption methods. Locally generated keys on each exhibit controller and regularly changed provide up-to-date encryption without the need to reconfigure exhibitions. Museums may provide seamless encryption security for exhibit interaction and usability by seamlessly offloading fast ChaCha20 encryption to display network endpoints. ChaCha20 is highly efficient and has a compact design, making it well-suited for safeguarding museum displays and providing a pleasant experience for visitors. According to the discussion, the museum has exhibited information like control logic, video, and audio as plain text (P). The P is converted into the C using the symmetric encryption key K and a nonce (N), in accordance with the ChaCha20 encryption mechanism. Then, the lightweight encryption is performed according to Equations (1) and (2), and the cipher operator on the exhibit endpoint controller. The ChaCHa20 encryption algorithm is applied to the embedded system components to improve security in different aspects. Then, the structure of lightweight encryption in embedded components is illustrated in Figure 3.

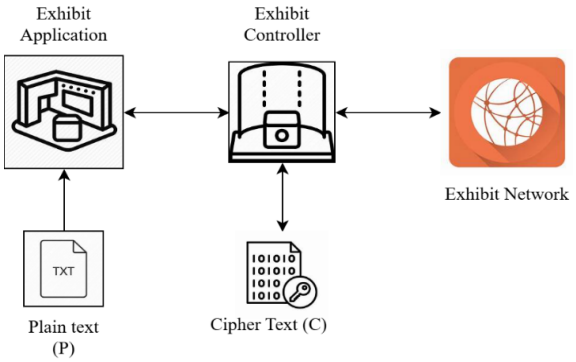


Figure 3. Embedded components in encryption process.

The simulated application logic transfers unencrypted plaintext data P to its local endpoint controller without any understanding of encryption. Using the lightweight ChaCha20 algorithm and a locally stored secret key K, the controller encrypts P into ciphertext C in a visible manner. The encryption process occurs exclusively on the controller hardware, which is designed to maximize the speed of cipher operations. The resultant ciphertext C is broadcast across the exhibit network to additional endpoints. After receiving it, the endpoint utilizes the same key K and ChaCha20 to decode C back into plaintext P. The initial data P is subsequently sent back to the local exhibit application. This approach enables the complete encryption process to be seamlessly delegated to the exhibit endpoint. The exhibit software and visitor experience remain unaltered, with the assurance that important data flows are safely safeguarded through the utilization of rapid ChaCha20 encryption, which is integrated into the show hardware controllers. The algorithm's lightweight structure reduces its influence on responsiveness effectively.

4. Results and Discussions

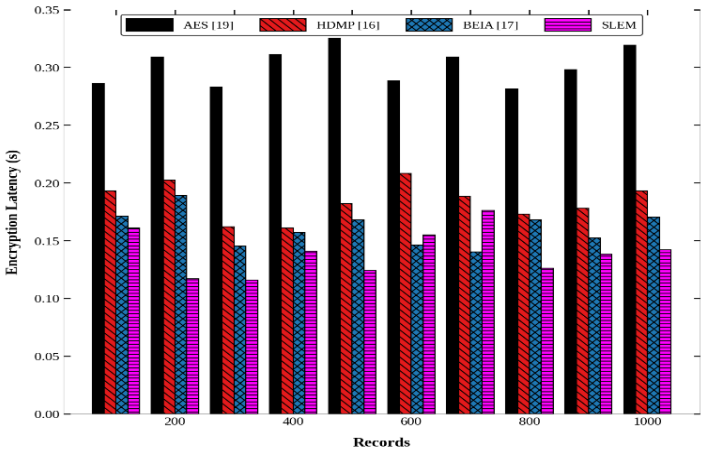
This section evaluates the SLEM efficiency while protecting Musume data from third-party users. An optimal museum encryption testing environment would include tangible gear such as servers, Raspberry Pi displays, HSM modules, and networking equipment. Python and C/C++ are programming languages that are well-suited for incorporating cryptography libraries such as Open Secure Sockets Layer (OpenSSL) and mbedTLS. The museum data may be stored on secure database servers that utilize encryption, while online and mobile applications facilitate visitor experiences. Prometheus enables the monitoring of performance parameters such as latency and throughput. Continuous

integration/deployment facilitates expedited testing. The encryption systems should have a hierarchical structure, integrating techniques such as AES-256, RSA, and Elliptic Curve Cryptography (ECC) that are specifically tailored for certain applications. There is a need to handle the comprehensive aspects of key generation, administration, and rotation. Encryption capabilities are necessary for storsage solutions and network connectivity. Comprehensive audit records ensure responsibility and transparency. The combination of authentic hardware, software integration tools, cryptographic libraries, and monitoring instrumentation allows for the comprehensive prototyping, profiling, and optimization of encryption systems for museums. This ensures efficiency prior to actual deployment in real-world scenarios.

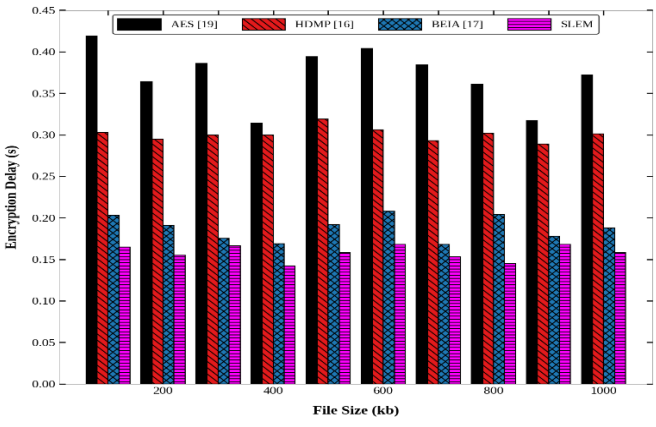
The efficiency of the system is evaluated using different metrics such as encryption latency, decryption latency, CPU usage, power consumption and throughput rate. The obtained SLEM results are compared with the HDMP [19], BEIA [25] and AES [22] to evaluate the system efficiency. During the analysis, the museum data files dataset (https://www.imls.gov/research-evaluation/data-collection/museum-data-files) information is utilized to evaluate the system efficiency. The dataset consists of United States-related museum information, which is processed using the SLEM approach to protect sensitive data. The dataset consists of several pieces of information like museum location, geocode data, museum discipline, exempt entities code, and other economic-related details. The museum details are gathered from various sources such as Institute of Museum and Library Services (IMLS) administrative records, non-profit data, internal revenue services, museum associations, etc. The gathered information is encrypted using the chacha20 encryption algorithm, which ensures the data security of the museum information and visitor's details.

4.1. Encryption latency analysis

Figure 4 illustrates the graphical analysis of encryption delay for varying numbers of records and file sizes. The analysis clearly shows that the SLEM approach attains a minimum delay value (0.116 to 0.155 s) compared to other encryption methods. The SLEM approach employed in the musume design achieves minimal encryption delay by strategically employing optimal encryption algorithms and selective encryption approaches. The SLEM utilizes the ChaCha20 encryption to secure confidential information. ChaCha20 is renowned for its exceptional speed and throughput, which it achieves by effectively using parallelization in contemporary CPUs. SLEM decreases the processing overhead and time needed to encrypt data by using a performance-optimized method.



a) Number of records.



b) Varying file size.

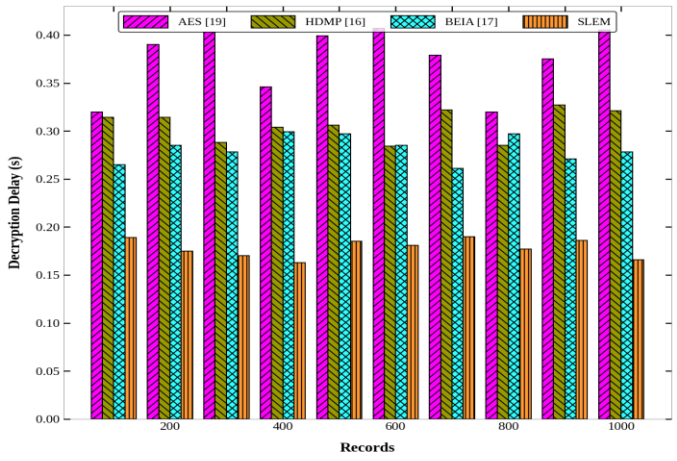
Figure 4. Encryption delay analysis.

The SLEM utilizes low-weight encryption algorithms for both interactive design elements and visitor-oriented components of the system. These ciphers sacrifice a certain level of security in exchange for improved speed and reduced resource use. SLEM enhances its algorithm selections by including role-based access restrictions that restrict the encryption requirements for certain data and design components. This targeted approach decreases the total encryption burden of the system in comparison to implementing strong encryption universally. The decreased workload leads to a shorter processing time and minimum delay.

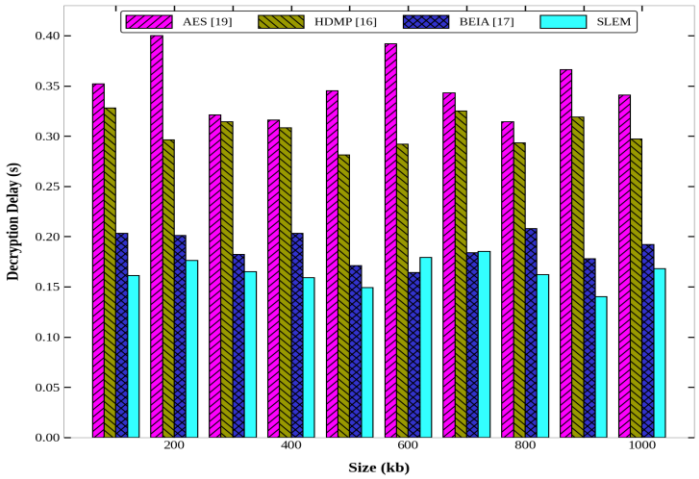
4.2. Decryption Delay

Figure 5 illustrates the graphical analysis of decryption delay for varying numbers of records and file sizes. The analysis clearly shows that the SLEM approach attains a minimum delay value (0.1456 to 0.185 s) compared to other encryption methods. SLEM utilizes the ChaCha20 cipher to encrypt sensitive data. This cipher enables rapid decryption speeds by facilitating parallel processing of encrypted blocks, reducing preprocessing, and employing straightforward round operations that are highly compatible with CPUs. Interactive components employ lightweight ciphers that promote efficiency over strength through the use of smaller keys, reduced mathematical operations, and streamlined logic that emphasizes rapid decryption.

SLEM employs access restrictions to selectively encrypt data, hence reducing the decryption burden only to include essential information. SLEM prioritizes efficient decryption for visitor traffic by allocating dedicated decryption resources to precomputing values and reducing pre-decryption processing. SLEM achieves minimal decryption time throughout the whole system by using technological improvements such as high-speed algorithms, efficient, lightweight ciphers, selective encryption, and prioritizing visitor experience.



a) Number of records.



b) Varying file size.

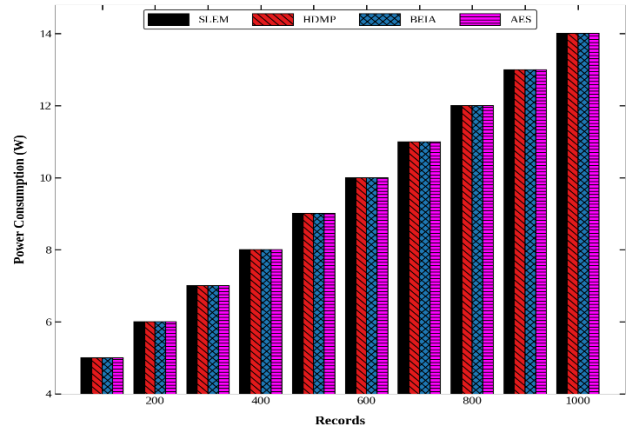
Figure 5. Decryption delay analysis.

4.3. Power Consumption Analysis

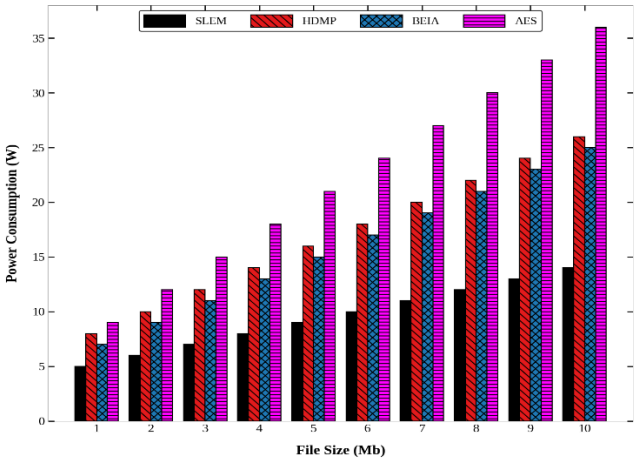
As demonstrated in Figure 6, SLEM has a reduced power consumption that increases gradually as the number of records increases, in contrast to other methods. The efficiency improvements of SLEM are showcased by its ability to selectively encrypt data, hence minimizing energy costs associated with encryption, even when dealing with enormous datasets. SLEM achieves efficient power usage during encryption by employing optimized algorithms and

selective encryption approaches.

SLEM decreases the computational and energy demands for data encryption by utilizing optimized ciphers such as ChaCha20. In addition, SLEM's selective encryption method encrypts only the essential data, hence reducing the total power requirements. SLEM offers a customized encryption solution that minimizes resource utilization and optimizes power consumption throughout the system, resulting in lower computation and electricity costs. This enables SLEM to sustain optimal performance without incurring excessive energy consumption.



a) Number of records.



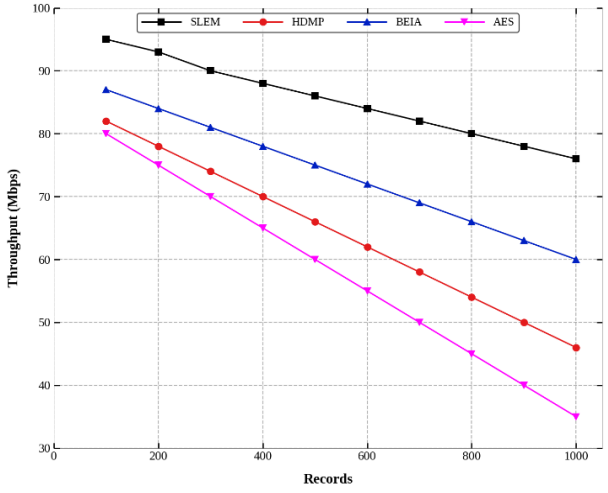
b) Varying file size.

Figure 6. Power consumption analysis.

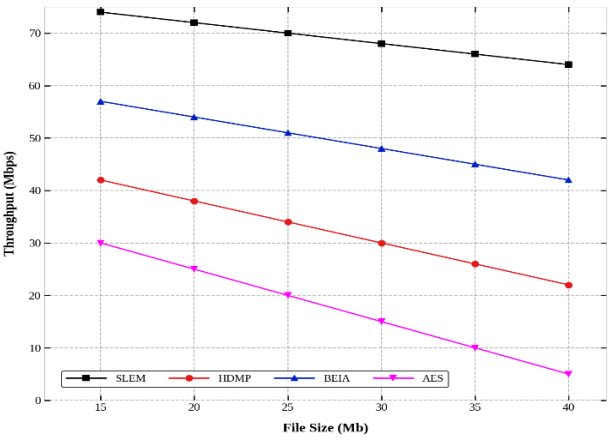
SLEM decreases the computational and energy demands for data encryption by utilizing optimized ciphers such as ChaCha20. In addition, SLEM's selective encryption method encrypts only the essential data, hence reducing the total power requirements. SLEM offers a customized encryption solution that minimizes resource utilization and optimizes power consumption throughout the system, resulting in lower computation and electricity costs. This enables SLEM to sustain optimal performance without incurring excessive energy consumption.

4.4. Throughput Analysis

SLEM has been designed to optimize data transfer rates by utilizing high-speed symmetric encryption techniques and employing selective encryption depending on access control roles. More precisely, SLEM employs ChaCha20 as its main data cipher, which offers a high data transfer rate thanks to its stream cipher design that enables simultaneous encryption of message blocks. ChaCha20 is characterized by its minimum preprocessing and straightforward round operations, making it highly suitable for efficient implementation on CPUs. SLEM employs lightweight ciphers that utilize simplified substitution-permutation networks, prioritizing efficiency above security for interactive parts. SLEM minimizes the overall encryption effort by encrypting just the data that is accessible by certain roles, as opposed to applying strong encryption to all data indiscriminately. Reducing the total workload and avoiding needless encryption allows for increased performance. SLEM allocates resources and optimizes the pathways taken by visitor traffic to provide the highest possible data transfer rate for end users. SLEM utilizes a combination of algorithm choices, selective role-based encryption, and visitor experience improvements to maximize the use of available resources for achieving high performance and efficient throughput (Figure 7) in all system encryption processes.



a) Number of records.



b) Varying file size.

Figure 7. Throughput analysis.

Thus, the SLEM approach successfully provides security and privacy to the museum holdings as well as visitor information with minimum delay and maximum throughput value.

5. Conclusions

Thus, the paper analyzes the SLEM based on the Musume design. The study utilized the ChaCha20 encryption algorithm to provide security to the museum's holding and visitor's information. Here, the collected museum information is explored frequently using the keystream block and nonce information that convert the data into the cipher text. In addition, role-based access control mechanisms are established to prevent the unauthorized access of museum holdings. For every user, specific roles are allocated, and the permission is established according to the roles, which improves overall privacy and security. Then, end-to-end encryption is utilized along with the chacha20 encryption method to protect the visitor's information and avoid irrelevant user participation. Finally, the microcontroller embedded system is incorporated into the encryption process to customize the secured museum design. The controller participated in the encryption process, which minimizes the encryption delay (o.15s) and maximizes throughput (95%) compared to other methods. In future, optimized deep learning techniques will be integrated with encryption techniques to improve the authentication and authroization process. [16]

Author Contributions

Study conception and design, data collection, draft manuscript preparation: X. Y. Li; analysis and interpretation of results, study conception and design: Y. H. Wu. All authors reviewed the results and approved the final version of the manuscript.

References

[1] Abed A., Abdelkader T., and Hashem M., "SLACPSS: Secure Lightweight Authentication for Cyber-Physical-Social Systems," *Computers*, vol. 13, no. 9, pp. 225, 2022. https://doi.org/10.3390/computers13090225

[2] Acheampong R., Popovici D., Balan T., Rekeraho A., and Ramos M., "Enhancing Security and Authenticity in Immersive Environments," *Information*, vol. 16, no. 3, pp. 1-23, 2025. https://doi.org/10.3390/info16030191

[3] Bodin T. and Duvana D., Key Factors in Interdisciplinary Interactive Exhibition Design: Exhibition Design Processes with Museum Professionals and Interaction Design and Technology Experts, Master's Thesis, Chalmers University of Technology and University of Gothenburg, 2021. https://hdl.handle.net/20.500.12380/304567

[4] Cameron H., Outdata-ed Museums: Creating Ethical and Transparent Data Collection Processes in Museums, University of Nottingham, Ph.D. dissertation, 2022. https://www.proquest.com/openview/0981a8b968921a04a41cac0bd04c694f/1?pq-origsite=gscholar&cbl=2026366&diss=y

[5] Farris G., Pinna A., Baralla G., Tonelli R., and et al., "Design of a Blockchain-Oriented System for the Sustainable Disintermediation in Tourism," *in Proceedings of the IoT Vertical and Topical Summit for Tourism*, Cagliari, pp. 1-6, 2021. DOI: 10.1109/IEEECONF49204.2021.9604896

[6] Ferrato A., Limongelli C., Mezzini M., and Sansonetti G., "Using Deep Learning for Collecting Data about Museum Visitor Behavior," *Applied Sciences*, vol. 12, no. 2, pp. 1-21, 2022. https://doi.org/10.3390/app12020533

[7] Gawade D., Ziemann S., Kumar S., Iacopino D., and et al., "A Smart Archive Box for Museum Artifact Monitoring Using Battery-Less Temperature and Humidity Sensing," *Sensors*, vol. 21, no. 14, pp. 1-17, 2021. https://doi.org/10.3390/s21144903

[8] Hu Y., Sun W., Liu X., Gan Q., and Shi J., "Tourism Demonstration System for Large-Scale Museums Based on 3D Virtual Simulation Technology," *The Electronic Library*, vol. 38, no. 2, pp. 367-381, 2020. https://doi.org/10.1108/EL-08-2019-0185

[9] Huang X. and Zhu S., "Optimization of Daylighting Pattern of Museum Sculpture Exhibition hall," *Sustainability*, vol. 13, no. 4, pp. 1-16, 2021. https://doi.org/10.3390/su13041918

[10] Ivanov R., "ExhibitXplorer: Enabling Personalized Content Delivery in Museums Using Contextual Geofencing and Artificial Intelligence," *ISPRS International Journal of Geo-Information*, vol. 12, no. 10, pp. 1-28, 2023. https://doi.org/10.3390/ijgi12100434

[11] James E. and Rabbi F., "Fortifying the IoT Landscape: Strategies to Counter Security Risks in Connected Systems," *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, vol. 6, no. 1, pp. 32-46, 2023. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Fortifying+the+IoT+Landscape%3A+Strategies+to+Counter+Security+Risks+in+Connected+Systems&btnG=

[12] Jingwen Z. and Lin L., "Limitations and Ethical Reflection on the Application of Big Data in Museum Visitor Research," *Museum Management and Curatorship*, vol. 38, no. 4, pp. 416-427, 2023. https://doi.org/10.1080/09647775.2022.2111333

[13] Kumar S., Kumar D., Dangi R., Choudhary G., and et al., "A Review of Lightweight Security and

Privacy for Resource-Constrained IoT Devices," *Computers, Materials and Continua*, vol. 78, no. 1, pp. 31-63, 2024. DOI: 10.32604/cmc.2023.047084

[14] Li J., Gopal R., and Sigappi A., "IoT in a Museum for Interactive Experience Design," *Annals of Operations Research*, vol. 326, pp. 111-111, 2021. DOI: 10.1007/s10479-021-04419-z

[15] Masal K., Bhatlawande S., and Shingade S., "Development of a Visual to Audio and Tactile Substitution System for Mobility and Orientation of Visually Impaired People: A Review," *Multimedia Tools and Applications*, vol. 83, pp. 20387-20427, 2023. https://doi.org/10.1007/s11042-023-16355-0

[16] Menandas J. and Subaja M., "An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL," *The International Arab Journal of Information Technology*, vol 22, no. 5, pp. 859-872, 2025. https://doi.org/10.34028/iajit/22/5/2

[17] Nugraha Y. and Martin A., "Cybersecurity Service Level Agreements: Understanding Government Data Confidentiality Requirements," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1-19, 2022. https://doi.org/10.1093/cybsec/tyac004

[18] Ogbuke N., Yusuf Y., Dharma K., and Mercangoz B., "Big Data Supply Chain Analytics: Ethical, Privacy and Security Challenges Posed to Business, Industries and Society," *Production Planning and Control*, vol. 33, no. 2-3, pp. 123-137, 2022. https://doi.org/10.1080/09537287.2020.1810764

[19] Shang R. and Li X., "Improved Heuristic Data Management and Protection Algorithm for Digital China Cultural Datasets," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 21, no. 5, pp. 1-11, 2023. DOI: 10.1145/3394114

[20] Thakor V., Razzaque M., and Khandaker M., "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177-28193, 2021. DOI: 10.1109/ACCESS.2021.3052867

[21] Tizi L., Ferrario D., Campanaro M., and Arico M., "The Impact of Museum Design on Visit Experience from an Environmental Psychology Perspective," *in Proceedings of the First ArCo Conference,* Firenze, 2023. https://www.researchgate.net/profile/Giorgio-Verdiani-2/publication/355680937_CH_representation_between_Monge's_projections_and_Augmented_Reality/links/6395fbbce42faa7e75b59a3d/CH-representation-between-Monges-projections-and-Augmented-Reality.pdf#page=87

[22] Vayadande K., Raut A., Bhonsle R., Pungliya V., and et al., "Secured Ticketless Booking System to Monuments and Museums Using Cryptography," *in Proceedings of the Intelligent Communication Technologies and Virtual Mobile Networks*, Tirunelveli, 2023. https://doi.org/10.1007/978-981-99-1767-9_28

[23] Wang Y., Chen C., and Deng Y., "Authorization Mechanism Based on Blockchain Technology for Protecting Museum-Digital Property Rights," *Applied Sciences*, vol. 11, no. 3, pp. 1-37, 2021. https://doi.org/10.3390/app11031085

[24] Wang Y., Chen C., and Deng Y., "Museum-Authorization of Digital Rights: A Sustainable and Traceable Cultural Relics Exhibition Mechanism," *Sustainability*, vol. 13, no. 4, pp. 1-26, 2021. https://doi.org/10.3390/su13042046

[25] Zhao L., Zhang J., Jing H., Wu J., and Huang Y., "A Blockchain-Based Cryptographic Interaction Method of Digital Museum Collections," *Journal of Cultural Heritage*, vol. 59, pp. 69-82, 2023. DOI:10.1016/j.culher.2022.11.001

Si Li received the B.S. degree in Computer Science and Technology from Northeastern University, Liaoning, China, in 2003, and the M.S. degree in Software Engineering from the School of Software and Microelectronics, Peking University, Beijing, China, in 2007. From 2007 to 2011, he was a Teaching Assistant at Dalian Neusoft University of Information, Liaoning, China. In 2011, he became a Lecturer at the same institution. In 2012, he served as an IT Project Manager at Dalian Tianwei Technology Co., Ltd. In 2016, he joined Beijing Jiahe Culture Technology Co., Ltd. as a Technical Lead. In 2017, he worked as an IT Technical Manager at Dajia Life Insurance Co., Ltd. In 2023, he joined the School of Information Engineering at Liaoning Institute of Technology. His research interests include Software Engineering, Virtual Reality (VR), Digital Twins, and Artificial Intelligence (AI).

Hui Dai received the Bachelor's degree in Chinese Language and Literature from Dalian Minzu University, Liaoning, China, in 2012. From 2018 to 2020, she worked as a Demand Analyst at Shanghai Gedi Electric Power Technology Co., Ltd. In May 2020, she joined iSoftStone Information Technology Co., Ltd. as an Intermediate Demand Analyst. In September 2023, she became a staff member in the Academic Affairs Office at Liaoning Institute of Technology. Her research interests include Chinese Language and Literature and Artificial Intelligence (AI).

Xiaoyuan Li is a lecturer at the School of Visual Art and Design, Guangzhou Academy of Fine Arts. Her main research focuses on the Integration of Art and Technology, Covering Interdisciplinary Media Art Design, Museum Exhibition Design and Unnatural Narrative Art. She has published numerous academic papers in relevant research fields.

Yihua Wu is a faculty member of the School of Painting Art, Guangzhou Academy of Fine Arts. He is engaged in professional research on painting art, with research interests focusing on Media Research on Physical Presentation of Digital Paintings. He has published plenty of academic papers in related fields.