ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 2 - 2026

Research on the application and guarantee of network security technology in the digital dissemination of non-heritage Bowen culture

Xiao Yu[1,*], *Yilin Wang*[1], *Jinming Zheng*[2], *Qihua Weng*[1] *and Jie Cai*[1]

1 School of Digital Intelligence Technology, Wenzhou Vocational College of Science and Technology, Zhejiang province, 325000, China
2 Institute of Digital and Intelligent Technology, Wenzhou Vocational College of Science and Technology (Wenzhou Academy of Agricultural Sciences), Wenzhou, 325000, China

SUMMARY: *This paper focuses on the digital communication security of non-heritage Bowen culture, focusing on analysing the network security risk of the platform architecture, the main types of security threats, vulnerability assessment, and proposing the key security technology system of identity authentication, data encryption, intrusion detection, and defense in depth. Combined with the security management system and emergency response mechanism, a multi-level security system is constructed to enhance the security, stability and credibility of digital communication of non-heritage culture. This study is of great practical significance for promoting the safe inheritance of intangible cultural heritage and digital cultural governance.*

KEYWORDS: *intangible cultural heritage; digital dissemination; network security; identity authentication*

1 Introduction

Intangible cultural heritage (ICH) is an important carrier of national culture, with profound historical value and unique artistic charm. Driven by digital technology, the dissemination of ICH is transforming from traditional media to network platforms, with the help of cloud computing, blockchain, artificial intelligence and other technologies to achieve cross-regional and cross-cultural sharing and inheritance [1]. While enhancing cultural accessibility, NRL digital communication platforms also face security threats such as data leakage, content tampering, and cyber attacks, posing serious challenges to the authenticity, integrity, and sustainability of cultural resources.

2 Cybersecurity Risk Analysis of the Digital Dissemination Platform for Afro-Chinese Heritage

2.1 Platform Architecture and Security Status

The digital communication platform of non-heritage Bowen culture is built on the basis of cloud computing and distributed storage technology, combined with Web front-end, mobile application, database, content distribution network (CDN) and security protection module.

*natr3147@outlook.com
https://doi.org/10.65102/is2026828
Published: 30 April, 2026

The platform adopts a multi-layer architecture, including data layer, business layer, application layer and user layer. The data layer is mainly responsible for the storage, management and encryption protection of non-heritage cultural resources; the business layer implements core functions such as content management, user interaction and permission control; the application layer provides interfaces on the Web side and mobile side to support user access and content interaction; and the user layer contains access permission settings for different roles such as ordinary users, management personnel, and research institutions. In addition, the platform introduces an API gateway to support cross-platform data interaction, and uses blockchain deposit technology to enhance the traceability and non-tampering of data [2].

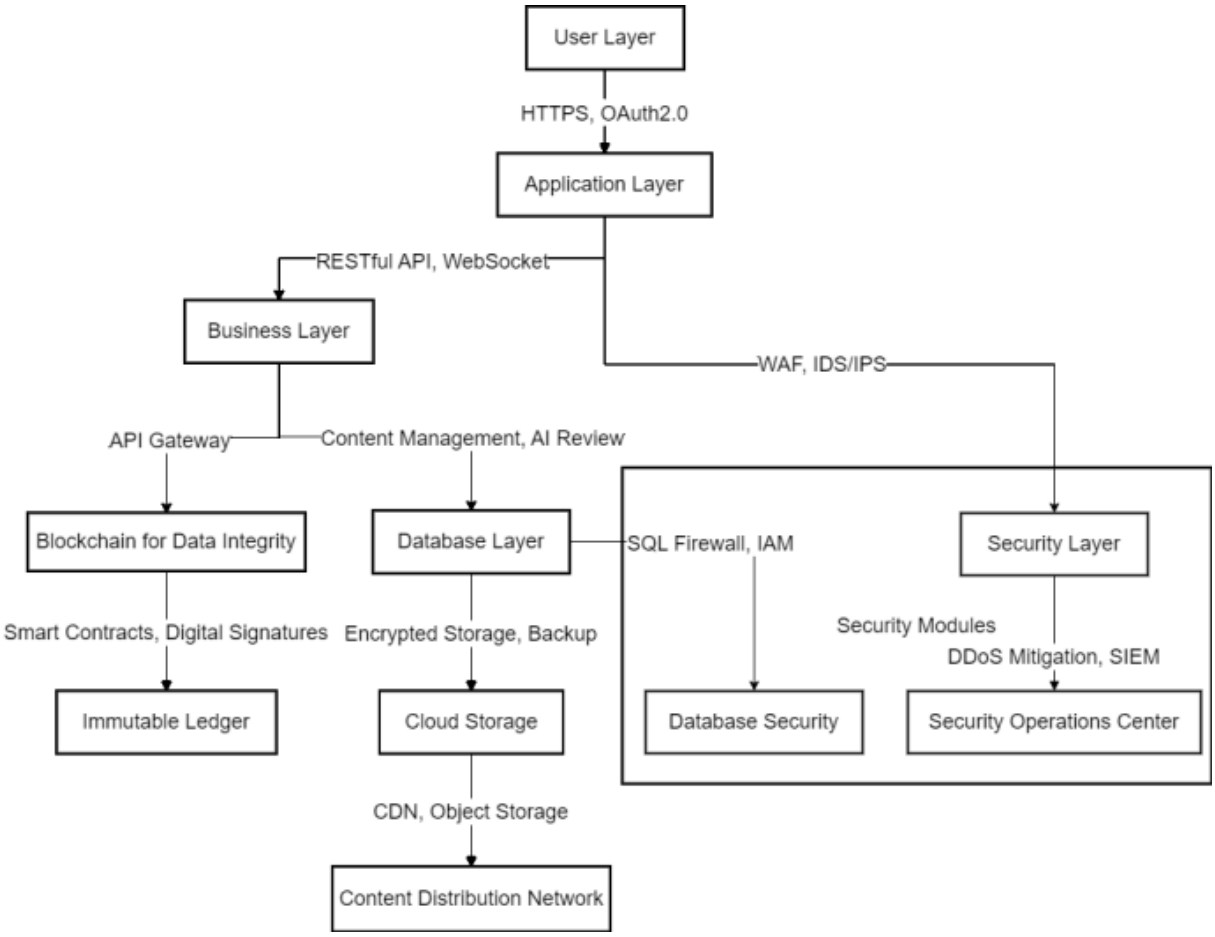

Figure 1: Platform architecture diagram

The digital dissemination platform of non-heritage has certain security guarantees in its technical structure, such as adopting HTTPS protocol for data transmission, user authentication based on OAuth2.0, and configuring firewalls and security groups for basic network access control. However, the current non-legacy digital communication platform still faces many challenges in terms of security:

(1) Data storage security: non-heritage cultural digital resources are usually stored in the cloud or local servers in various forms such as high-definition images, audio, video, documents, etc. [3]. Due to the distributed nature of the storage medium, the data may face risks such as unauthorised access, data leakage and malicious tampering. Databases that lack perfect encryption and backup mechanisms are vulnerable to SQL injection attacks, ransomware attacks, and other threats.

(2) Access control and privilege management vulnerability: Since the digital dissemination platform for non-legacy involves multi-role user management, including ordinary users, researchers, content administrators, etc., privilege classification and access control have become the key point of security management. Currently, some platforms still adopt the traditional role-based access control (RBAC) mechanism, but lack of more refined dynamic access control (ABAC) or zero-trust security model, which may lead to security risks such as overstepping access and abuse of privileges.

(3) Content Supply Chain Security: As a dissemination carrier of NRL culture, the platform needs to support the functions of uploading, auditing and publishing content by multiple parties. Due to the diversity of non-heritage cultural resources, some of the content may be subject to copyright disputes, falsification of information, alteration of history, etc. The platform's content supply chain may be subject to falsification of data. The platform's content supply chain may be subject to new types of security threats such as fake data injection, phishing attacks and Deepfake, affecting the authenticity and credibility of cultural communication.

(4) Insufficient network attacks and intrusion defence: In recent years, distributed denial of service (DDoS) attacks, cross-site scripting (XSS), cross-site request forgery (CSRF) and other attack methods have become more and more sophisticated, and the digital communication platform of non-legacy heritage is easy to become a target of attacks due to its public access characteristics [4]. At present, some platforms still mainly rely on traditional WAF (Web Application Firewall) for basic protection, lacking intelligent intrusion detection and abnormal behaviour analysis mechanisms, making it difficult to identify and respond to advanced persistent threats (APT) in a timely manner.

(5) Data transmission security and privacy protection: In the process of digital dissemination of non-legacy, it involves user interaction, resource sharing, academic research and other forms of data flow. If strong encryption transmission technologies, such as TLS 1.3 and end-to-end encryption (E2EE), are not used, sensitive data may be stolen or tampered with. Some platforms have not yet established comprehensive user privacy protection mechanisms, such as the data minimisation principle and de-identification processing, resulting in the risk of user information leakage.

2.2 Main types of security threats

During the development of information technology, the digital communication platform of non-legacy Bowen culture still faces a variety of security threats, even though it has improved its data processing capacity and security protection level through cloud computing, distributed storage, encryption technology, and so on. These threats not only affect the stable operation of the platform, but also may lead to data leakage, tampering, and even affect the authenticity and integrity of cultural communication. The following is an analysis of the main types of security threats.

(1) Data security threats: As an important part of cultural heritage, NRM digital resources are stored in cloud databases or distributed storage systems, and their security is crucial. Data leakage is the most common risk, which may originate from improper database configuration, missing access rights management or insufficient encryption mechanism. Once hackers obtain sensitive data through SQL Injection, brute-force cracking or insider leakage, NCS cultural resources may be stolen, tampered with or even maliciously destroyed. Data Integrity Attack (Data Integrity Attack) is also a key threat. Attackers can make use of unencrypted or inadequately protected storage media to tamper with historical documents, audio and video materials, distorting digitised cultural content and affecting public perception.

(2) Authentication and Access Control Vulnerabilities: The digitisation platform for

non-heritage culture involves multiple roles of users, including ordinary visitors, academic researchers, cultural management departments, platform administrators and so on. Deficiencies in the authentication and access control mechanisms may lead to problems such as overstepping access and abuse of privileges. If only relying on traditional Role-Based Access Control (RBAC) and lacking fine-grained privilege management based on Attribute-Based (ABAC) or Zero-Trust Architecture, attackers can bypass authentication and illegally access confidential data through Privilege Escalation (PEA) or Session Hijacking (SH). In addition, weak passwords and multi-factor authentication (MFA) are not mandatorily enabled, making it easier for Brute Force Attacks to succeed.

(3) Network Attacks and Platform Availability Threats: As a public-facing online platform, NRL digital communication platforms are easy targets for hacker attacks. Distributed Denial of Service Attack (DDoS) is a common attack method, in which the attacker sends a large number of invalid requests to the platform server by controlling a large number of Botnets (Botnets), which exhausts the system resources and leads to access delays and even service interruptions [5]. Application layer attacks (Layer 7 Attacks), such as HTTP Flooding, Slowloris Attack, etc., also consume server resources and affect normal user access.

(4) Malicious code and intrusion risk: With the open sharing of digitised content of non-heritage culture, the platform needs to support the uploading and interaction of content from multiple parties, which also provides a channel for the dissemination of malicious code. Attackers may perform cross-site scripting (XSS) attacks by uploading files containing malicious scripts and embedding malicious links to steal user credentials or tamper with webpage content. File Inclusion Vulnerability (RFI) and Cross-Site Request Forgery (CSRF) are also common risks. Attackers can take advantage of the platform's automated processing mechanism to remotely load malicious code, take control of the server or perform unauthorised operations. If there is a lack of strict code review and protection mechanisms, malware may proliferate at the user's end, affecting overall network security.

(5) Content tampering and deep forgery threat: The core of digital dissemination of non-heritage culture is the authenticity and authority of the content. In recent years, the development of Artificial Intelligence Generated Content (AI-Generated Content, AIGC) technology has made cultural content tampering and deepfake (Deepfake) a serious threat. Attackers can use deep learning models to falsify historical audio and video, modify image information, and even synthesise false historical documents, thus misleading public perception and affecting the academic research and transmission of cultural heritage. Especially in the absence of effective Digital Watermarking (Digital Watermarking) and blockchain traceability mechanisms, it is difficult for platforms to identify the true source of content, leading to information pollution and misleading communication.

(6) Supply chain security risk: Non-legacy digital communication platforms often rely on cloud computing, CDN, database, artificial intelligence processing and other functions provided by third-party technology service providers. Supply chain security vulnerability may become a breakthrough for attackers. If the platform introduces open-source components that have not been subject to strict security audits, attackers can implant a backdoor in the code through Supply Chain Attack to gain long-term control of the platform. The lack of access control and encryption protection of third-party API interfaces may lead to sensitive data leakage or theft by Man-in-the-Middle (MITM) attacks, affecting the platform's data security and privacy protection capabilities [6].

(7) Privacy leakage and compliance risk: When providing personalised recommendations, user behaviour analysis and other functions, the non-heritage cultural communication platform will collect and process a large amount of user data, including access records, interest preferences, social interactions and so on. If the data storage is not secure or the privacy policy

is not transparent, user information may be illegally collected, trafficked, or even subjected to precise phishing attacks (Phishing Attack). With the increase in data compliance requirements, such as the implementation of the Data Security Law and the Personal Information Protection Law (PIPL), platforms that fail to establish a comprehensive data compliance management system may face legal risks, affecting the normal operation of the platform and international cooperation.

2.3 Risk Assessment and Vulnerability Analysis

When facing complex cybersecurity threats, the digital communication platform of non-legacy Bowen culture needs to establish a systematic risk assessment methodology to quantify the potential impact of security hazards and formulate effective protection strategies [7]. Currently, common risk assessment frameworks include NIST SP 800-30 risk assessment model, ISO/IEC 27005 information security risk management standard and CVSS (Common Vulnerability Scoring System) vulnerability scoring system. Combined with the actual needs of the platform, the Asset-Threat-Vulnerability (ATV) analysis method can be used to form a comprehensive risk matrix and specify high-priority protection targets by identifying key assets, assessing potential threats, and analysing system vulnerabilities.

Based on the analysis of the platform architecture and security status quo, the main sources of risk include data security, identity authentication, cyber-attacks, malicious code, content tampering, supply chain security and privacy protection. In order to accurately assess the degree of impact of various types of security threats, a risk scoring model can be used to calculate the risk score (Risk Score, R) with the threat likelihood (Probability, P), the degree of impact (Impact, I) and the vulnerability index (Vulnerability, V) as the core parameters with the following formula:

$R=P\times I\times V$

Among them:

P (threat likelihood): assessment based on historical attack events, industry trends and the maturity of the attack technology (level 1-5, with 5 being extremely high).

I (degree of impact): assess the impact of the threat on platform data, user privacy, system stability, etc. (level 1-5, with 5 being extremely high).

V (Vulnerability Index): analyse the system's defensive capability under the threat, including the effectiveness of existing security measures (level 1-5, with 5 being extremely vulnerable). Based on the above model, the main security risks of the digital communication platform for NRM are assessed.

Table 1: Risk score analysis of digital communication platforms for NRHs

serial number	Type of security risk	Threat likelihood (P)	Level of impact(I)	Vulnerability index(V)	Risk score(R)	risk level
1	Data leakage (unauthorised access)	5	5	4	100	extremely high
2	SQL injection attack	4	5	5	100	extremely high
3	Authentication vulnerabilities (weak passwords, credential theft)	5	4	4	80	high
4	DDoS attacks (platform availability threats)	5	4	3	60	high
5	Malicious Code and Cross-Site Scripting (XSS)	4	4	3	48	middle
6	Deepfake (Deepfake content manipulation)	3	5	4	60	high
7	Supply Chain Attacks (Third Party Component Vulnerabilities)	3	5	4	60	high
8	User privacy breach (illegal data collection)	4	4	3	48	middle
9	Social engineering attacks (phishing, identity forgery)	3	4	3	36	middle

From the risk scorecard, data leakage, SQL injection, identity authentication vulnerability and DDoS attack of the digital communication platform of non-legacy belong to high-risk risks, with high occurrence probability and influence, and need to prioritise the reinforcement of protection measures [8]. In addition, although the probability of occurrence of deep forgeries and supply chain attacks is relatively low, once they occur, they may have a serious impact on the platform credibility and data integrity, and therefore they also need to be focused on. For these security risks, the main vulnerabilities are analysed as follows:

(1) Weak data access control: part of the database storage adopts the default configuration and does not strictly implement the access control based on the principle of least privilege, which results in data being easily accessed or tampered by unauthorised users.

(2) Insufficient code security: Some inputs in Web applications are not strictly verified, which may lead to code vulnerabilities such as SQL injection and XSS attacks, enabling attackers to perform malicious operations.

(3) Single authentication mechanism: relying only on username/password login without mandatory enablement of Multi-Factor Authentication (MFA), resulting in accounts that are

vulnerable to brute-force cracking or misuse after credentials are leaked.

(4) Insufficient DDoS protection: relying only on traditional firewalls, without deploying efficient traffic cleaning and intelligent scheduling strategies, which can easily lead to unavailability of services under large-scale attacks.

(5) Lack of guarantee for content authenticity: digital watermarking, blockchain deposit and other technologies have not been widely adopted, making it difficult to verify the authenticity of non-legacy cultural content, which may be tampered with by deep forgery techniques.

(6) High supply chain security risk: some third-party cloud services and API interfaces lack strict security audits, and there are potential backdoors, misconfigurations or security loopholes, which may become the entry point for attacks.

Through systematic risk assessment and vulnerability analysis, the security threats of the digital dissemination platform of non-legacy Bowen culture are mainly concentrated in data leakage, identity authentication loopholes, cyber-attacks and content tampering. In response to these high-risk risks, a hierarchical security reinforcement strategy should be adopted, including reinforcing access control, upgrading the identity authentication mechanism, enhancing the DDoS protection capability, adopting intelligent intrusion detection, and introducing credible content authentication technology, etc., in order to reduce the security risks and ensure the long-term security and credible dissemination of non-heritage cultural digital resources.

3 Network security protection technology system construction

3.1 Authentication and Access Control

(1) Construction of identity authentication mechanism: Identity authentication is the core link of the security system of the non-legacy Bowen cultural digital communication platform, aiming at ensuring the legitimacy of the access subject and preventing unauthorised access and data leakage. The traditional user name and password based (Username-Password Based Authentication) mode adopted by the current platform has security risks, such as insufficient password strength, repeated use of passwords by users, and leakage of credentials [9]. In order to improve the security of authentication, multi-layer security mechanisms such as Multi-Factor Authentication (MFA), Biometric Authentication, Risk-Based Authentication (RBA), etc. need to be introduced in order to improve the system resistance to attacks. to improve the system's ability to resist attacks. The mathematical model of multi-factor authentication can be expressed as:

$$A = f\left(F_1, F_2, \ldots, F_n\right)$$

A represents the security of authentication; F_i is different authentication factors, such as Password (Knowledge-Based Factor), Hardware Token (Possession-Based Factor), Biometrics (Inherence-Based Factor), etc.; and f is a comprehensive computational function, which can be used as a weighted scoring mechanism for authentication Level Evaluation. The Authentication Trust Level (ATL) can be calculated by the following formula:

$$ATL = \sum_{i=1}^{n} w_i S_i$$

w_i represents the weights of the authentication factors to satisfy $\sum w_i = 1$; S_i represents the security strength score of each factor, which can be assigned according to the factor type and security assessment. For example, the security score of password authentication is generally low ($S_1 \approx 0.3$), while the security of hardware token-based authentication is high ($S_2 \approx 0.8$), and when two-factor authentication (password+hardware token) is used with equal weights, the final trustworthiness is:

$$\text{ATL}=0.5\times0.3+0.5\times0.8=0.55$$

Significantly higher trustworthiness compared to single password authentication (ATL=0.3). Risk-based dynamic authentication can be adaptively adjusted according to user behavioural patterns, and user trustworthiness is calculated using a Bayesian decision model:

$$P(A \mid B)=\frac{P(B \mid A)P(A)}{P(B)}$$

P(A | B) represents the trustworthiness of the user under the behavioural characteristic B; P(B | A) represents the probability of the behavioural pattern of the legitimate user; P(A) is the a priori probability of the legitimate user; and P(B) is the total probability of all the user behaviours. If the user's access behaviour is abnormal (e.g., sudden change of geographic location, change of access device, multiple failed logins in a short period of time, etc.), the authentication policy can be dynamically adjusted, such as triggering secondary authentication or restricting access rights.

(2) Optimisation of access control model: After identity authentication is completed, permission management based on the access control model is required to prevent risks such as unauthorised access and data leakage. The current mainstream access control models include Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Zero Trust Architecture (ZTA). (a) Role-Based Access Control (RBAC)

(a) Role-Based Access Control (RBAC): RBAC is a traditional access control model, and the core idea is to give appropriate permissions to users according to their roles. Its mathematical expression is as follows:

$$P(U)=\bigcup_{R\in Roles(U)}P(R)$$

P(U) is the set of permissions that user U has; Roles(U) represents the set of roles that the user belongs to; P(R) is the set of permissions that role R has. Although the structure of RBAC is clear and simple to manage, its static permission setting is difficult to adapt to the complex business needs, and cannot flexibly control temporary access rights.

(b) Attribute-Based Access Control (ABAC): In order to solve the limitations of RBAC, ABAC adopts the attribute matching mechanism, and carries out dynamic authorisation based on User Attributes, Resource Attributes and Environmental Attributes. Its access decision formula is as follows:

$$D = f(A_U, A_R, \ldots, A_E)$$

D is access decision (allow or deny); A_U is user attributes (e.g., identity, position, department, etc.); A_R is resource attributes (e.g., data category, access level, etc.); and A_E is

environment attributes (e.g., time, geographic location, device type, etc.).ABAC can dynamically adjust the access privileges and improve the security, but with high computational complexity and high requirements on system performance.

(c) Zero Trust Architecture (ZTA): Under the background of Advanced Persistent Threat (APT) and other attacks, the traditional network boundary security model is gradually failing, and ZTA has become a new trend in access control. Its core principle is 'Never Trust, Always Verify' (Never Trust, Always Verify). In the ZTA model, all access requests need to be evaluated based on real-time authentication, device health status, behavioural analysis and other factors, the formula is as follows:

$$T_A = f(I, D, C, B)$$

T_A is the trustworthiness of the access decision; I is the authentication result (MFA score, etc.); D is the device health (security patches, vulnerability scanning results, etc.); C is the access context (network environment, geographic location, etc.); and B is the user behaviour (logging frequency, access pattern, etc.). The zero-trust architecture combines Micro-Segmentation and Continuous Monitoring to ensure that it is difficult for attackers to expand horizontally even if they break through the perimeter defences.

3.2 Data Encryption and Integrity Protection

(1) Data encryption technology system: data encryption is the core means to ensure the data security of the digital dissemination platform of non-legacy Bowen culture, mainly used to prevent unauthorised access, data leakage and tampering. At present, data encryption is divided into three categories: symmetric encryption, asymmetric encryption and hashing algorithms, which are applicable to different security scenarios [10].

(a) Symmetric Encryption: Symmetric encryption is an encryption and decryption method with the same key, featuring high computational efficiency and fast encryption speed, which is commonly used in database storage and data transmission protection. Common algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES) and so on. The encryption process can be expressed by mathematical expressions:

$$C = E_k(P)$$

The decryption process is:

$$P = D_k(C)$$

P stands for plaintext data; C stands for ciphertext data; k is the encryption key; E_k is the encryption function; D_k is the decryption function. aES encryption adopts 128-bit, 192-bit or 256-bit key, and its security is far more than DES. aES-256 encryption is adopted during the storage of non-heritage cultural data, which can ensure the security of the data in databases, distributed storage and cloud environment.

(b) Asymmetric Encryption: Asymmetric encryption uses public and private keys to encrypt and decrypt data, which is suitable for digital signatures, key exchange and other security scenarios. Typical algorithms include RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) and so on. The mathematical expression for asymmetric encryption is as follows:

$$C = E_{K_{pub}}(P)$$

$$P = D_{K_{pri}}(C)$$

K_{pub} is the public key; K_{pri} is the private key; $E_{K_{pub}}$ is the public key encryption function; $D_{K_{pri}}$ is the private key decryption function. Compared with RSA, ECC has higher security and computational efficiency. For example, a 256-bit ECC key is equivalent to a 3072-bit RSA key, which is suitable for secure transmission on mobile and resource-constrained devices[11].

(c) Hashing: Hashing algorithms are used to ensure data integrity and avoid tampering and forgery. Common hash functions include SHA-256 (Secure Hash Algorithm 256-bit), MD5 (Message Digest Algorithm 5) and so on. Hash algorithms map inputs of arbitrary length to output values of fixed length:

H=Hash(P)

H is the hash value; P is the original data; Hash is the hash function (e.g. SHA-256). Before storing the data, the hash value can be calculated first, and retained together when storing for integrity checking.

(2) Data Integrity Protection Mechanisms:Data integrity protection ensures that non-legacy cultural data has not been tampered with or damaged during storage and transmission[12]. The following are common integrity protection mechanisms:

(a) Digital Signature: Digital Signature uses asymmetric encryption to verify the authenticity and integrity of the data, and common algorithms include RSA-SHA256, ECDSA (Elliptic Curve Digital Signature Algorithm) and so on. Its mathematical expression is as follows:

$$S = Sign_{K_{pri}}(H)$$

Verify the signature:

$$Verify_{K_{pub}}(S, H) \rightarrow True\ or\ False$$

If the authentication result is False, the data has been tampered or forged.

(b) Message Authentication Code (MAC, Message Authentication Code), MAC calculates the data digest through the shared key to verify the integrity of the data. Its calculation formula is as follows:

$$MAC = HNAC_k(P)$$

$HNAC_k$ stands for key-based hash message authentication code; k is a shared key. The MAC is calculated before the data is stored or transmitted and verified at the receiving end to ensure that the data has not been tampered with.

(c) Blockchain-Based Provenance, blockchain technology can be used for the traceability and integrity protection of non-legacy cultural digital resources. Before the data is stored, its hash value is calculated and deposited into the blockchain, forming a tamper-proof record:

$$Block_n = Hash(Block_{n-1} + Data + Timestamp)$$

The decentralisation and immutability of blockchain ensures the long-term credibility of NRM cultural data.

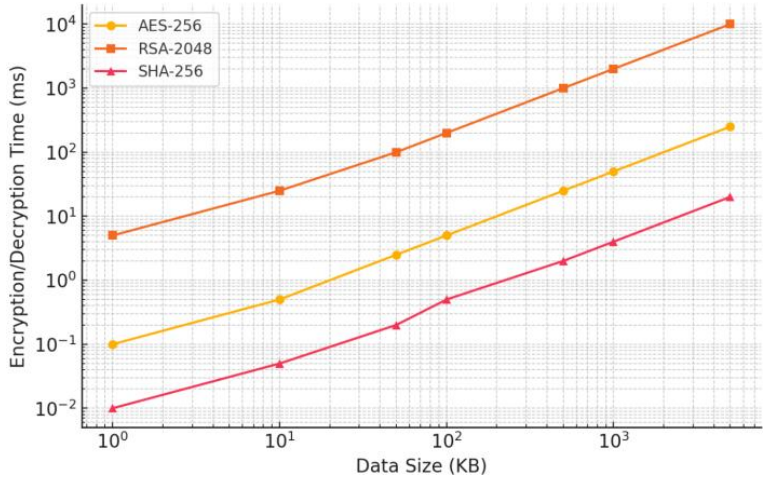

Figure 2: Comparison chart of encryption performance

In terms of data encryption and integrity protection, AES-256 symmetric encryption should be combined to guarantee storage security, RSA-2048/ECC for secure transmission of critical data, and SHA-256 and digital signatures to achieve integrity verification. At the same time, blockchain technology can be introduced to record the data change history and improve the data tamperability. Experimental analyses show that AES-256 has the highest encryption efficiency under large data volume, while RSA is suitable for small data encryption and SHA-256 is suitable for integrity verification.

3.3 Intrusion Detection and Defence Mechanism

(1) Intrusion Detection System (IDS) model construction: Intrusion Detection System (IDS) is an important defence mechanism to safeguard the security of the digital communication platform of non-legacy Bowen culture, and its core objective is to detect, analyse, and respond to abnormal behaviours, in order to prevent cyber-attacks and data manipulation[13].IDS can be divided into Signature-Based Detection, SBD, and Anomaly-Based Detection, ABD. Signature-Based Detection, SBD) and Anomaly-Based Detection (ABD).

(a) Signature-Based Detection (SBD), Signature Detection relies on matching feature libraries of known attack patterns and is suitable for detecting traditional attacks (e.g., SQL injection, XSS, DDoS, etc.). Its detection mechanism can be expressed as:

$$D = \sum_{i=1}^{N} f(A_i, S)$$

D is the detection result (0 means normal, 1 means attack); A_i represents the input network traffic or log data; S is the library of known attack features; $f(A_i, S)$ is the feature matching function, which returns 1 if a match occurs between A_i and S, otherwise it returns 0. Although SBD is fast in detecting, it has limited ability to detect unknown attacks and is difficult to identify Zero-Day Attacks (ZDAs).

(b) Abnormal Behaviour Based Detection (ABD), ABD detects unknown attacks by identifying abnormal patterns of network traffic or user behaviour through machine learning algorithms. Its detection model can be measured by Mahalanobis Distance to measure the

degree of anomaly:

$$M(X)=\sqrt{(X-\mu)^T S^{-1}(X-\mu)}$$

X is the vector of currently observed behaviours; μ is the mean value of normal behaviours; S is the covariance matrix. If M(X) exceeds the set threshold, it is judged as abnormal behaviour.ABD is suitable for detecting complex threats such as Advanced Persistent Threats (APT), insider attacks, etc., but the computational cost is high, and the detection model needs to be continuously optimized[14].

(2) Intrusion Prevention System (IPS) strategy, Intrusion Prevention System (IPS) in the IDS to monitor the attack behaviour, to take automated response measures to prevent damage caused by the attack. The main defence mechanisms include:

(a) Rule-based defence, where the IPS combines access control lists (ACLs) and web application firewalls (WAFs) to automatically block malicious IPs or block suspicious traffic after an attack is detected. The policy can be expressed as follows:

$$R=\sum_{i=1}^{N} W_i \times D_i$$

R is the blocking decision value; W_i is the weight of different attack categories (e.g., SQL injection, XSS, DDoS); and D_i is the probability of detected attacks. If R exceeds the preset threshold T, the blocking policy is triggered.

(b) AI-based dynamic defence, artificial intelligence (AI) combined with reinforcement learning (Reinforcement Learning) to optimize IPS rules to achieve adaptive security protection. Q-Learning is used for policy optimisation:

$$Q(s,a)=(1-\alpha)Q(s,a)+\alpha\left[r+\gamma \max_{a'} Q(s',a')\right]$$

Q(s,a) represents the score of taking action a in state s; α is the learning rate; γ is the discount factor; and r is the current reward value. the AI-IPS can dynamically adjust the defence policy to cope with the ever-changing cyber-attack.

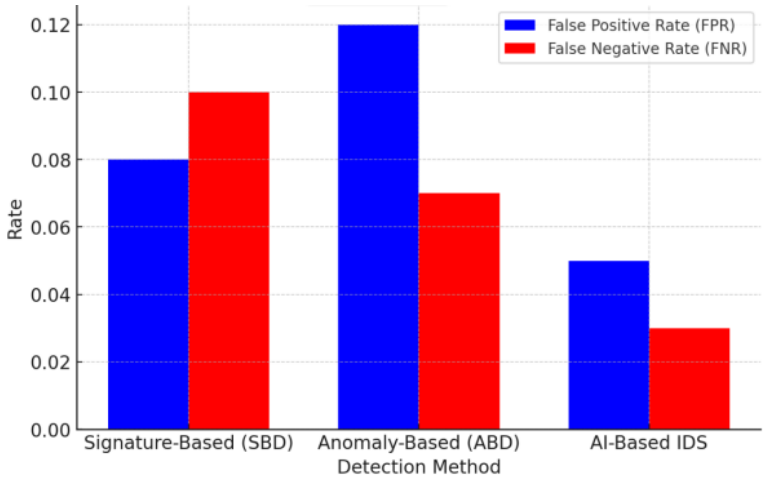

Figure 3: Detection performance graph of SBD, ABD and AI-IDS

The digital communication platform of non-legacy Bowen culture faces multiple intrusion risks, and needs to build a hybrid intrusion detection system (IDS) based on feature detection (SBD) and abnormal behaviour detection (ABD), and combine it with an AI-driven intrusion prevention system (IPS), to achieve automated and intelligent security protection. From the data analysis, AI-IDS has the lowest false alarm rate (5%) and missed alarm rate (3%), which is better than traditional methods in detection accuracy.

4 Security Protection Strategy for Digital Resources of Non-legacy Culture

4.1 Technical Security Protection Specification

The security protection of non-heritage cultural digital resources involves multiple levels such as data storage, transmission, access control and content authenticity. In order to ensure the security, integrity and traceability of non-heritage cultural resources, it is necessary to establish a systematic technical security protection specification to achieve multi-level security from basic security protection to high-level security mechanism.

In terms of data security storage, non-heritage cultural resources are mainly stored in various formats such as text, audio, video and image in databases, cloud storage or distributed storage systems. To prevent data leakage, all stored data should be encrypted using the AES-256 encryption algorithm to ensure that even if the data is illegally accessed, it is impossible to directly parse the plaintext content. Role-based access control (RBAC) or attribute-based access control (ABAC) should be implemented to strictly limit user rights and avoid overstepping access. To improve data availability, it is recommended to adopt distributed storage technology (e.g., IPFS) to reduce the security risks associated with a single point of failure. In addition, an off-site backup strategy should be developed to ensure that data can be quickly recovered in the event of hardware damage or ransomware attacks.

In terms of data transmission and network protection, all data transmission must adopt TLS 1.3 encryption protocol to ensure end-to-end data security and prevent man-in-the-middle attacks (MITM). For API interfaces provided by the platform, OAuth 2.0 and JWT (JSON Web Token) should be combined for authentication to prevent unauthorised access and interface abuse[15]. Meanwhile, in order to cope with large-scale distributed denial-of-service attacks (DDoS), intelligent traffic cleaning and CDN (content distribution network) can be deployed to prevent malicious traffic from affecting platform availability. In addition, in terms of Web security protection, it combines Web Application Firewall (WAF) and Runtime Application Self-Protection (RASP) technologies to provide real-time defence against common threats such as SQL Injection and Cross-Site Scripting Attack (XSS).

Identity authentication and access security are important links in the security management of digital cultural resources, and need to be strengthened by combining Multi-Factor Authentication (MFA) and Zero Trust Architecture (ZTA), which can adopt Time-based One-Time Password (TOTP) + Hardware Token (e.g., FIDO2) to improve the security of identity authentication. In addition, the Zero Trust Architecture based on ABAC combined with User Behaviour Analysis (UEBA) can dynamically determine the access risk of users and adjust the privileges in real time according to the risk level, thus effectively preventing account hijacking, internal misuse and unauthorized access.

The core value of digital resources of non-heritage culture lies in the authenticity and authority of the content, so it is necessary to adopt digital signature and trusted deposit technology to ensure the tamperability of the content. For data such as pictures, audio and video, robust digital watermarking technology can be used to embed invisible identification

information in the files to ensure traceability of content attribution. The use of blockchain technology to record the change history of data can improve the transparency and tamperability of data and enhance the credibility of cultural resources. To guard against risks such as Deepfake, AI-driven content traceability detection can also be used to verify the authenticity of audio and video data to avoid misleading public perception.

To cope with unexpected security events, the platform should establish a security monitoring and emergency response system. Security Information and Event Management (SIEM) technology is used to analyse access logs and abnormal traffic to warn of potential attacks in advance. Combined with the automated threat response (SOAR) system, it can automatically execute response strategies after detecting security threats to reduce the impact of attacks. Red Team & Blue Team Exercise is conducted regularly to simulate real attack scenarios, optimise security defence capabilities and ensure the continuous evolution of the platform security system.

4.2 Multi-Layer Security Defence Model

The security protection of digital resources of non-heritage culture requires the construction of a Multi-Layer Security Defence Model, which combines security policies at multiple levels, such as network, system, data and application, to achieve Defence in Depth and ensure the security and sustainable dissemination of cultural resources under different threat environments. Security in Depth

In terms of network layer security, Zero Trust Architecture (ZTA) should be adopted to dynamically authenticate all access requests and ensure that users, regardless of where they are located, must undergo authentication and permission review before they can access the system. At the same time, the combination of Deep Packet Inspection (DPI), Web Application Firewall (WAF), and DDoS traffic cleaning technologies prevent malicious traffic from entering the system and protect against network layer attacks. Use Secure Access Service Edge (SASE) architecture to optimise remote access security and prevent unauthorised device access. In terms of system layer security, host and server security hardening should be strengthened, including measures such as least privilege configuration, memory protection (DEP/ASLR), and malicious code detection (EDR/XDR). At the same time, the risk of system intrusion is reduced through artificial intelligence (AI)-driven intrusion detection systems (IDS), which use machine learning algorithms to analyse user access behaviours and accurately identify abnormal operations.

In terms of data layer security, End-to-End Encryption (E2EE) technology is used to ensure that data is always encrypted during storage and transmission. Combined with the blockchain traceability mechanism, the integrity hash value of the data is recorded to achieve tamper-proof and traceable data. In addition, Homomorphic Encryption technology is applied to make the data computable in the encrypted state to meet the dual needs of data sharing and security. In terms of application layer security, an artificial intelligence-based threat detection system is used to monitor user interaction data in real time, identify abnormal access patterns, and prevent security risks such as account hijacking and internal abuse. Digital watermarking technology and AI deep forgery detection are used to ensure the authenticity of non-heritage cultural resources and prevent the content from being maliciously modified or forged.

4.3 Security management system and emergency response mechanism

The security management of digital resources of non-heritage culture not only relies on technical means, but also requires a perfect security management system and emergency response mechanism to ensure that network attacks, data leakage, system failures and other security events can be quickly responded to and effectively disposed of, minimising losses

and guaranteeing the long-term security availability of non-heritage cultural resources. In terms of security management system, a comprehensive information security management system (ISMS, Information Security Management System) should be established, covering data classification and hierarchical management, access rights control, log auditing, personnel security training and other contents. Data is graded according to confidentiality, integrity and availability, and access control policies are formulated for different security levels. Regular security audits are conducted, and access logs are analysed using the security information and event management system (SIEM) to detect abnormal activities and ensure internal compliance.

In terms of the emergency response mechanism, a standardised security incident handling process should be built based on the NIST Computer Security Incident Handling Framework (Preparation, Detection & Analysis, Containment & Eradication, Recovery, Post-Incident Activity). When a security event occurs, threats are first detected and analysed in real time by the Intrusion Detection System (IDS) and the Security Operation Centre (SOC), and then measures such as quarantining the infected system, blocking malicious traffic, and fixing vulnerabilities are taken to deal with it. The recovery phase involves rolling back data, repairing system configurations, and continuously optimising response strategies through emergency drills.

Table 2: Table of security incidents and their corresponding response indicators

Type of security incident	Mean Time to Detection (MTTD, Min)	Mean Time to Respond (MTTR, Min)	data loss rate	System recovery time
Cyber attacks (DDoS, APT)	5	15	lower (one's head)(<1%)	30 min
Data leakage (SQL injection, XSS)	10	25	be hit by(5-10%)	60 min
Account hijacking (credential leakage, brute force)	8	20	lower (one's head)(<1%)	45 min
Internal threats (malicious operations, data misuse)	15	30	your (honorific)(10-20%)	90 min
System failures (storage crashes, database corruption)	2	10	Depending on backup	120 min

5 Conclusion

This paper conducts an in-depth study on the security risk analysis, network security protection system construction and security management strategy of the digital communication platform of non-heritage, and puts forward a systematic security guarantee system from identity authentication, data encryption, intrusion detection, defence mechanism to multi-level security defence model, management system and emergency response. The security protection of digital resources of non-heritage culture requires the construction of a deep defence system in multiple dimensions such as network layer, system layer, data layer, application layer, etc., combining advanced technologies such as zero-trust architecture, end-to-end encryption, blockchain traceability, artificial intelligence security analysis, etc., to

improve the security and trustworthiness of the platform. Through the security management system and intelligent emergency response, the impact of security events can be effectively reduced to guarantee the integrity and sustainable dissemination of non-legacy cultural data. In the future, intelligent security strategies should be further strengthened and the adaptive defence capability of the platform should be enhanced to cope with evolving cyber threats and achieve the long-term safe inheritance and digital innovation and development of non-heritage culture.

Funding

Cangnan Agriculture and Rural Bureau Science and Technology Special Project (No. 2024CNYJY05)

References

[1] Aqeel S, Khan U S, Khan S A, et al.Retraction Note: DNA encoding schemes herald a new age in cybersecurity for safeguarding digital assets[J]. Scientific Reports, 2025, 15(1):5028-5028.

[2] Göbel T, Breitinger F, Baier H.Optimising data set creation in the cybersecurity landscape with a special focus on digital forensics: Principles, characteristics, and use cases[J].Forensic Science International: Digital Investigation, 2025, 52301882-301882.

[3] Miranda R P D F, Segura I R, Garrido C Y, et al.Validation of a scale based on the DigComp framework on internet navigation and cybersecurity in older adults[J]. Frontiers in Education, 2025, 101520929-1520929.

[4] Nonhlanhla N C, Sheila K.Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review[J].Journal of Financial Crime, 2025, 32(1):31-48.

[5] Liang X, Xu Y.A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud[J].Computers & Security, 2025, 151104339-104339.

[6] Mari A.Cybersecurity in digital supply chains in the procurement process: introducing the digital supply chain management framework[J].Information & Computer Security, 2025, 33(1):5-24.

[7] Morshed A, Khrais T L.Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region[J].Journal of Risk and Financial Management, 2025, 18(1):41-41.

[8] Zhu D, Wei Y, Cai J, et al.A security data detection and management method in digital library network based on deep learning[J].Frontiers in Physics, 2025, 121492114-1492114.

[9] Muhlert M.“Navigating the Cyber Maze: insights and humor on the digital frontier” — a multi-dimensional exploration of cybersecurity with heart and humor[J].EDPACS,

2025, 70(1):52-57.

[10] Palanichamy N, R. M, U.S. R.Digital Twins and Cybersecurity:Safeguarding the Future of Connected Systems[M].John Wiley & Sons, Inc.:2024-12-19.

[11] Tridgell J.Open or closing doors? The influence of ‘digital sovereignty’ in the EU's Cybersecurity Strategy on cybersecurity of open-source software[J].Computer Law & Security Review: The International Journal of Technology Law and Practice, 2025, 56106078-106078.

[12] Kumar A, Chaudhary K N, Shastri S A, et al.Digital Defence:Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics[M].CRC Press:2024-12-03.

[13] Singh T.Digital Resilience, Cybersecurity and Supply Chains[M].Taylor & Francis: 2024-12-03. DOI:10.4324/9781003604969.

[14] Saeed S, Gull H, Aldossary M M, et al.Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications[J].Information, 2024, 15(12):764-764.

[15] Fadare, Adetoye A, Omiko, et al.Securing the Future: Cybersecurity Challenges and Solutions inDigital Oilfields[J].Asian Journal of Research in Computer Science, 2024, 17(11):134-154.