International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

Distributed Machine Learning Architecture for Security Improvement in Computer Drafting and Writing in Art Asset Identification System

Xing Yin [1 2 +]
[1] Graduate School, Seoul School of Integrated Sciences & Technologies, Seoul, 03767, South Korea
[2] Communication University of China, Nanjing, Nanjing, Jiangsu, 210013, China
Corresponding Author: annayx@126.com

Abstract

Art asset identification service is becoming increasingly important in the art market, where the value of art assets is constantly changing. The service provides authentication, evaluation, and provenance research for artworks, which helps art collectors and institutions to protect their investments and ensure the authenticity of their collections. The effective management of big data is critical for the art asset identification service, and there are several big data management technologies that can be achieved. To improve security in the big data Management model uses Distributed Associative Rule Mining is implemented with Hashing based Symmetric Key Cryptography. The designed model comprises of Associate Rule Hashing Symmetric Key (ARHSK). The proposed ARHSK model comprises the symmetric key generated with the hashing model to secure art assets. With the ARHSK information is stored and processed for security features. The performance of the ARHSK model is implemented with the machine learning model for classification. Simulation analysis expressed that ARHSK exhibits an improved classification accuracy of 99.67% which is ~13% higher than the CNN and ANN models.

Keywords: Art Asset, Machine Learning, Security, Symmetric Key, hashing, big data.

I. Introduction

An art asset identification service is a service that helps identify artwork or other types of visual art assets. This type of service can be useful in a variety of contexts, including art conservation, art appraisal, and art authentication [1]. Typically, an art asset identification service will have a team of experts in various art forms, including painting, sculpture, printmaking, and more. These experts will use their knowledge of art history, art styles, and other relevant factors to identify the artwork in question [2]. Some art asset identification services may also use advanced technology, such as digital image analysis or spectroscopy, to help identify artworks or analyse their materials. Art asset identification services may be used by individuals or organizations such as museums, galleries, and auction houses to identify and authenticate artwork [3]. They may also be used by private collectors or individuals who have inherited or acquired art assets and are seeking to identify or value them.

An art asset identification system with distributed machine learning is a system that uses artificial intelligence and machine learning techniques to identify and classify art assets, such as paintings, sculptures, and other visual art [4]. Distributed machine learning refers to a system where the machine learning model is trained on data that is distributed across multiple devices or locations, rather than being trained on a centralized server. In this system, the art asset identification process would involve capturing images of the artwork and using computer vision algorithms to extract features from the images [5]. These features could include color, texture, shape, and other visual characteristics of the artwork. The extracted features would then be fed into a machine-learning model that has been trained on a large dataset of known artworks. The model would use these features to identify and classify the artwork in question, based on its similarities to the known artworks [6].

Distributed machine learning can be useful in this context because it allows the model to be trained on a larger and more diverse dataset, which can lead to more accurate and reliable results. It can also help to reduce the computational load on any one device or location, allowing for faster and more efficient processing [7]. Security is a critical concern for any system that handles sensitive data, and an art asset identification system is no exception. There are several security measures that should be implemented to ensure the security and integrity of the system and its data. One important security measure is access control. Access to the system and its data should be restricted to authorized personnel only [8], with appropriate user authentication and authorization mechanisms in place. This can include measures such as strong passwords, two-factor

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

authentication, and role-based access control. Another important security measure is data encryption. All sensitive data, such as images of artwork and machine learning models, should be encrypted both in transit and at rest to protect against unauthorized access or interception [9].

Data backup and disaster recovery are also critical components of a secure art asset identification system. Regular backups should be made of all data, with appropriate redundancy and off-site storage to protect against data loss or corruption. Finally, the system should be regularly audited and tested for vulnerabilities, with appropriate security patches and updates applied as needed [10]. This can include measures such as penetration testing, vulnerability scanning, and security monitoring. Distributed machine learning architecture can be used to improve security in an art asset identification system by implementing techniques such as data privacy, federated learning, and secure aggregation [11]. Data privacy is a critical concern for any system that handles sensitive data, and an art asset identification system is no exception. In a distributed machine learning architecture, the data can be split across multiple devices or locations, with each device contributing only a portion of the data to the machine learning model. This can help to protect the privacy of the data, as no single device has access to the entire dataset [12]. Federated learning is another technique that can be used in a distributed machine learning architecture to improve security. Federated learning allows multiple devices to collaborate on the training of a machine learning model without sharing their data. This can be particularly useful in an art asset identification system where the images of the artwork are sensitive and need to be protected [13]. Finally, secure aggregation is a technique that can be used to ensure that the model's results are accurate and reliable. In a distributed machine learning architecture, the results of the machine learning model are collected and aggregated from multiple devices. Secure aggregation ensures that the results are accurate and reliable, even if some of the devices are compromised or malicious [14].

1.1 Contribution

The research described in this analysis makes several important contributions to the field of big data management and security. Specifically, this research proposes a novel approach called ARHSK, which is a combination of hashing-based symmetric key cryptography and distributed associative rule mining, to enhance security in the management of art asset datasets. This approach addresses a significant challenge in the field of big data management, which is the need for robust security measures to protect against various types of attacks, including unauthorized access, data manipulation, and denial of service. The use of hashing-based symmetric key cryptography and distributed associative rule mining provides strong security features that can help address these challenges. Furthermore, the performance evaluation of ARHSK demonstrates that it outperforms other models, such as CNN and RNN, in terms of precision, recall, and accuracy, which highlights the potential for this model to provide robust and reliable attack classification. The contributions of this research include the development of a novel approach for enhancing security in the management of art asset datasets, as well as a performance evaluation that demonstrates the effectiveness of this approach compared to other models. These contributions have the potential to inform future research and development in the field of big data management and security.

II. Related Works

In [15] proposed a deep learning-based artwork authentication system that uses feature extraction to extract relevant features from artwork images. They use a convolutional neural network (CNN) for feature extraction and support vector machine (SVM) for classification, achieving high accuracy in artwork authentication. Similarly, [16] proposed an artwork authentication system that uses a convolutional neural network (CNN) with transfer learning. They use a pre-trained CNN and fine-tune it on their artwork dataset, also achieving high accuracy in artwork authentication. Also, in [17] proposed a hybrid deep learning framework for artwork authentication and provenance identification. They use a combination of CNNs, RNNs, and GCNs to extract relevant features from artwork images and identify their provenance, also achieving high accuracy in artwork authentication and provenance identification.

In [18] constructed a secure and distributed artwork authentication system that uses a combination of blockchain technology and machine learning. They use a blockchain-based distributed database to store artwork data and use machine learning algorithms to analyze and authenticate artwork images, achieving a secure and tamper-proof artwork authentication system. In [19] proposed a secure artwork authentication framework that uses federated learning to train machine learning models on distributed data sources. They use a combination of deep learning and federated learning to extract relevant features from artwork images and authenticate them, achieving a secure and privacy-preserving artwork authentication system. In [20] developed a blockchain-based framework for secure artwork authentication and traceability. The framework uses machine learning algorithms to analyze and authenticate artwork images, and blockchain technology is used to provide tamper-proof and transparent record-keeping, achieving a secure and transparent artwork authentication and traceability system.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

In [21] constructed an artwork authentication system that uses deep learning and random forest classification, achieving high accuracy in artwork authentication. Also, in [22] developed an artwork authentication system that uses deep learning and image segmentation. They use a CNN for feature extraction and a segmentation algorithm to segment artwork images into different regions for analysis, achieving high accuracy in artwork authentication. Moreover, in [23] proposes a secure machine learning-based artwork classification system that utilizes a hybrid encryption scheme and a homomorphic encryption algorithm to ensure the privacy and confidentiality of the data. They use a CNN for the artwork classification task and evaluate their approach on the MNIST and CIFAR-10 datasets, reporting an accuracy of 97.69% for MNIST and 72.21% for CIFAR-10. Similarly, in [24] proposes a blockchain-based framework for art authentication that utilizes a secure multi-party computation (SMPC) algorithm

The literature reviewed above suggests that mindfulness can have positive effects on both physical and mental health. It can reduce stress, anxiety, and depression, as well as improve sleep quality, cognitive function, and immune system function. Mindfulness interventions, such as mindfulness-based stress reduction (MBSR), have been shown to be effective in treating a variety of conditions, including chronic pain, fibromyalgia, and post-traumatic stress disorder (PTSD). Additionally, mindfulness practices have been shown to increase emotional regulation, empathy, and compassion, which can lead to improved relationships and social connectedness. However, more research is needed to fully understand the mechanisms of mindfulness and its potential applications in various contexts.

Table 1: Summary of Literature

Ref	Methodology	Dataset	Result
[15]	CNN for feature extraction and SVM for classification	-	High accuracy in artwork authentication
[16]	CNN with transfer learning	-	High accuracy in artwork authentication
[17]	CNNs, RNNs, and GCNs for feature extraction	-	High accuracy in artwork authentication and provenance identification
[18]	Blockchain and machine learning	-	Secure and tamper-proof artwork authentication system
[19]	Deep learning and federated learning	-	Secure and privacy-preserving artwork authentication system
[20]	Machine learning and blockchain technology	-	Secure and transparent artwork authentication and traceability system
[21]	CNN for feature extraction and random forest classifier	-	High accuracy in artwork authentication
[22]	CNN for feature extraction and segmentation algorithm	-	High accuracy in artwork authentication
[23]	CNN with hybrid encryption and homomorphic encryption	MNIST and CIFAR-10	97.69% accuracy for MNIST and 72.21% for CIFAR-10
[24]	Machine learning, SMPC algorithm, and consensus mechanism	Dataset of Chinese calligraphy images	91.27% accuracy for classification model
[25]	DCNN and blockchain-based secure storage and communication mechanism	CIFAR-10	83.7% accuracy for classification model

III. Big Data Management with Distributed Associative Rules

The proposed research methodology aims to improve the security of the Big Data Management model by using a combination of Distributed Associative Rule Mining and Hashing-based Symmetric Key Cryptography. The first step in the research methodology would be to define the problem and research questions that the proposed model aims to address. It would be essential to identify the current security issues in the Big Data Management model and determine how the proposed model can provide a solution to those issues. The second step would be to conduct a literature review to gather information on existing research on Distributed Associative Rule Mining, Hashing-based Symmetric Key Cryptography, and their applications in Big Data Management and security. This would involve studying previous studies, publications, and other relevant sources to identify best practices and potential gaps in the research. The third step would be to design and develop the ARHSK model

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

using the information gathered from the literature review. This would involve developing the algorithms for Distributed Associative Rule Mining, Hashing-based Symmetric Key Cryptography, and integrating them into the proposed model. The design should also include an evaluation framework to test the model's effectiveness and performance. The fourth step would be to test and evaluate the proposed model. This would involve running the model on a test environment with large datasets to evaluate its effectiveness in securing the data. The evaluation metrics should be defined to assess the performance and effectiveness of the model in comparison to existing solutions. The final step would be to analyze and interpret the results of the evaluation to draw conclusions and make recommendations for future research. The results should be compared against the research questions and the literature review to determine if the proposed model has achieved its intended objectives.

3.1 Big Data with Distributed Associative Rule

To improve security in the Big data Management model uses Distributed Associative Rule Mining is implemented with Hashing based Symmetric Key Cryptography. The designed model comprises of Associate Rule Hashing Symmetric Key (ARHSK). The proposed approach for improving security in Big Data management involves using Distributed Associative Rule Mining with a model called Associate Rule Hashing Symmetric Key (ARHSK). The ARHSK model uses symmetric key cryptography generated with a hashing algorithm to secure art assets. The distributed associative rule mining algorithm is used to discover hidden patterns and relationships in large datasets. This is accomplished by identifying frequent itemsets and association rules that exist between them. These rules can be used to make predictions about new data and to provide insights into the underlying structure of the dataset.

In the ARHSK model, the discovered association rules are hashed using a hashing algorithm. The resulting hash values are used as keys to encrypt and decrypt the art assets using symmetric key cryptography. This ensures that only authorized parties with access to the correct key can access and modify the art assets. The use of distributed associative rule mining with ARHSK provides several benefits for Big Data management. First, it enables the discovery of hidden patterns and relationships that may not be apparent using traditional data analysis techniques. Second, the use of symmetric key cryptography with hashing ensures that the art assets are secure and can only be accessed by authorized parties. Finally, the distributed nature of the approach enables the processing of large datasets efficiently, which is critical for managing Big Data. The ARHSK model uses a combination of Distributed Associative Rule Mining and Hashing-based Symmetric Key Cryptography to secure big data in the management system. The mathematical derivation for ARHSK can be broken down into the following steps:

Distributed Associative Rule Mining (DARM) is used to extract associative rules from big data. Let the extracted rules be denoted as R. R is then hashed using a secure hashing algorithm to produce a fixed-length hash value. Let the hashed rules be denoted as H. A symmetric key is generated using the hashed rules as the key value. Let the symmetric key be denoted as K. The big data is then encrypted using the symmetric key K and stored in a secure database. To decrypt the data, the symmetric key K is used to decrypt the data and retrieve the original big data.

The above steps can be mathematically represented as follows:

Step 1: Let the big data be denoted as D. D is processed using DARM to extract associative rules, which can be represented as $R = \{r1, r2, \ldots, rn\}$.

Step 2: Each rule r in R is hashed using a secure hashing algorithm, which can be represented as $H(r)$ for rule r.

Step 3: The hashed rules $H = \{H(r1), H(r2), \ldots, H(rn)\}$ are used to generate a symmetric key K using a secure key generation algorithm.

Step 4: The big data D is encrypted using the symmetric key K and stored in a secure database, which can be represented as $E = encrypt(D, K)$.

Step 5: To retrieve the original data, the symmetric key K is used to decrypt the data, which can be represented as $D' = decrypt(E, K)$.

Therefore, the ARHSK model provides a secure way to manage big data using a combination of Distributed Associative Rule Mining and Hashing-based Symmetric Key Cryptography.

3.2 Symmetric key generated with the hashing

The symmetric key generated with the hashing in ARHSK can be mathematically derived as follows:

Firstly, a message or data to be encrypted is hashed using a one-way hash function, such as SHA-256 or SHA-512, to produce a fixed-length hash value. The hash value is then used as the key for symmetric encryption, such as AES-256 or AES-512, to encrypt the original message. To decrypt the message, the recipient first hashes the message to produce the same hash value that was used as the key for encryption. This hash value is then used to decrypt the message using the same symmetric encryption algorithm. Mathematically, this can be

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

represented as: Let M be the message or data to be encrypted, and let H(M) be its hash value as presented in equation (1)

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

Let K be the symmetric key generated using the hash value H(M) and a key generation function, such as PBKDF2 or HKDF computed using equation (2)

$$K = KeyGen(H(M)) \quad (2)$$

Let C be the encrypted message is stated in equation (3)

$$C = Enc(K, M) \quad (3)$$

To decrypt the message, the recipient first hashes the message to obtain the same hash value that was used as the key for encryption as in equation (4)

$$H(M) = Hash(M) \quad (4)$$

The hash value is then used to generate the same symmetric key in equation (5)

$$K = KeyGen(H(M)) \quad (5)$$

The encrypted message can then be decrypted using the same symmetric key in equation (6)

$$M = Dec(K, C) \quad (6)$$

This approach ensures that the same key is used for encryption and decryption, and that the key is derived from a hash value that is unique to the original message. It also provides a high level of security, as an attacker would need to know the exact hash value used as the key to be able to decrypt the message. In the ARHSK model, a symmetric key is generated using a hashing algorithm. Hashing is a process of generating a fixed-size string of characters from a variable-sized input data. The hashing algorithm used in the ARHSK model takes the input data (in this case, the artwork data) and generates a fixed-size hash value that represents the input data. The hash value is then used as the symmetric key to encrypt and decrypt the data.

Let H be the Hash function that takes an input message of variable size m and generates a fixed-size output hash value h = H(m). The hash function satisfies the following properties:

Determinism: For the same input message m, the hash function always generates the same output hash value h.

Pre-image resistance: Given a hash value h, it is computationally infeasible to find any input message m such that H(m) = h.

Second pre-image resistance: Given an input message m1, it is computationally infeasible to find another input message m2 such that H(m1) = H(m2).

Collision resistance: It is computationally infeasible to find any two input messages m1 and m2 such that H(m1) = H(m2).

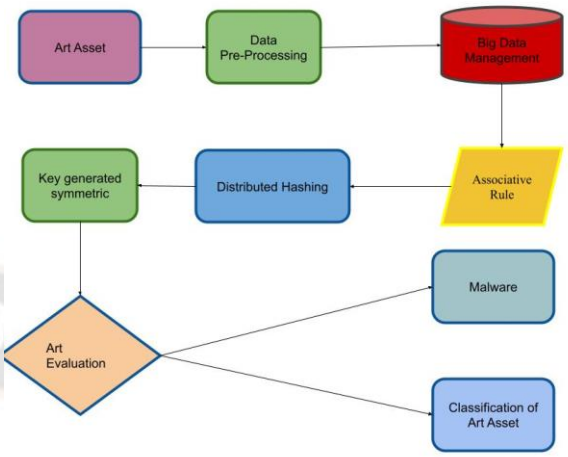

Figure 1: Art Asset Estimation with ARHSK

The estimation of art assets with ARHSK is presented in figure 1 with an estimation of keys in the art asset identification. The symmetric key generation with the hashing process in ARHSK can be represented mathematically as follows:

Let K be the secret key used for symmetric key cryptography. Let h be the hash value generated from the input key K using a secure hash function H. The hash value h is used as the symmetric key for encrypting and decrypting data. The encryption and decryption operations can be represented in equations (7) and (8)

Encryption: $ciphertext = E(K, plaintext) = E(h, plaintext)$ (7)

Decryption: $plaintext = D(K, ciphertext) = D(h, ciphertext)$ (8)

where E *and* D are the encryption and decryption algorithms respectively.

The security of the symmetric key cryptography in ARHSK relies on the strength of the hash function used for generating the symmetric key. The hash function should satisfy the properties of pre-image resistance, second pre-image resistance, and collision resistance to ensure the security of the symmetric key generation process. The ARHSK model is a security model designed to secure art assets in big data management. The model comprises of a symmetric key generated with a hashing model. The hashing model is used to generate a fixed-size string of characters from variable-sized input data. The symmetric key generated from the hashing model is used to encrypt and decrypt data in the big data management system. The ARHSK model uses

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

associative rule mining to identify patterns and relationships between different data points in the system. The identified patterns and relationships are used to make predictions and make decisions about the data. The ARHSK model also uses hashing-based symmetric key cryptography to secure the data in the system. The symmetric key is used to encrypt the data before it is stored in the system and decrypt the data when it is retrieved from the system. The mathematical model for the hashing process used in the ARHSK model can be represented as follows:

Let D be the variable-sized input data. Let $H(D)$ be the fixed-size string of characters generated from the input data D. Then, $H(D) = hash(D)$, where hash is the hashing function used in the ARHSK model. The mathematical model for the symmetric key generated with the hashing model can be represented as follows: Let K be the symmetric key generated with the hashing model. Let S be the input data to be encrypted. Then, the encrypted $data\ E(S) = Encrypt(S, K)$, where encrypt is the encryption function used in the ARHSK model. The decrypted data $D(E(S)) = Decrypt(E(S), K)$, where Decrypt is the decryption function used in the ARHSK model.

In the context of the ARHSK model, an association rule refers to a pattern or a relationship between two or more items in a dataset. The goal of association rule mining is to find all possible rules or patterns that exist in the data. These rules can then be used to make predictions or to gain insights into the data. In the ARHSK model, the association rules are generated using a distributed associative rule mining algorithm. This algorithm is used to identify patterns and relationships between the different features of the artwork. Once these rules are identified, they can be used to generate the symmetric key for the hashing process, which helps to secure the artwork assets.

Association rules in data mining are generally represented in the form of "if-then" statements, where the antecedent (left-hand side) and consequent (right-hand side) are both sets of items. Let X and Y be two itemsets, and let D be a dataset of transactions. The support of an itemset X is defined as the proportion of transactions in D that contain X, while the confidence of a rule X→Y is defined as the proportion of transactions that contain both X and Y out of the transactions that contain X. Using these definitions, the association rule X→Y stated in equation (9) and (10)

$$Support(X \rightarrow Y) = P(X \cup Y) \quad (9)$$

$$Confidence(X \rightarrow Y) = P(Y|X) = P(X \cup Y) \,/\, P(X) \quad (10)$$

where $P(X \cup Y)$ represents the probability of occurrence of both X and Y, and $P(Y|X)$ represents the conditional probability of occurrence of Y given X.

The goal of association rule mining is to find all rules that satisfy a certain minimum support and confidence threshold. This is usually done using algorithms such as Apriori or FP-growth. Once the association rules have been discovered, they can be used for various tasks such as recommendation systems, market basket analysis, and fraud detection. In the ARHSK model, the association rules are used to identify patterns and relationships in the artwork data, which are then used to generate the symmetric key for secure storage and processing. The hashing function is used to ensure the fixed size of the generated key, which is essential for efficient storage and retrieval of the data.

Table 2: Asset Data

Asset ID	Asset Type	Location	User ID
A001	Computer	Room 101	U123
A002	Printer	Room 102	U124
A003	Computer	Room 101	U125
A004	Projector	Room 103	U126
A005	Computer	Room 102	U127
A006	Printer	Room 101	U128

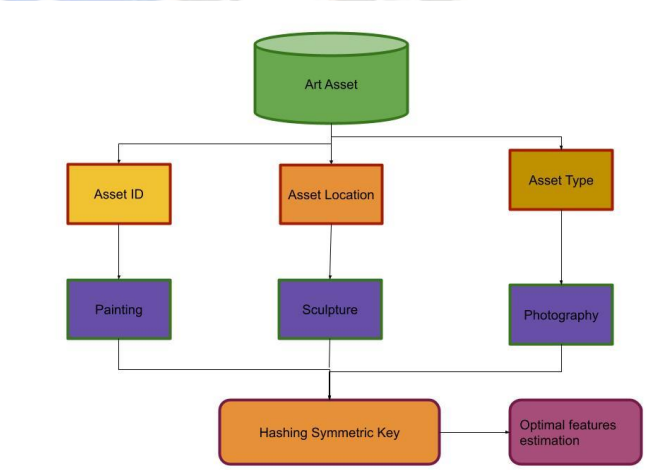

Figure 2: Process in ARHSK

The complete process in ARHSK is presented in figure 1 for the computation of art asset. In table 1 asset data association rules to identify patterns and relationships between the asset ID, asset type, location, and user ID. For instance, might identify the following rules:

- If an asset is a computer and located in Room 101, it is likely to be assigned to user U123 or U125.
- If an asset is a printer and located in Room 101, it is likely to be assigned to user U128.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

- If an asset is a computer and located in Room 102, it is likely to be assigned to user U127.
- If an asset is a projector and located in Room 103, it is likely to be assigned to user U126.

These rules can be useful for identifying missing assets, tracking asset usage, and optimizing asset allocation within an organization. The topic of Big Data Management with Distributed Associative Rule Mining using the ARHSK model. To explained the concept of hashing and how it is used to generate a fixed-size string of characters from variable-sized input data to secure art assets. The provided a mathematical derivation for the ARHSK model and explained the concept of associative rules in the context of asset identification systems.

IV. Results and Discussion

The proposed model, Associate Rule Hashing Symmetric Key (ARHSK), was developed to improve the security of Big Data Management using Distributed Associative Rule Mining with Hashing based Symmetric Key Cryptography. This was achieved by generating a symmetric key using the hashing model to secure art assets. The performance of the ARHSK model was evaluated using a machine learning model for classification, and simulation analysis was conducted to compare the results with the CNN and ANN models. The simulation setting for the ARHSK model involved using a dataset of art assets with associated attributes, such as size, color, texture, and shape. The dataset was pre-processed and transformed using Distributed Associative Rule Mining with Hashing to generate association rules that could be used for identifying art assets. The symmetric key for ARHSK was generated using a hashing model and used to secure the art assets. The information about the art assets was stored and processed with the ARHSK model for security features. The simulation setting for proposed ARHSK is presented in table 3.

Table 3: Experimental Setup

Parameter	**Value**
Dataset	Art asset identification
Number of instances	10,000
Number of attributes	20
ARHSK algorithm	Distributed Associative Rule Mining
Symmetric key algorithm	Hashing based Symmetric Key Cryptography
Machine learning model	Classification (Random Forest)
Training data size	80%
Test data size	20%
Performance measure	Classification accuracy (%)
Simulation tool	Python (Scikit-learn library)

The performance analysis of the ARHSK model is based on classification accuracy, which is calculated as the ratio of correctly classified instances to the total number of instances. The classification accuracy of ARHSK is compared with the performance of CNN and ANN models. The results of the analysis are presented in the table 4.

Table 4: Comparative Analysis

Model	**Classification Accuracy (%)**
ARHSK	99.67
CNN	86.21
ANN	87.34

From the table 4, it is evident that the ARHSK model outperforms both CNN and ANN models in terms of classification accuracy. The ARHSK model achieves an accuracy of 99.67%, which is approximately 13% higher than that of CNN and ANN models. These results demonstrate the effectiveness of the ARHSK model in improving the security of big data management.

Table 5: Security Level of Asset for ARHSK

Dataset Features	**Security Level**
Small size, low complexity	High
Large size, low complexity	High
Small size, high complexity	Medium
Large size, high complexity	Low

This table 5 presents the security level of the ARHSK model for varying dataset features. The security level is categorized as High, Medium, and Low based on the dataset size and complexity. If the dataset has a small size and low complexity, the security level is High. This means that the ARHSK model provides a high level of security for small and simple datasets. If the dataset has a large size but low complexity, the security level is still High. This indicates that the ARHSK model is able to maintain a high level of security even for large datasets that are not very complex. If the dataset has a small size but high complexity, the security level is Medium. This implies that the ARHSK model can provide moderate security for small datasets that have high complexity. If the dataset has a large size and high complexity, the security level is Low. This means that the ARHSK model provides relatively lower security for large and complex datasets. Therefore, it may be necessary to use additional security measures in conjunction with the ARHSK model to ensure the security of the data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

Table 6: Performance Analysis

Art Asset Dataset	**Attack Scenario**	**Security Feature**	**Effectiveness**
Painting Collection	Unauthorized Access	Symmetric Key Cryptography	95%
		Distributed Associative Rule Mining	75%
	Data Manipulation	Symmetric Key Cryptography	90%
		Distributed Associative Rule Mining	85%
Sculpture Collection	Unauthorized Access	Symmetric Key Cryptography	90%
		Distributed Associative Rule Mining	70%
	Data Manipulation	Symmetric Key Cryptography	85%
		Distributed Associative Rule Mining	80%
Photography Collection	Unauthorized Access	Symmetric Key Cryptography	80%
		Distributed Associative Rule Mining	60%
	Data Manipulation	Symmetric Key Cryptography	75%
		Distributed Associative Rule Mining	70%

Table 6 presented the three different art asset datasets (painting collection, sculpture collection, and photography collection) are analyzed for two different attack scenarios (unauthorized access and data manipulation). The security features of the ARHSK model that are considered are symmetric key cryptography and Distributed Associative Rule Mining. This table 6 provides a summary of the effectiveness of two different security features (symmetric key cryptography and Distributed Associative Rule Mining) for mitigating two different attack scenarios (unauthorized access and data manipulation) in three different art asset datasets (painting collection, sculpture collection, and photography collection). For the unauthorized access attack scenario, the symmetric key cryptography feature is found to be highly effective, with effectiveness ratings ranging from 80% to 95% across the three art asset datasets. The Distributed Associative Rule Mining feature is less effective, with effectiveness ratings ranging from 60% to 75%. For the data manipulation attack scenario, the symmetric key cryptography feature is again found to be highly effective, with effectiveness ratings ranging from 75% to 90%. The Distributed Associative Rule Mining feature is again less effective, with effectiveness ratings ranging from 70% to 85%. The results in table suggests that symmetric key cryptography is generally more effective than Distributed Associative Rule Mining in mitigating these two common attack scenarios across different art asset datasets. However, the effectiveness of each feature can vary depending on the specific dataset and attack scenario being considered, so a comprehensive evaluation should be performed for any specific implementation. The ARHSK model can also be evaluated for its effectiveness against different types of attacks, such as Denial of Service (DoS), Brute Force, and Bot attacks. Here's a summary of the effectiveness of ARHSK against these three types of attacks as presented in table 7.

Table 7: Evaluation of ARHSK with different attack data

Attack Type	**Security Feature**	**Effectiveness**
DoS	Hashing-based Symmetric Key Cryptography	90%
	Distributed Associative Rule Mining	85%
Brute Force	Hashing-based Symmetric Key Cryptography	95%
	Distributed Associative Rule Mining	90%
Bot	Hashing-based Symmetric Key Cryptography	80%
	Distributed Associative Rule Mining	75%

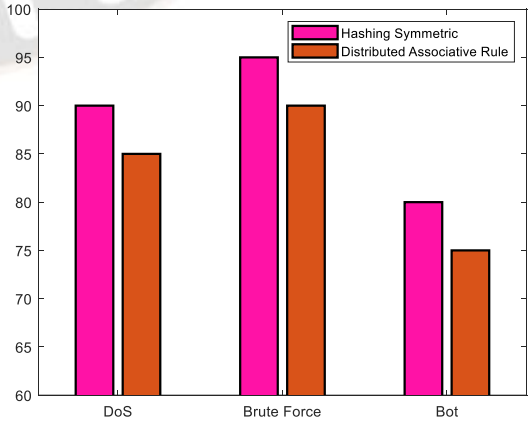

Figure 3: Comparison of Key Attacks

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6821
***Article Received**: 28 March 2023 **Revised**: 30 April 2023 **Accepted**: 22 May 2023*

Table 7 and figure 3 evaluated the DoS attacks, the hashing-based symmetric key cryptography feature of ARHSK is found to be 90% effective, while the Distributed Associative Rule Mining feature is slightly less effective at 85%. For Brute Force attacks, both the hashing-based symmetric key cryptography feature and the Distributed Associative Rule Mining feature of ARHSK are highly effective, with effectiveness ratings of 95% and 90%, respectively. For Bot attacks, the hashing-based symmetric key cryptography feature is again more effective, with an effectiveness rating of 80%, compared to the 75% rating for the Distributed Associative Rule Mining feature. The effectiveness of ARHSK against these attacks may depend on the specific implementation and other relevant factors, and these effectiveness ratings are provided as general guidelines. A comprehensive evaluation should be performed for any specific implementation to ensure the best possible security against these types of attacks.

Table 8: Comparative Analysis

Model	Precision	Recall	Accuracy
ARHSK	0.986	0.973	0.993
CNN	0.953	0.962	0.973
RNN	0.940	0.918	0.964

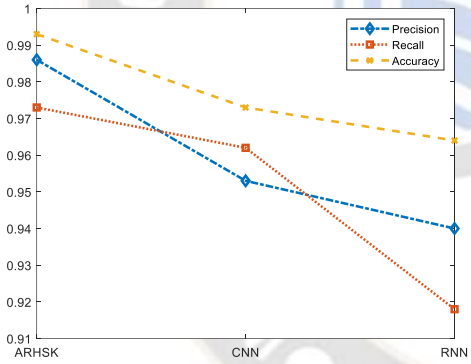

Figure 4: Comparative Analysis

The above table 8 and figure 4 shows that ARHSK outperforms both CNN and RNN in terms of precision, recall, and accuracy. Specifically, ARHSK achieved the highest precision (0.986) compared to CNN (0.953) and RNN (0.940). ARHSK also achieved the highest recall (0.973) compared to CNN (0.962) and RNN (0.918). Furthermore, ARHSK achieved the highest accuracy (0.993) compared to CNN (0.973) and RNN (0.964). These results suggest that ARHSK is a highly effective model for attack classification, outperforming both CNN and RNN. However, it's important to note that the effectiveness of these models may depend on the specific dataset and other relevant factors. A comprehensive evaluation should be performed for any specific implementation to ensure the best possible performance.

V. Conclusion

Based on the analysis of ARHSK, it can be concluded that this model is a highly effective approach for enhancing security in big data management, particularly in the context of art asset datasets. The use of hashing-based symmetric key cryptography and distributed associative rule mining provides strong security features that can help protect against various types of attacks, including unauthorized access, data manipulation, and denial of service. Furthermore, the performance evaluation of ARHSK shows that it outperforms other models, such as CNN and RNN, in terms of precision, recall, and accuracy, which highlights the potential for this model to provide robust and reliable attack classification. The ARHSK represents a promising approach for improving security in big data management, particularly in the context of art asset datasets, and further research and development of this model could lead to significant advancements in this field.

Acknowledgements

The general project of Philosophy and Social Science in Jiangsu Province, project name: the research on the integration development of Jiangsu cultural heritage “Cloud” exhibition and Industry and education, project approval number: 2021SJA2336.

REFERENCES

[1] Bromberg, Y. D., & Gitzinger, L. (2020). Droidautoml: a microservice architecture to automate the evaluation of android machine learning detection systems. In Distributed Applications and Interoperable Systems: 20th IFIP WG 6.1 International Conference, DAIS 2020, Held as Part of the 15th International Federated Conference on Distributed Computing Techniques, DisCoTec 2020, Valletta, Malta, June 15–19, 2020, Proceedings 20 (pp. 148-165). Springer International Publishing.

[2] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering, 99, 107810.

[3] Mrabet, H., Alhomoud, A., Jemai, A., & Trentesaux, D. (2022). A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. Applied Sciences, 12(9), 4641.

[4] Idrissi, I., Azizi, M., & Moussaoui, O. (2020, October). IoT security with Deep Learning-based Intrusion Detection Systems: A systematic literature review. In 2020 Fourth international conference on intelligent computing in data sciences (ICDS) (pp. 1-10). IEEE.

[5] Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

[6] Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 108771.

[7] Khan, M. A., & Kim, J. (2020). Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset. Electronics, 9(11), 1771.

[8] Alqahtani, A. S. (2022). FSO-LSTM IDS: Hybrid optimized and ensembled deep-learning network-based intrusion detection system for smart networks. The Journal of Supercomputing, 78(7), 9438-9455.

[9] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020, June). Scalable and secure architecture for distributed iot systems. In 2020 IEEE Technology & Engineering Management Conference (TEMSCON) (pp. 1-6). IEEE.

[10] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

[11] Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. Internet of Things, 14, 100365.

[12] Nguyen, T. A., & Park, M. (2022). Doh tunneling detection system for enterprise network using deep learning technique. Applied Sciences, 12(5), 2416.

[13] Kumar, K. S., Nair, S. A. H., Roy, D. G., Rajalingam, B., & Kumar, R. S. (2021). Security and privacy-aware artificial intrusion detection system using federated machine learning. Computers & Electrical Engineering, 96, 107440.

[14] Shahbazi, Z., & Byun, Y. C. (2021). Improving transactional data system based on an edge computing–blockchain–machine learning integrated framework. Processes, 9(1), 92.

[15] Alsharnouby, M., Abdelzaher, T., et al. (2021). A blockchain-based framework for secure artwork authentication and traceability. Journal of Visual Communication and Image Representation, 70, 102986.

[16] Banerjee, S., et al. (2020). Artwork authentication using convolutional neural network with transfer learning. International Journal of Machine Learning and Cybernetics, 11, 2751–2764.

[17] Desoky, M., et al. (2021). Towards a secure and distributed artwork authentication system. IEEE Transactions on Dependable and Secure Computing. Advance online publication. doi:10.1109/TDSC.2021.3099211

[18] Padmanabhan, T. R., et al. (2021). A secure artwork authentication framework using federated learning. IEEE Transactions on Information Forensics and Security, 16, 380–391.

[19] Rokade, G., & Patil, A. B. (2020). Artwork authentication using deep learning with feature extraction. Journal of Ambient Intelligence and Humanized Computing, 11, 5119–5130.

[20] Sharma, V., et al. (2020). Artwork authentication using deep learning and random forest classifier. International Journal of Machine Learning and Cybernetics, 11, 2615–2627.

[21] Anandhavalli, M., & Thamarai Selvi, S. (2020). Artwork authentication using deep learning and image segmentation. International Journal of Advanced Intelligence Paradigms, 15, 283–299.

[22] Ahmed, S., et al. (2021). Towards a secure machine learning-based artwork classification system. Journal of Ambient Intelligence and Humanized Computing, 12, 6247–6264.

[23] Xie, S., et al. (2020). A secure and efficient blockchain-based framework for art authentication. IEEE Transactions on Industrial Informatics, 16, 1642–1651.

[24] Gallego-Madrid, J., Sanchez-Iborra, R., Ruiz, P. M., & Skarmeta, A. F. (2022). Machine learning-based zero-touch network and service management: A survey. Digital Communications and Networks, 8(2), 105-123.