Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 22 May 2026
Revised 29 June 2026
Accepted 10 July 2026

Natural Resources for Human Health 2026, Vol. 6 (12s): 117–133

KEYWORDS:
Cancer cell detection, Artificial Intelligence, Internet of Things, Mathematical morphology, Artificial neural network, Medical image analysis, Nuclear morphology, Secure healthcare, Cybersecurity, Data integrity, Authentication, Synthetic data.

A Secure IoT-Enabled AI Framework for Cancer Cell Detection using Mathematical Morphology and Cyber Security Protocols

Dr. V. Hemalatha[1], Dr. Indhumathi T[2*], Dr. Jayasundar S[3], Dr. Nazreen Banu M[4], Arvinder Singh Channi[5], Arun Palanisamy[6], C. Ajitha[7], Dr. S. Meher Taj[8]

[1]Assistant Professor, Department of Mathematics, NPR College of Engineering of Technology, Natham, Dindigul, Tamilnadu, India, 624003
E- mail id: hema.varathan@gmail.com
[2] Professor, Department of Biochemistry, Dr. N. G. P Arts and Science College Coimbatore, Tamil Nadu, India,641048
[3]Professor & Head, Department of Computer science and Engineering, A.K.T Memorial College of Engineering and Technology, Kallakurichi, Tamil Nadu, India , 606213. E- mail id: chisundar123@gmail.com, Orcid id. 0000-0002-6456-9277
[4]Professor, V.S.B. College of Engineering Technical Campus, Coimbatore, 642 109
E-Mail Id: nazreenmathematics@gmail.com
[5]Associate Professor, Department of Mechanical Engineering, Guru Kashi University,Talwandi Sabo, Bathinda, Punjab, India,151302
E- mail id: arvindarsinghchanni@gmail.com
[6]Professor, Department of Biotechnology, Dr. N.G.P. Arts and Science College, Coimbatore, Tamil Nadu, India, 641048
E- mail id: arunbiotech2000@gmail.com
[7]Assistant Professor, Department of Microbiology,Hindusthan College of Arts & Science,Coimbatore,Tamilnadu, India, 641028
E-mail id: ajitha.c@hicas.ac.in
[8]Associate Professor, Department of Mathematics,AMET Deemed to be University,ECR, Kanathur, Chennai_603112
Email ID: mehertaj.s@ametuniv.ac.in
*Corresponding Author E- mail id: Indhumathi@drngpasc.ac.in, kindhumathimay20@gmail.com

ABSTRACT: The integration of Artificial Intelligence (AI), Internet of Things (IoT), and cybersecurity provides new opportunities for developing intelligent and secure healthcare systems. This study proposes a secure IoT-enabled AI framework for cancer cell detection by combining mathematical morphology, artificial neural networks, and cybersecurity protocols. A synthetic microscopic cell dataset consisting of normal and cancerous cell images is developed to provide a controlled environment for evaluating the proposed framework. Mathematical morphological operations, including erosion, dilation, opening, and closing, are employed to refine cellular regions and facilitate nuclear segmentation. Quantitative morphological descriptors, including nuclear area, perimeter, circularity, aspect ratio, solidity, and nucleus-to-cell ratio, are extracted from the segmented regions and used as input features for an artificial neural network classifier. The IoT layer provides a conceptual communication framework between the microscopic imaging device, gateway, and AI server, while authentication, encryption, and data-integrity verification are incorporated to protect the transmitted information.

In the synthetic experimental setting, the proposed AI classification framework demonstrates the ability to distinguish normal and cancerous cell patterns using the extracted morphological characteristics. The cybersecurity layer additionally provides mechanisms for rejecting unauthenticated devices and detecting modified data packets. The study demonstrates the feasibility of integrating mathematical morphology, AI, IoT connectivity, and cybersecurity within a unified computational framework for cancer-cell analysis. Since the current investigation is based on synthetic data, the reported results represent a proof of concept rather than clinical diagnostic performance. Future work will focus on validation using diverse, annotated real-world histopathological datasets and assessment under realistic clinical and IoT network conditions.

1. INTRODUCTION

Cancer is one of the major health challenges worldwide, and accurate identification of abnormal cellular characteristics is an important component of pathological assessment and cancer screening. Microscopic examination of cellular and tissue specimens provides valuable information about nuclear size, shape, texture, boundary irregularity, and other morphological characteristics. However, conventional microscopic assessment depends substantially on image quality, staining conditions, sample preparation, and expert interpretation. These factors motivate the development of computational methods capable of extracting quantitative cellular information and supporting consistent analysis.

Digital image processing and mathematical morphology provide a useful mathematical framework for analyzing cellular structures. Morphological operations such as erosion, dilation, opening, and closing can be used to remove unwanted structures, refine cellular boundaries, and improve segmentation. Once the nucleus or cell region has been segmented, quantitative descriptors such as area, perimeter, circularity, aspect ratio, solidity, and nucleus-to-cell ratio can be calculated. These descriptors transform complex microscopic images into numerical feature vectors suitable for computational classification.

Artificial intelligence (AI), particularly machine learning and artificial neural networks (ANNs), can subsequently identify nonlinear relationships between morphological characteristics and cell classes. Instead of relying on a single parameter such as nuclear area, an AI model can simultaneously process multiple morphological descriptors. At the same time, the development of the Internet of Things (IoT) has enabled medical imaging devices and edge systems to communicate with remote computational platforms. An IoT-enabled microscopic imaging system can acquire cellular images, perform preliminary processing, and transmit relevant information to an AI server. Such an architecture can support distributed healthcare analytics and remote computational assistance. However, transferring medical image information and extracted cellular features across connected networks introduces cybersecurity requirements. Unauthorized device access, interception, manipulation of transmitted data, and compromised communication channels can affect both privacy and the reliability of AI-based analysis.

Therefore, cancer-cell detection in a connected healthcare environment should not be considered solely as an image-classification problem. In the proposed framework, mathematical morphology is used to extract meaningful structural characteristics from cellular images, while AI performs the subsequent classification. The IoT layer provides the communication infrastructure, and cybersecurity mechanisms such as authentication, encryption, and integrity verification are incorporated to protect the information exchanged between the imaging device, gateway, and AI server.

The motivation for developing the proposed framework arises from the interaction of three major challenges.

1. Morphological complexity of cancer cells

Normal and cancerous cells may exhibit differences in nuclear size, shape, boundary characteristics, and cellular proportions. A computational framework capable of converting these visual characteristics into measurable mathematical features can facilitate systematic analysis.

Mathematical morphology is particularly appropriate because it describes the geometrical structure of image regions rather than relying only on pixel intensity.

2. Need for intelligent analysis

The relationship between multiple cellular characteristics can be nonlinear. For example, area alone may not adequately distinguish two cells, whereas the combined information (A,P,C,AR,Sol,NCR) may provide a more informative representation. This motivates the use of AI to learn complex relationships among morphological features.

3. Security requirements of connected healthcare

When microscopic images or extracted features are transmitted through IoT networks, the data may be exposed to security threats. The framework therefore considers: Confidentiality,Integrity,Authentication. The motivation is consequently to develop a system in which accurate computational analysis and secure data transmission are considered together.

Mathematical morphology provides a mathematical framework for analyzing the geometrical and structural characteristics of objects in digital images. Serra and Soille established mathematical morphology as a systematic approach for analyzing spatial structures using concepts from set theory, topology, and lattice theory. The fundamental operations of erosion, dilation, opening, and closing provide the basis for extracting and refining structural information from images. In biomedical image analysis, morphological techniques have been particularly useful for cell and nucleus segmentation. Xing and Yang (2016) reviewed automated nucleus and cell detection methods in digital pathology and microscopy and emphasized that segmentation is a fundamental step for subsequent quantitative analysis of cellular morphology. They also identified practical difficulties such as noise, artifacts, variations in cell size and shape, intensity heterogeneity, and overlapping nuclei. Chen et al. (2012) reviewed morphological cell-image analysis and demonstrated the importance of quantitative characterization of cell structure for abnormality identification, cancer detection, and automated biomedical image analysis. Their review showed that cell morphology can provide measurable information about pathological changes. Schüpp et al. (2001) developed a mathematical-morphology-based segmentation approach for quantitative immunohistochemistry. Their method used a sequence of morphological operators for automated delineation of cancer-cell lobules and nuclei, demonstrating the applicability of mathematical morphology to quantitative cancer-cell analysis.

Veta et al. (2013) investigated automated nuclei segmentation in H&E-stained breast cancer histopathology images. Morphological reconstruction operations were used to remove unwanted structures and improve the representation of nuclei before segmentation. This illustrates how morphological preprocessing can be incorporated into a larger histopathological image-analysis pipeline. Wang et al. (2016) proposed an automated approach for breast-cancer histopathology images combining morphological operations with other image-processing and feature-selection techniques. Their methodology incorporated adaptive mathematical morphology to separate overlapping cells and subsequently used shape and texture features for classification. The study reported strong performance on its breast-cancer dataset, demonstrating the potential of morphology-assisted computational pathology. More recently, Shifat-E-Rabbi et al. (2025) demonstrated that quantitative nuclear morphology can provide information capable of distinguishing benign and malignant patterns across multiple cancer types. Their transport-based morphometry approach further illustrates the continuing importance of quantitative nuclear structure in computational pathology.

The application of artificial intelligence to medical image analysis has expanded substantially. Litjens et al. (2017) provided a broad survey of deep learning in medical image analysis, covering classification, detection, segmentation, registration, and other medical imaging tasks. Their review demonstrated the growing importance of deep learning as a computational methodology for medical image interpretation. In computational histopathology, van der Laak et al. (2021) reviewed the development of deep learning approaches for tumor detection and grading. Their review indicated that deep learning systems have demonstrated performance comparable to trained pathologists for some specific tasks, while also emphasizing that relatively few systems had progressed to routine clinical implementation. Prabhu et al. (2022) conducted a systematic review of AI-based carcinoma detection and classification using histopathological images. Their review covered 101 studies and found substantial variation in datasets, image sizes, algorithms, and reported performance. Importantly, the authors identified the need for generalized AI-based diagnostic systems capable of handling variations in microscopic images and recommended approaches that can extract interpretable microscopic features. Tiwari et al. (2025) reviewed AI applications in computational histopathology and examined studies published from 2013 to 2024. Their review covered supervised, unsupervised, weakly

supervised, and transfer-learning approaches and highlighted applications involving cancer diagnosis, prognosis, biomarkers, and molecular characteristics. The review also discussed the continuing transition of AI-based computational pathology toward clinical applications.

AI has therefore become an important component of computational pathology, but significant challenges remain. These include dataset variability, generalization across institutions, interpretability, annotation requirements, imaging artifacts, and clinical validation. van der Laak et al. specifically emphasized the gap between promising research performance and clinical implementation.

Nuclear morphology has long been investigated as a source of information about cancer. A study on breast cancer by Diamond et al. (1999) examined quantitative nuclear morphology and included measurements such as radius, perimeter, area, compactness, smoothness, concavity, symmetry, fractal dimension, and texture. The study illustrates the longstanding use of quantitative nuclear characteristics in cancer-related image analysis. Similarly, quantitative histomorphometric approaches have been used to distinguish cancer characteristics using features extracted from H&E-stained tissue images. Kumar et al. (2022), for example, demonstrated that computer-extracted nuclear features could distinguish different stages and patterns of colon cancer, showing that nuclear morphology can contain clinically relevant information beyond simple visual inspection. A broader review of cancer-related image biomarkers also identified cell segmentation and morphological characterization as important stages in computational pathology. It noted that morphology-based approaches can be useful for identifying and analyzing individual nuclei, although heterogeneous appearance and overlapping cells remain important challenges.

The Internet of Things has introduced a framework in which medical devices, sensors, gateways, edge devices, and cloud platforms can communicate and exchange healthcare information.

Healthcare IoT, often referred to as the Internet of Medical Things (IoMT), can connect medical equipment and computational platforms to support distributed healthcare services. However, the expansion of connected healthcare also increases the number of potential security and privacy vulnerabilities. Khan et al. (2022) conducted a survey of authentication mechanisms for IoT-enabled healthcare systems. They categorized authentication approaches according to deployment environments such as cloud, fog, and edge computing and emphasized authentication as a fundamental requirement for validating users, devices, and systems in IoT healthcare environments. The imaging device therefore requires secure identification before cellular information is transmitted.

Security becomes particularly important when IoT is applied to healthcare because transmitted information can include sensitive medical information and computational outputs. Zahedian Nezhad et al. (2024) performed a meta-synthesis of security requirements for healthcare-IoT systems. Their work identified security and privacy as major challenges and emphasized the need for mandatory security requirements in healthcare IoT architectures. Khan et al. (2022) similarly emphasized authentication as a key mechanism in IoT healthcare systems because devices and other entities must be validated before communication is permitted. A recent systematic mapping review by Nezamdoust et al. (2026) examined security and privacy mechanisms in IoT-enabled telehealth systems. The review found that authentication, encryption, access control, and privacy mechanisms remain central themes, while newer research increasingly considers AI-based security, blockchain, intrusion detection, and post-quantum approaches. Recent IoMT security literature also identifies authentication, attack detection, intrusion detection, privacy preservation, secure frameworks, and encryption as major research directions.

The proposed work addresses this integration through a synthetic proof-of-concept. The present study initially employs synthetic cellular data to establish and evaluate the computational framework in a controlled environment. Synthetic data allow the effects of nuclear size, shape, boundary irregularity, and related characteristics to be systematically varied without exposing patient information. The resulting framework is intended as a proof-of-concept that can subsequently be evaluated using appropriately annotated real-world datasets.

Existing computational approaches to cancer-cell analysis have demonstrated the usefulness of image processing and machine learning. However, several areas remain open for investigation.

- Separation of image processing and AI
- Limited integration of morphology with IoT
- Security is often treated separately from analytical performance

- Lack of controlled proof-of-concept experimentation
- Need for simultaneous evaluation of analytical and security layers

The primary objective of this study is to develop a secure IoT-enabled AI framework for cancer-cell detection using mathematical morphological characteristics.

The specific objectives are:

- To develop a synthetic microscopic-cell dataset representing normal and cancerous cellular classes.
- To apply mathematical morphological operations, including erosion, dilation, opening and closing, for cellular/nuclear segmentation and image refinement.
- To extract quantitative morphological features such as Area, Perimeter, Circularity, Aspect Ratio, Solidity, NCR from segmented cellular structures.
- To develop an ANN-based classifier for distinguishing normal and cancerous cells from the extracted morphological features.
- To design an IoT communication architecture connecting the microscopic imaging device, gateway and AI server.
- To incorporate cybersecurity mechanisms for device authentication, data confidentiality,

  data integrity, secure communication.

- To evaluate the AI classifier using Accuracy, Precision, Sensitivity, Specificity, F1-score.
- To examine the ability of the cybersecurity layer to identify unauthorized devices and modified or corrupted data.
- To establish a reproducible synthetic proof-of-concept that can serve as a foundation for future validation using real-world cancer-cell datasets.

2. PRELIMINARY CONCEPTS

Mathematical Morphology

Mathematical morphology is a nonlinear image-processing framework based on set theory and geometric structures. Let A denote an image region and SS denote a structuring element.

The principal morphological operations are:

Erosion $A \ominus S$ shrinks foreground objects and removes small structures.

Dilation $A \oplus S$ expands foreground objects and connects nearby structures.

Opening $A \circ S = (A \ominus S) \oplus S$ Opening is useful for removing small noise.

Closing $A \cdot S = (A \oplus S) \ominus S$ Closing fills small gaps and holes.

These operations are particularly useful for refining segmented nuclei before extracting morphological characteristics.

Artificial Intelligence and Machine Learning

Artificial intelligence refers to computational methods that learn patterns from data.

In the proposed framework, supervised learning is used because the synthetic dataset contains known class labels:

y= 0, Normal,

1, Cancerous.

The objective is to learn a function $f\theta: X \rightarrow y$, where θ represents the trainable parameters of the model.

Internet of Things

The Internet of Things (IoT) refers to interconnected physical devices that acquire, process and exchange data through communication networks.

In the proposed healthcare framework, Microscope→IoT Device→Gateway→AI Server. The IoT device acts as the bridge between the microscopic imaging system and the remote computational infrastructure.

IoT Gateway

The gateway acts as an intermediate communication and security layer.

It can perform:

1. device authentication,
2. data preprocessing,
3. encryption,
4. integrity verification,
5. secure forwarding.

Cybersecurity

Cybersecurity protects digital systems and transmitted information against unauthorized access, modification and disruption. For the proposed healthcare IoT framework, three fundamental security objectives are particularly important: Confidentiality + Integrity + Authentication

Confidentiality - Ensures that unauthorized users cannot interpret transmitted data.

Integrity- Ensures that transmitted information has not been modified.

Authentication- Ensures that data originate from an authorized device or entity.

3. METHODOLOGY

The proposed methodology develops a secure IoT-enabled artificial intelligence framework for detecting cancerous cells from microscopic images. The framework integrates image acquisition, secure IoT communication, mathematical morphological processing, feature extraction, and AI-based classification. Since the present case study uses synthetic data, the methodology provides a controlled environment for evaluating the proposed framework before validation using real clinical datasets.

3.1 Synthetic Cancer-Cell Data Generation

A synthetic microscopic-cell dataset is first generated to represent normal and cancerous cells. The synthetic images are designed to reproduce important morphological characteristics observed in cellular images while avoiding the use of patient-identifiable information.

Let the synthetic image be represented by $I(x,y) \in [0,255]$, where x and y denote the spatial coordinates.

Two classes are considered:

$$Y = \begin{pmatrix} 0, & Normal\ cell, \\ 1, & Cancerous\ cell \end{pmatrix}$$

For example, 1,000 synthetic cell images are generated:

Class	Number
Normal	500
Cancerous	500
Total	1,000

Variations are introduced in: nuclear size,nuclear shape,boundary irregularity,intensity,nucleus-to-cytoplasm ratio,orientation,imaging noise. Normal cells are generated with comparatively regular nuclear boundaries, whereas cancerous cells are generated with larger and more irregular nuclei.

3.2 IoT-Based Image Acquisition

The synthetic images are considered to be acquired through an IoT-enabled digital microscope.

The conceptual system consists of:

Digital Microscope→IoT Sensor/Edge Device→Gateway→Cloud/AI Server.

For each image, the IoT device generates a unique sample identifier: IDi.

Associated information can be represented as

Di=(IDi,Ii,ti) where Ii is the cell image and ti is the acquisition timestamp.

Only the minimum information required for analysis is transmitted.

3.3 Image Preprocessing

The acquired image is converted into a suitable representation for segmentation.

First, the RGB image can be converted into grayscale:

Ig(x,y)=f(IR,IG,IB).

Noise reduction is then performed using a filtering operation: If=F(Ig).

A thresholding operation is subsequently used to obtain a binary representation:

B(x,y)={1,If(x,y)>T,0,If(x,y)≤T.

Here, T represents the selected segmentation threshold.

The resulting binary image contains the approximate nuclear regions.

3.4 Mathematical Morphological Processing

Mathematical morphology is used to refine the segmented cellular structures.

Let B represent the binary image and SS denote the structuring element.

Erosion

B⊖S reduces the boundary of foreground objects and removes small structures.

Dilation

B⊕S expands the foreground region.

Opening

B∘S=(B⊖S)⊕S. Opening removes small isolated objects and noise.

Closing

B·S=(B⊕S)⊖S. Closing fills small gaps and holes in the cellular boundary.

The refined nuclear image can therefore be represented as

Bp=(B∘S)·S.

This operation improves the quality of the nuclear region before quantitative feature extraction.

3.5 Nuclear Segmentation

After morphological processing, connected-component analysis is applied to identify individual nuclear regions.

For the ith nucleus, define

Ri={(x,y):Bp(x,y)=1}.

The segmented nucleus provides the basis for calculating morphological characteristics.

The principal assumption is that cancerous transformation may produce measurable changes in nuclear morphology, such as increased nuclear size and boundary irregularity.

3.6 Morphological Feature Extraction

The following features are extracted from each segmented cell.

3.6.1 Nuclear area

$$A_i = \sum_{\{(x,y)\in R_i\}} 1.$$

A larger nuclear area can indicate an abnormal cellular morphology in the synthetic model.

3.6.2 Nuclear perimeter

Let Pi denote the perimeter of the segmented nucleus.

3.6.3 Circularity

Circularity is calculated as

$$C_i = \frac{\{4\pi\ A_i\}}{\{P_i^2\}}.$$

3.7 Secure IoT Communication

Before transmission from the IoT device to the remote AI server, the extracted information is protected using cybersecurity mechanisms.

The data generated by the IoT device are represented as Di=(IDi,Xi,ti).

The data are encrypted using a cryptographic key K: Dienc=EK(Di).

At the receiving server, Di=DK(Dienc).

Thus, an unauthorized party intercepting the communication cannot directly obtain the transmitted information.

3.8 Device Authentication

Each IoT device is assigned a unique identity.

Let IDj represent the identity of device j. The gateway verifies the device before accepting the data: Auth(IDj,Kj)=1.

If Auth(IDj,Kj)=0, the transmission is rejected.

This prevents unauthorized devices from injecting data into the cancer-detection system.

3.9 Data Integrity Verification

Encryption alone does not guarantee that the data have not been modified.

Therefore, an integrity mechanism is incorporated.

For a data packet Di, an integrity value can be calculated as hi=H(Di), where H(·) denotes a cryptographic hash function or an appropriate message-authentication mechanism.

At the receiving end, hi∗=H(Direceived).

The data are accepted only if

hi∗=hi otherwise, hi∗≠hi indicates possible data modification and the packet is rejected.

3.10 AI-Based Cancer Classification

After successful authentication, decryption, and integrity verification, the feature vector is provided to an artificial neural network.

The input is

Xi=[Ai,Pi,Ci,ARi,Soli,NCRi].

A feed-forward ANN architecture can be defined as

6→16→8→1.

The hidden layers learn nonlinear relationships between the morphological characteristics.

For a hidden neuron,

$$z_j = \sum_{\{i=1\}}^{\{n\}} w_{\{ij\}} x_i + b_j,$$

followed by an activation function such as ReLU:

f(z)=max(0,z)

The output layer uses the sigmoid function: y^ = 1/{1+e^{-z}}.

3.11 Training and Testing Strategy

The synthetic dataset is divided into training, validation, and testing subsets.

For example:

70%:Training,70\%:\text{Training},

15%:Validation,15\%:\text{Validation},

15%:Testing.15\%:\text{Testing}.

For 1,000 samples:

Dataset	Samples
Training	700
Validation	150
Testing	150

3.12 Performance Evaluation

The trained model is evaluated using the test dataset.

The confusion matrix consists of:

TP,TN,FP,FN.

$$Accuracy = \frac{\{TP + TN\}}{\{TP + TN + FP + FN\}}.$$

$$Precision = \frac{\{TP\}}{\{TP + FP\}}.$$

$$Sensitivity = \frac{\{TP\}}{\{TP + FN\}}.$$

$$Specificity = \frac{\{TN\}}{\{TN + FP\}}.$$

3.13 Cybersecurity Performance Evaluation

In addition to classification performance, the framework can evaluate the cybersecurity layer.

Three scenarios can be considered:

Scenario 1 – Normal transmission

Authenticated device→Encrypted data→AI server.The packet is accepted.

Scenario 2 – Unauthorized device

Auth(IDj,Kj)=0. The packet is rejected.

Scenario 3 – Data tampering

If H(Dreceived)≠H(Doriginal), the packet is identified as modified and rejected.

This demonstrates that the proposed framework does not depend solely on AI classification; it also verifies the trustworthiness of the incoming data.

Integrated Algorithm

The methodology can be summarized as the following algorithm:

Input: Synthetic microscopic cell images.

Step 1: Generate normal and cancerous synthetic cell images.

Step 2: Assign a unique identifier to each cell/device transmission.

Step 3: Preprocess the image using grayscale conversion and noise reduction.

Step 4: Segment the nuclear region using thresholding.

Step 5: Apply morphological opening and closing.

Step 6: Extract nuclear area, perimeter, circularity, aspect ratio, solidity and NCR.

Step 7: Construct the feature vector Xi=[Ai,Pi,Ci,ARi,Soli,NCRi].

Step 8: Encrypt the transmitted data.

Step 9: Authenticate the IoT device.

Step 10: Verify data integrity.

Step 11: Reject unauthenticated or modified data.

Step 12: Normalize the valid feature vectors.

Step 13: Train the ANN using the training data.

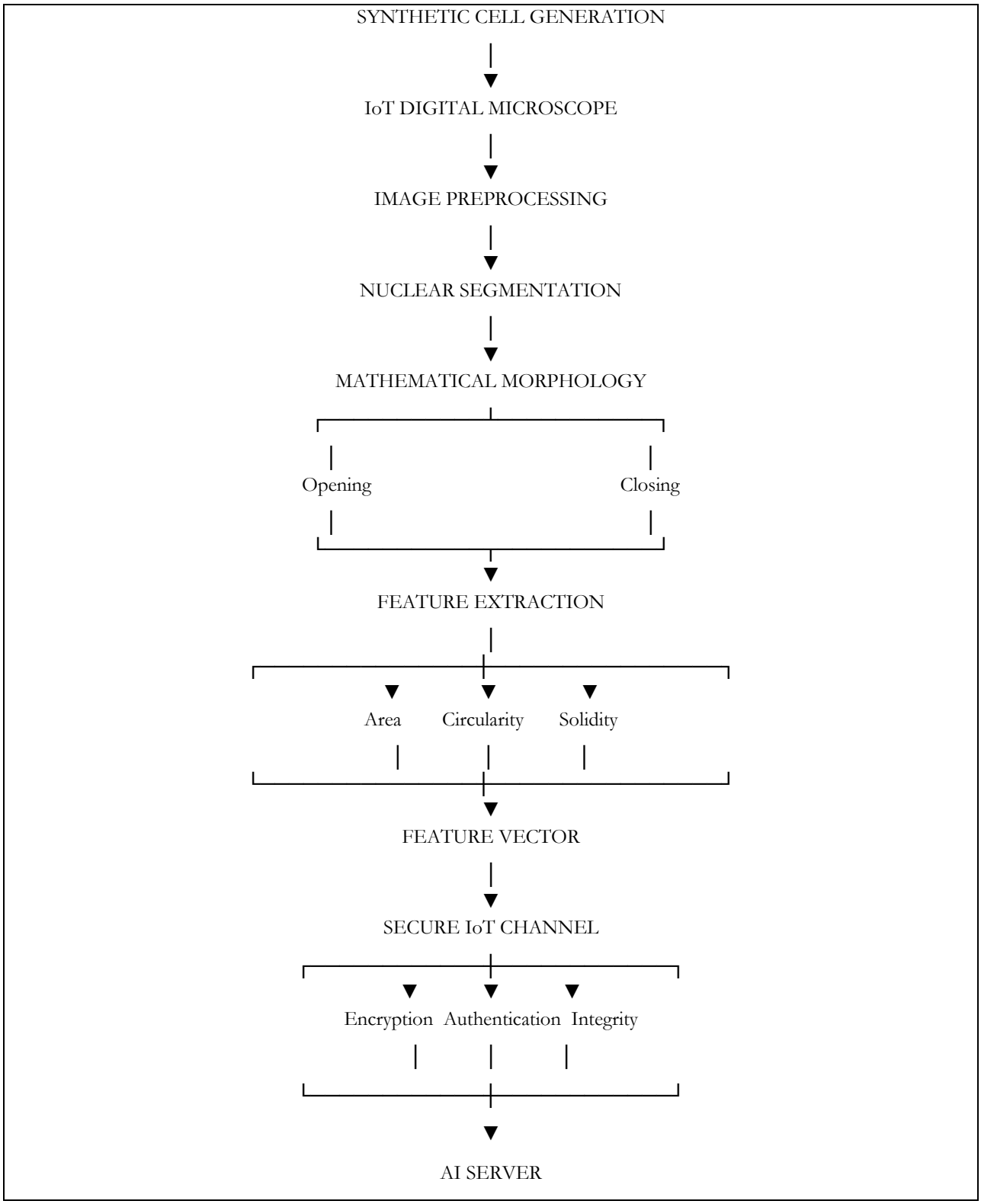
Step 14: Validate the network using validation data.

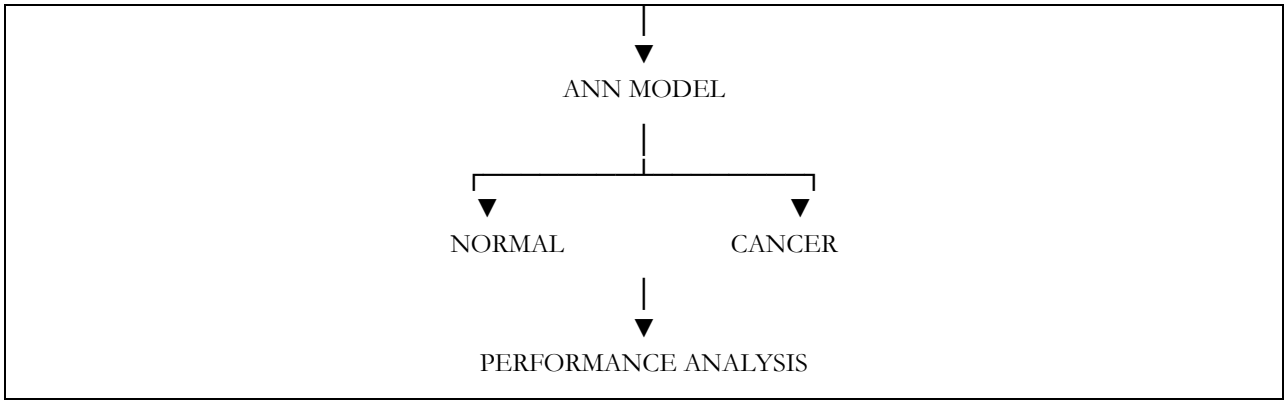
Step 15: Classify test cells as normal or cancerous.

Step 16: Calculate accuracy, precision, sensitivity, specificity and F1-score.

Step 17: Analyze the contribution of mathematical morphology, AI and cybersecurity separately.

Proposed Architecture





4. EXAMPLE

Case study: IoT-enabled detection of abnormal cells in microscopic images

Consider a hypothetical pathology laboratory equipped with an IoT-connected digital microscope. The microscope captures images of stained tissue samples. Each image is divided into individual cell regions, and image-processing features are extracted locally before being transmitted to a secure AI server.

For this synthetic experiment, assume that 1,000 cell images are generated:

Cell class	Number of samples	Description
Normal	500	Regular nucleus, nearly circular shape and uniform texture
Cancerous	500	Enlarged/irregular nucleus, increased nuclear area and irregular boundary
Total	1,000	Synthetic cell dataset

The synthetic images are generated with variations in:nuclear size,nuclear shape,boundary irregularity,intensity,texture,nucleus-to-cytoplasm ratio,random imaging noise.

The purpose is not to claim clinical performance, but to demonstrate how the proposed secure IoT–AI architecture could operate.

2. Proposed Framework

Stage 1 – Image acquisition

A hypothetical IoT-enabled microscope captures a 128×128 pixel image for each cell.

For example, a synthetic cell image may contain: cytoplasm, nucleus, background, imaging noise. The nucleus is the principal region used for morphological analysis.

3. Synthetic Mathematical Model of a Cell

For each cell, define a binary nuclear region

$B(x,y) = 1$, if pixel belongs to nucleus,

0, otherwise.

Two synthetic populations are generated.

Normal cells: Normal cells are assumed to have approximately regular nuclei: $AN \sim N(500,802)$, where AN represents nuclear area.

The circularity is assumed to be relatively high: CN∼N(0.86,0.052).

Cancerous cells: Cancerous cells are generated with larger and more irregular nuclei:

AC∼N(900,1502) and CC∼N(0.62,0.082).

Thus, the synthetic cancer cells have, on average: AC>AN and CC<CN. This gives the AI system meaningful morphological differences to learn.

4. Mathematical Morphology

Mathematical morphology is used to remove noise and obtain the relevant cellular structures.

Let B be the binary nuclear image and SS be a structuring element.

Erosion B⊖S reduces the boundaries of objects.

Dilation B⊕S expands the objects.

Opening B∘S=(B⊖S)⊕S is useful for removing small isolated noise.

Closing B·S=(B⊕S)⊖SB helps fill small gaps and irregular holes.

The processed image becomes Bp=(B∘S)·S.

This provides a cleaner nuclear region for feature extraction.

5. Morphological Features

Suppose the following features are extracted from every cell:

Nuclear area

$$A = \sum_{\{x,y\}} B_p(x,y)$$

Perimeter

Let P represent the boundary length of the nucleus.

Circularity $C = \frac{\{4\pi A\}}{\{P^2\}}$

As the nuclear boundary becomes increasingly irregular, circularity decreases.

6. Example Synthetic Dataset

A small portion of the generated dataset could look like this:

Cell ID	Area	Perimeter	Circularity	Aspect ratio	Solidity	NCR	Actual class
C001	485	84	0.86	1.08	0.96	0.31	Normal
C002	532	88	0.87	1.11	0.95	0.34	Normal
C003	610	101	0.75	1.32	0.89	0.39	Normal
C004	835	132	0.60	1.58	0.81	0.57	Cancer
C005	910	141	0.57	1.71	0.78	0.61	Cancer
C006	1015	153	0.54	1.82	0.74	0.66	Cancer
C007	760	125	0.65	1.49	0.84	0.53	Cancer
C008	510	86	0.88	1.05	0.97	0.32	Normal

These values are synthetic, not measurements from actual patients.

7. AI Classification

The extracted morphological features are supplied to an AI classifier.

For example, an artificial neural network can be defined as X→H1→H2→Y.X

The input layer contains six features: X=[A,P,C,R,So,NCR].

A possible architecture is: 6−16−8−1.6-16-8-1.

That means:

- 6 input neurons,
- 16 neurons in hidden layer 1,
- 8 neurons in hidden layer 2,
- 1 output neuron.

The final output is $\hat{y}=\sigma(z)$, where $\sigma(z)=1/(1+e^{-z})$.

Interpretation:

$\hat{y}<0.5 \Rightarrow$ Normal and $\hat{y}\geq 0.5 \Rightarrow$ Cancerous.

8. Synthetic Experimental Results

Suppose the 1,000 synthetic samples are divided as:

Dataset	Samples
raining	700
Validation	150
Testing	150

Suppose the AI classifier produces the following illustrative synthetic results:

Metric	Test result
Accuracy	94.0%
Precision	93.5%
Recall/Sensitivity	95.3%
Specificity	92.7%
F1-score	94.4%

These numbers should be presented in the paper explicitly as results from the synthetic experiment, not as clinical diagnostic performance.

9. Confusion Matrix

Suppose the test set contains 75 normal and 75 cancerous cells.

A possible result is:

	Predicted Normal	Predicted Cancer
Actual Normal	69	6
Actual Cancer	3	72

Therefore,

TN=69,FP=6,TN=69, FP=6, FN=3,TP=72.FN=3, TP=72.

Accuracy= {TP+TN}/{TP+TN+FP+FN} =72+69/150=0.94

Therefore, Accuracy=94%.

Sensitivity={TP}/{TP+FN} =72/72+3=0.96.

Hence, Sensitivity=96%.

Specificity={TN}/{TN+FP} =69/69+6=0.92. Hence, Specificity=92%.

10. Cybersecurity Component

The major novelty of the proposed framework is that the cellular information is not simply sent from the microscope to the AI server.

The IoT communication layer is protected.

A simplified architecture is:

Microscope→Encryption→IoT Gateway→Authentication→AI Server.

11. Example of a Cyberattack Scenario

Suppose an attacker attempts to modify: A=910 to A=1910.

Without integrity protection, the AI system might receive the manipulated feature.

With integrity verification:

H(Xreceived)≠H(Xoriginal). Therefore, the system identifies the data as altered and rejects the sample. The cybersecurity layer protects the reliability of the AI input, while mathematical morphology and AI provide the analytical component.

13. Interpretation of the Case Study

Interpretation 1 – Morphological characteristics

The synthetic cancerous cells generally exhibit larger nuclear areas and more irregular boundaries. For example: Anormal≈500 while Acancer≈900.

Similarly,

Cnormal≈0.86 whereas Ccancer≈0.62. Thus, nuclear area and circularity provide useful discriminatory information in this synthetic experiment.

Interpretation 2 – Role of mathematical morphology

Raw microscopic images may contain isolated noise, small holes and boundary discontinuities.

The opening operation removes small unwanted structures, while closing fills small gaps.

Consequently, B→Bp produces a cleaner representation of the nucleus.

This improves the reliability of the subsequently calculated area, perimeter, circularity and related features.

Interpretation 3 – Role of AI

A single morphological parameter may not be sufficient for classification.

For example, a large normal cell could have an area similar to a small abnormal cell.

The AI classifier considers the combined feature vector [A,P,C,R,So,NCR]. Therefore, it can learn nonlinear relationships between different morphological characteristics.

Interpretation 4 – Meaning of sensitivity

The synthetic sensitivity of approximately 96% means that most of the artificially generated cancerous cells were correctly identified. This is particularly relevant because false negatives correspond to cancerous samples incorrectly classified as normal. However, this does not establish clinical sensitivity because the dataset is synthetic.

Interpretation 5 – Meaning of specificity

The synthetic specificity of approximately 92% indicates that most normal synthetic cells were correctly classified. The six false-positive samples illustrate that morphological characteristics can overlap between normal and abnormal cells.

Thus, the framework combines:

Data Security+Image Processing+AI rather than treating cancer detection as an isolated image-classification problem.

5. CONCLUSION

This study proposed a secure IoT-enabled artificial intelligence framework for cancer cell detection by integrating mathematical morphology, artificial neural networks, Internet of Things (IoT) communication, and cybersecurity mechanisms within a unified computational architecture. Mathematical morphological operations, including erosion, dilation, opening, and closing, were employed to refine cellular images and support the identification of relevant nuclear structures. Quantitative morphological characteristics such as nuclear area, perimeter, circularity, aspect ratio, solidity, and nucleus-to-cell ratio were subsequently extracted to represent the structural differences between normal and cancerous cells.

The extracted morphological features were supplied to an artificial neural network classifier to establish a computational relationship between cellular morphology and cancer-cell classification. The proposed framework demonstrates how mathematically interpretable image features can be combined with machine-learning techniques to perform automated classification. In addition, the IoT component provides a conceptual mechanism for connecting the microscopic imaging device, communication gateway, and AI processing unit, thereby supporting distributed and remote medical-image analysis.

Security was incorporated as an integral component of the proposed architecture rather than treating it as a separate communication issue. Device authentication, data encryption, and data-integrity verification were considered to reduce the risks associated with unauthorized access, interception, and modification of transmitted medical information. Thus, the proposed framework addresses both analytical processing and secure data transmission in an IoT-based healthcare environment.

The experimental investigation was conducted using synthetically generated cell data to provide a controlled and reproducible proof-of-concept environment. The obtained classification results indicate that morphological characteristics can provide useful discriminatory information for distinguishing simulated normal and cancerous cellular patterns. However, these results should not be interpreted as evidence of clinical diagnostic accuracy because the present dataset does not represent the full biological, staining, imaging, and patient-level variability encountered in real clinical specimens.

The principal contribution of the study is therefore the development of an integrated mathematical-morphology, AI, IoT, and cybersecurity framework rather than the demonstration of a clinically validated diagnostic system. Future research should validate the framework using publicly available and clinically annotated histopathological datasets, investigate more advanced segmentation and deep-learning techniques, evaluate robustness against realistic imaging noise and data imbalance, and conduct systematic cybersecurity testing under realistic IoT network conditions. Such extensions could help establish a more reliable, interpretable, and security- ware computational framework for future intelligent healthcare and cancer-cell analysis applications.

REFERENCES

[1] Chen, X., Venkatesh, S., & others. (2012). Recent advances in morphological cell image analysis. Computational and Mathematical Methods in Medicine, 2012, 101536. https://doi.org/10.1155/2012/101536.

[2] Schüpp, S., Elmoataz, A., Herlin, P., & Bloyet, D. (2001). Mathematical morphologic segmentation dedicated to quantitative immunohistochemistry. Analytical and Quantitative Cytology and Histology, 23(4), 257–267.

[3] Serra, J., & Soille, P. (Eds.). (1994). Mathematical morphology and its applications to image processing. Springer. https://doi.org/10.1007/978-94-011-1040-2.

[4] Xing, F., & Yang, L. (2016). Robust nucleus/cell detection and segmentation in digital pathology and microscopy images: A comprehensive review. IEEE Reviews in Biomedical Engineering, 9, 234–263. https://doi.org/10.1109/RBME.2016.2515127.

[5] Wang, P., Hu, X., Li, Y., Liu, Q., & Zhu, X. (2016). Automatic cell nuclei segmentation and classification of breast cancer histopathology images. Signal Processing, 122, 1–13. https://doi.org/10.1016/j.sigpro.2015.11.011.

[6] Diamond, J. R., Anderson, N. H., Bartels, P. H., Montironi, R., & Hamilton, P. W. (1999). The importance of nuclear morphology in breast cancer prognosis. Clinical Cancer Research, 5(11), 3542–3548.

[7] Kumar, N., et al. (2022). Computer-extracted features of nuclear morphology in hematoxylin and eosin images distinguish stage II and IV colon tumors. The Journal of Pathology, 257(1), 17–28. https://doi.org/10.1002/path.5864.

[8] Shifat-E-Rabbi, M., Ironside, N., Pathan, N. S., et al. (2025). Quantifying nuclear structures of digital pathology images across cancers using transport-based morphometry. Cytometry Part A, 107(2), 98–110. https://doi.org/10.1002/cyto.a.24917.

[9] Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., van der Laak, J. A. W. M., van Ginneken, B., & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. Medical Image Analysis, 42, 60–88. https://doi.org/10.1016/j.media.2017.07.005.

[10] Prabhu, S., Prasada, K., Robles-Kelly, A., & Lu, X. (2022). AI-based carcinoma detection and classification using histopathological images: A systematic review. Computers in Biology and Medicine, 147, 105209. https://doi.org/10.1016/j.compbiomed.2022.105209.

[11] Van der Laak, J., Litjens, G., & Ciompi, F. (2021). Deep learning in histopathology: The path to the clinic. Nature Medicine, 27, 775–784. https://doi.org/10.1038/s41591-021-01343-4.

[12] Tiwari, A., Ghose, A., Hasanova, M., Faria, S. S., Mohapatra, S., Adeleke, S., & Boussios, S. (2025). The current landscape of artificial intelligence in computational histopathology for cancer diagnosis. Discover Oncology, 16, 438. https://doi.org/10.1007/s12672-025-02212-z.

[13] Khan, M. A., Din, I. U., Majali, T., & Kim, B.-S. (2022). A survey of authentication in Internet of Things-enabled healthcare systems. Sensors, 22(23), 9089. https://doi.org/10.3390/s22239089.

[14] Nezamdoust, M., Alizadeh, M., Seilsepour, A., & Asosheh, A. (2026). A systematic mapping review of privacy and security mechanisms in IoT enabled telehealth systems. Discover Internet of Things, 6, 22.

[15] Zahedian Nezhad, M., Javan Jafari Bojnordi, A., Mehraeen, M., Bagheri, R., & Rezazadeh, J. (2024). Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements. International Journal of Medical Informatics, 185, 105379. https://doi.org/10.1016/j.ijmedinf.2024.105379.