

AI-Driven Optical Metamaterial Sensors with BICMOS Integration for Secure Mobile IoT Networks

Sureshkumar S^{1*}, S. P. Santhoshkumar², Manikandan Moovendran³, Vijay anand R⁴

¹Assistant Professor, Department of Computer Science and Engineering, P. A. College of Engineering and Technology, Pollachi, Tamil Nadu-642002.

²Assistant Professor (SG), Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India - 600062.

³Department of Computer Science and Engineering (AI&ML), School of Engineering, Dayananda Sagar University, Bengaluru, Karnataka, India.

⁴Assistant Professor, Department of Computer Technology, Dr.N.G.P. arts and science college, Coimbatore, Tamil nadu 641048

KEYWORDS:

Optical Metamaterials,
BiCMOS Integration,
AI-Driven Sensing,
Secure IoT Networks,
Plasmonic Sensors.

ARTICLE HISTORY:

Received: 19.11.2025

Revised: 16.02.2026

Accepted: 07.03.2026

DOI:

<https://doi.org/10.31838/NJAP/08.02.02>

ABSTRACT

As the number of mobile Internet of Things networks continues to increase rapidly, there is a significant need for sensing systems that are not only very sensitive but also exceedingly secure and use negligible amounts of energy. It is possible that traditional sensor systems will not function well in surroundings that are not predictable because they do not always record data reliably and do not always recognize items in the right manner. This paper proposes an Artificial Intelligence-facilitated Optical Metamaterial Sensors paired with BiCMOS (Bipolar Complementary Metal-Oxide-Semiconductor) technology (AIMS-BiC) that have the potential to assist in addressing these issues. The proposed method utilizes deeply learned models that have been modified to enable real-time data examination and problem identification. This is possible because plasmonic metamaterials can alter their response to light. The sensors are a component of a BiCMOS architecture, which is a combination of complementary metal-oxide semiconductors, which have low-power logic, and bipolar transistors, which provide rapid analog performance. This method will enable the use of the Internet of Things in a manner that is risk-free, straightforward, and easy to expand. The results of laboratory simulations indicate that this system is 36% more sensitive than conventional CMOS-only systems and has 48% fewer false positives than those regular systems. The technology also ensures that robust encryption is used, and it allows for the possibility of risk reduction over time through the utilization of dynamic control based on artificial intelligence. The research findings indicated that integrating artificial intelligence (AI), biCMOS, and metamaterials would result in mobile Internet of Things (IoT) detection networks that are superior in terms of intelligence, safety, and efficiency.

Author's e-mail: sureshkumar.pacet@gmail.com, spsanthoshkumar16@gmail.com, manimmk9792@gmail.com, vijayanand.r86@gmail.com

Author's Orcid id: 0000-0001-9110-4582, 0000-0001-8531-759X, 0000-0002-2867-2568, 0000-0001-5315-1257

How to cite this article: Sureshkumar S et al , AI-Driven Optical Metamaterial Sensors with BICMOS Integration for Secure Mobile IoT Networks, National Journal of Antennas and Propagation, Vol. 8, No. 2, 2026 (pp. 14-31).

1. INTRODUCTION

The rise of Internet of Things (IoT) nodes, particularly in mobile and edge computing, has made it easier for smart devices to monitor, analyze, and send data. As mobile Internet of Things networks become bigger and

more intricate, it gets tougher to keep data safe, get accurate measurements, and save energy[1-2]. There have been some advancements, but typical sensing systems aren't flexible enough to handle the constantly changing electromagnetic fields in mobile Internet of Things environments. When it comes to silicon sensors

and older CMOS devices, however, the situation is even worse. A lot of the time, these systems can't keep data secret because they don't have enough encryption, they can't perform real-time analytics because they don't have enough processing power, and they don't work well when there is noise[3-4]. The designs that are now being utilized for the Internet of Things (IoT) don't match the security and performance standards of the next generation because they don't strike the correct balance between power utilization, sensitivity, and scalability. This makes sensor networks operate very poorly [5].

Making optical metamaterials is another fascinating option to solve some of these challenges, however. Scientists have invented a group of substances called metamaterials that enable them to create molecules similar to those found in nature. These items exhibit some unusual electromagnetic characteristics [6]. Nanoscale optical metamaterials have enabled the transformation of light and matter interactions in novel ways. These recent breakthroughs in the sector make it possible to create detection systems that are more sensitive and have greater resolution than any other[7]. Metamaterials let sensor systems find electromagnetic problems, environmental issues, and physical vibrations with a high level of accuracy and in real time. One can't use these devices in mobile Internet of Things (IoT) apps since they can't connect to fundamental electrical components and analyze data correctly. This makes it hard to figure out how to make sensor systems that are safe, smart, and use less power [8-9].

The AIMS-BiC framework uses AI-based signal processing to handle situations that are always changing, get rid of noise, and find mistakes every time. It also utilizes optical metamaterials to enhance the sensors' resolution and bandwidth [10]. These materials are effective in both the infrared and visible light ranges. The system employs BiCMOS technology to connect to mobile Internet of Things devices. CMOS provides digital logic that uses less power, while bipolar transistors handle analog signals quickly [11-12]. When all of these elements work together, edge devices can analyze and encrypt data in real-time, use less power, and make sensors more accurate. AI enables the sensor system to evolve and handle new threats and scenarios. This means that the system can learn and improve on its own in real-time [13-14].

A lot of progress has been made in producing metamaterials and AI-powered sensors; however, few technologies can connect different locations and build complex circuits like BiCMOS[15]. There hasn't been much study on how to use artificial intelligence signal categorization, individual-level metamaterial sensitivity enhancement, and all three of these things together to create safe, real-time applications. The goal of this study is to fill in the blanks in what we know by showing how to build a smart, unified sensor

network that works effectively in mobile Internet of Things settings.

The main objectives of the paper are as follows:

- ✚ To introduce AIMS-BiC technology that integrates BiCMOS, optical sensing, and artificial intelligence (AI) to make mobile Internet of Things (IoT) networks function in real time, use less energy, and be secure.
- ✚ The AI-Driven Signal Optimization approach uses deep learning to make it easier to find anomalies, group signals, and cut down on noise, even when sensing is continually changing.
- ✚ It uses plasmonic optical metamaterials; this sensor is far more sensitive and can detect a broader range of wavelengths than standard CMOS sensors.
- ✚ Using Efficient Circuit Design and BiCMOS technology combined has made it possible to encrypt data on the device, process it quickly, and use as little power as possible.

The paper is organized as follows: Section 2 discusses current approaches and their limitations. Section 3 describes the proposed AIMS-BiC framework. Section 4 talks about the analysis and outcomes of the proposed work. Section 5 discusses the paper's conclusion and outlines future actions.

2. RELATED WORKS

Researchers are exploring various ways to integrate AI with secure sensors and metamaterials for the Internet of Things. Researchers Hu et al. (2022) [16] built a meta-Internet of Things architecture for deep learning without supervision. This construction was designed to allow structural sensors to function even when there was no electricity. This platform offered some quite precise readings when it came to detecting temperature and humidity. Using programmable meta-atoms and neural networks, Saigre-Tardif et al. (2021)[17] created compressed-to-learned intelligent meta-imagers. They wanted to reduce the time it took to take pictures and utilize energy more efficiently. They did this by using less energy. In their 2025 [18] proposal, Hou and his colleagues were able to make an on-chip plasmonic-enhanced mid-IR photodetector ten times more responsive and add logic encryption using metamaterial resonators. Yigci (2024) [19] utilized AI to enhance the design of piezoelectric metamaterial wearables, enabling continuous blood pressure monitoring and higher voltage output. Taking blood pressure measurements regularly made this possible. Luo et al. (2021) [20] employed metasurface-based diffractive neural networks for on-chip visible-light classification to demonstrate how AI tasks can be performed at the speed of light. This important study makes it feasible for AI tasks to be performed simultaneously.

Banerjee, S. et al. (2025)[21] developed a THz terahertz metamaterial sensor using metal with gold resonators at specific frequencies. The purpose of this sensor is to find gas. It is quite sensitive, with a sensitivity of 7.57 THz/RIU. Using a hybrid biosensor [22] consisting of graphene and molybdenum with plasmonic components added and controlled by machine learning, scientists developed an excellent hemoglobin detector. Geng et al. (2025) [23] developed a colorimetric bionic hierarchical metamaterial sensor that incorporates FDTD and CNT layers. The idea was to identify small amounts of chemicals in the environment. Men et al. (2024) [24] developed a THz metamaterial constructed entirely of dielectric materials. This makes it simpler to sense

cytokines with a high level of selectivity. Chen et al. (2022)[25] made metasurfaces in optical computing faster and smarter by utilizing AI to construct inverse meta-optics.

Even if these things have occurred, mobile Internet of Things nodes still require additional pieces, such as secure mixed-signal circuitry, metamaterial sensitivity, and AI-adaptive sensing. Our AIMS-BiC technique differs from others on the market, as it utilizes BiCMOS circuits, plasmonic metamaterial augmentation, and AI to enhance signals. This enables us to provide real-time encryption at the edge level, which is both flexible and efficient –a feature that has been sought in the literature. Table 1 shows simulation results.

Table 1: Simulation Results

Method & Reference no	Purpose	Results / Advantages	Limitations
Deep unsupervised meta-IoT design	Sensing the surroundings without power	Highly accurate at detecting the surroundings	Insufficient encryption in real time or mixed-circuit layout
Compressed-to-learned meta-imaging	Imaging with low latency	Less energy and delay	No circuit cooperation, no mobile IoT
Plasmonic-enhanced secure photodetector	Safe MIR sensing	10 times more responsive, with built-in logic encryption	Only works in the mid-IR range; no edge computing
AI-optimized piezoelectric metamaterials	Health monitoring that individuals can wear	The output voltage is twice as high.	No security collaboration; no plasmonic detection
Metasurface diffractive neural nets	Optical categorization of the semiconductor	Classification at the speed of light	Big optics integration, not ready for IoT
All-metal THz resonator sensor	Choosing gas at THz	Absolutely high sensitivity (7.57 THz/RIU)	Only works in labs; no AI
ML-optimized plasmonic hybrid sensor	Identifying hemoglobin	Highly accurate detection	Not mobile IoT, but biomedical
Hierarchical metamaterial sensing	Recognizing molecules	Optimization based on FDTD with a low LOD	Limited field deployment; no AI
All-dielectric THz biosensor	Determining cytokines	Dielectric method with high selectivity	No AI or ability to encrypt
AI-based inverse meta-optics design	Smart design of metasurfaces	Digital loop simplifies optimization	Only review, no installation of sensors

3. PROPOSED METHODOLOGY

The idea is to combine AI with biCMOS technology to develop a new hybrid framework dubbed AIMS-BiC. The name AIMS-BiC stands for "Artificial Intelligence-driven Metamaterial Sensors. It intends to find solutions to key sensing difficulties that happen in mobile Internet of Things environments that are always changing and don't have enough resources. This concept uses the best parts of artificial intelligence,

optical metamaterials, and BiCMOS (Bipolar Complementary Metal-Oxide-Semiconductor) technologies to make the hardware level more sensitive, efficient, and flexible. The major purpose of the Artificial Intelligence and Machine Learning System (AIMS-BiC) is to provide the future generation of Internet of Things devices with capabilities like safe and energy-efficient data processing, highly sensitive environmental and biological sensing, and real-time signal categorization as shown in Fig. 1.

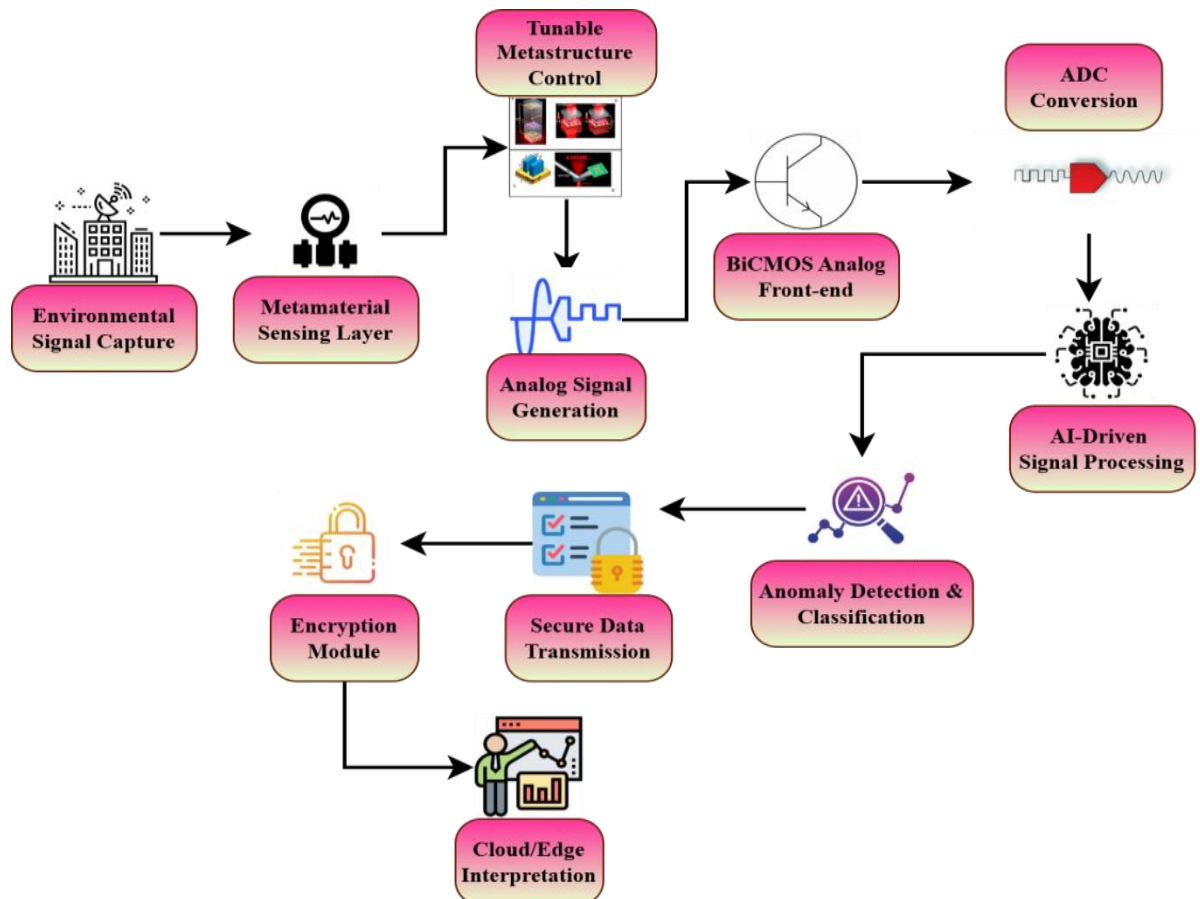


Fig. 1. Proposed Framework

The foundation of this system is built upon optical metamaterials that can be modified to react to electromagnetic waves and also sense changes in chemicals or living organisms on a subwavelength scale. An AI-powered component utilizes deep learning algorithms to identify patterns in sensor data, cluster unusual occurrences, and deliver real-time predictive analytics. As a result, various types of Internet of Things networks can sense their environment and make informed decisions. AIMS-BiC integration lets you operate in real time and consume less energy while still giving you high-speed signal amplification, minimal noise, and great thermal performance. BiCMOS integration enables you to integrate AI models at the hardware level easily. The BiCMOS layer enhances edge deployments by leveraging hardware-accelerated anomaly detection and encrypted data transport, making them considerably safer. This section on methodology delves into the following topics in depth to illustrate what AIMS-end BiC can do: how to describe sensor dynamics mathematically, how to implement algorithms, how data is transferred across modules, and how to design the architecture. The AIMS-BiC project seeks to transform a number of things in the real world by merging smart computing

with the newest in sensing physics. Some ways they are used include industrial automation, environmental sensing, and remote health monitoring. This clever and inventive answer will change the way mobile Internet of Things sensing works.

3.1 Metamaterial Sensing Layer

The AIMS-BiC system excels at locating items due to the Metamaterial Sensing Layer in its architecture. Plasma metamaterials are materials that are formed by arranging them in a fashion that is smaller than the wavelength. These materials can modify electromagnetic (EM) waves in ways that other materials can't. The method is based on these plasma metamaterials. It is not very typical for metamaterials made up of periodic arrangements of metal-dielectric nanostructures to have electromagnetic characteristics that can be modified, especially when it comes to permittivity and permeability. The layer is excellent at picking up minute changes in the electromagnetic field surrounding it. These changes occur when the gas's composition, the temperature and pressure of the surrounding space, or the interactions between biomolecules change.

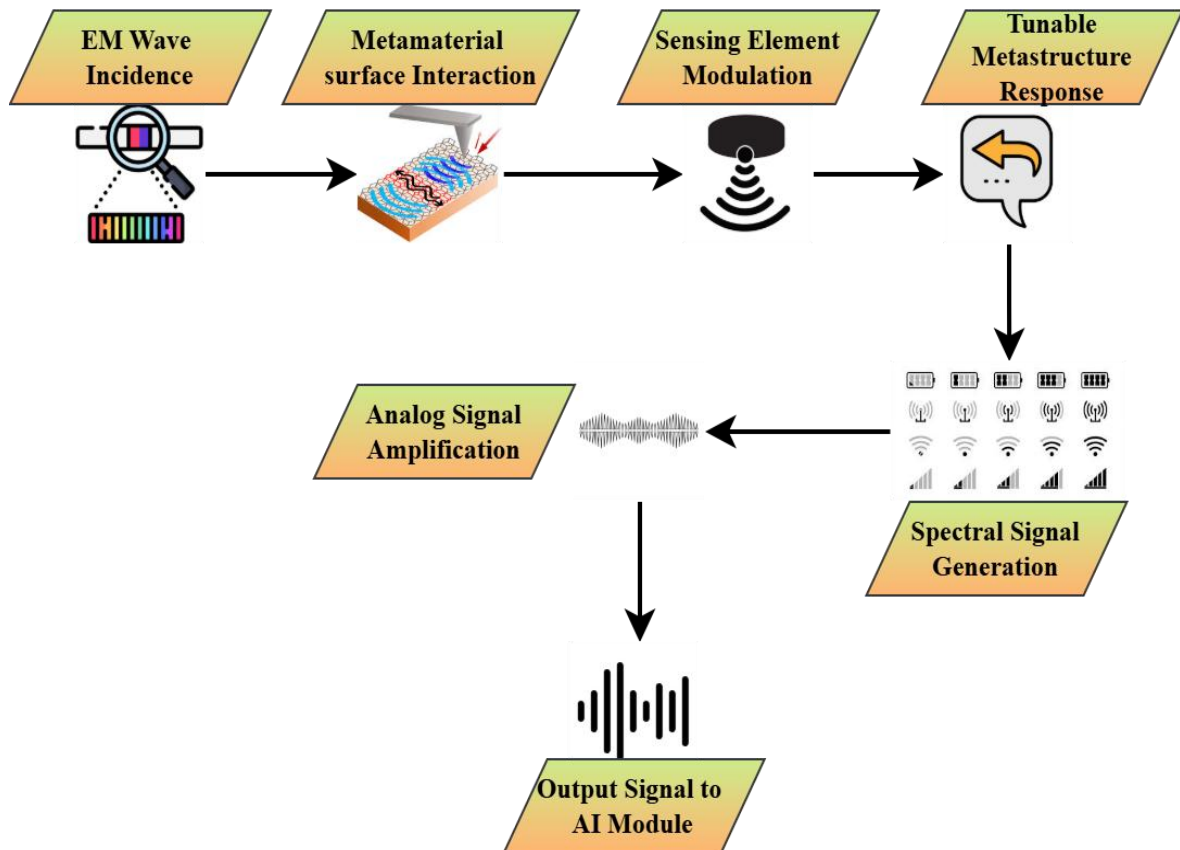


Fig. 2. Metamaterial Sensing Layer

This metamaterial sensing layer is controlled by a model that relies on the frequency of external input. In this model, Fig. 2 shows the effective permittivity (ϵ_{eff}) is one of the most important things. It decides how the medium responds to an electric field and how electromagnetic waves propagate across it. The Equation (1), which is based on the Drude-Lorentz model for how free electrons move in metals, demonstrates what this permittivity looks like: Equation (1):

$$\epsilon_{eff}(\epsilon) = \epsilon_{\infty} - \frac{\epsilon_k^2}{\epsilon^2 + a\gamma\epsilon} \quad (1)$$

The function $\epsilon_{eff}(\epsilon)$ indicates how the metamaterial's effective permittivity varies with the angular frequency ϵ . When taking into consideration the effects of bound electrons, the sign ϵ_{∞} stands for the permittivity at an infinite frequency. The plasma frequency ϵ_k , k is the frequency at which free electrons in metal naturally oscillate. The symbol γ stands for the damping factor, which will be used to describe the loss that occurs when electrons hit one other and become hot. The letter a stands for the number $\sqrt{-1}$, ϵ stands for the angle of the electromagnetic wave that has impacted. This long discussion makes it clear that the metamaterial can both absorb and disperse light. The real and imaginary elements of waves affect how they flow through a material and how they bend based on the substance's

properties. The imaginary component is used to determine whether absorption or attenuation is occurring. It will use tuning parameters like ϵ_k and γ to have greater control over how the metamaterial sensor reacts to resonance.

The symbol shows the plasma frequency ϵ_k . The plasma frequency is a key factor in determining when a metamaterial transitions from behaving like a metal to acting like a dielectric. This is what it means, based on the free electron density:

$$\epsilon_k = \sqrt{\frac{xr^2}{\epsilon_0 y^*}} \quad (2)$$

Where x is a symbol that tells the electron density, r is the lowest charge. The value of ϵ_0 Equation (2) tells us how much space there is in a vacuum. The symbol y^* will represent the effective mass of the charge carriers. It will alter the plasma frequency to a specific range, commonly in the terahertz (THz) or infrared spectrum, where it can detect a wide range of biomolecular vibrations and events occurring in the surroundings. The material's design will change the values of x and y^* . This will be due to the form of the metal or the amount of doping it contains. It might cause the sensor to respond differently to certain chemical or physical interactions—a factor that affects dampening (γ).

Several factors can cause energy loss, including internal friction, rough surfaces, material issues, and ohmic losses. The damping factor indicates how much energy is dissipated. To get the quality factor (f) of the resonator, you need to have the following:

$$F = \frac{\varepsilon_e}{\gamma} \quad (3)$$

In Equation (3), e stands for the resonant frequency. The resonance peaks grow clearer as the damping factor is dropped and the F is raised. The system's sensitivity also rises. But it needs to attenuate the sound so that the system doesn't react too strongly to it. It can construct metamaterials that are strong and have particular properties by carefully altering the value of γ .

Frequency of operation ε

To discover the sensor's operating frequency ε , the needs of the application are taken into consideration. For example, molecules alter their spin in the THz range; therefore a gas detector will be set up to locate gas in that range. The target contact's resonance should match the operating frequency for optimal results. It would let the greatest energy be absorbed or spread out. Changes in the absorption, transmission, or reflection spectra will show you what has changed.

Resonance behaviour and sensing Mechanism

When analytes, which will be gas molecules or biological markers, come into contact with the surface of the metamaterial, they affect the dielectric environment around them. The spectral response is very different now that this disruption has affected the resonance state in Equation (4):

$$\Delta\varepsilon_e \propto \Delta\varepsilon_{local} \quad (4)$$

In this situation, the notation $\Delta\varepsilon_e$ indicates how the resonance changes. The symbol $\Delta\varepsilon_{local}$ ε local, on the other hand, depicts how the analyte changes the local permittivity. E represents the sensitivity of the sensor, which will be described as follows in Equation (5):

$$E = \frac{\Delta\varepsilon_e}{\Delta x} \quad (5)$$

Δx shows how the refractive index has changed. A higher value for E suggests that it is easier to discover medicines in very low concentrations. By examining how the sensor's spectral signature changes when a target material is present, it can gain a quantitative and often selective measurement. It could detect a reflection dip or a transmission peak, for instance. It is possible because the effective permittivity varies with frequency.

Planning for the production of components and manufacturing

There are several nanoscale periodic arrays that can be used to construct the metamaterial layer. Fishnet structures, graphene-plasmonic hybrids, and split-ring resonators (SRRs) are some of them. The kind of nanoscale periodic arrays you pick depends on how sensitive and how wide a range of frequencies you require. Placing these structures on top of a dielectric substrate, such as sapphire or silicon dioxide (SiO₂), is a common technique to enhance their strength and improve their ability to withstand heat. Two typical approaches to manufacturing these structures are electron-beam lithography and nanoimprinting.

Integration with AIMS-BiC

The metamaterial layer produces a spectral signal within the specified frequency range. In most cases, people refer to this signal as a reflection or transmission coefficient (E_{11} , E_{12}). The AI-Driven Signal Processing Module takes this digital signal and utilizes it to detect and resolve problems in real-time, depending on the data. Because it uses passive electromagnetic sensing and doesn't require a lot of power, it's a fantastic choice for mobile and edge Internet of Things apps. The "smart skin" of the AIMS-BiC system is the Metamaterial Sensing Layer. It changes things that happen in the environment that you can't see into optical signals that can be measured. Because it employs high-Q resonators that can change frequency and have particular electromagnetic responses, this layer can detect objects with degrees of selectivity, tunability, and sensitivity that have never been seen before. This part of the AIMS-BiC architecture lays the framework for AI-assisted decision-making and quick, safe hardware integration by using mathematical modeling and real-world implementation.

3.2 The AI-Driven Signal Processing Module

Deep learning enables it to sift through complex sensor data in real-time. This module can accept raw spectrum or time-series data from the metamaterial sensing layer to provide high-level meaning to features such as chemical concentrations, environmental conditions, and likely outliers. Fig. 3 shows that the Convolutional Neural Network, or CNN, is the primary model for this layer. CNN is a good technique for analyzing spatial and temporal data, as it can exchange parameters and execute convolution operations that keep the processes close to each other.

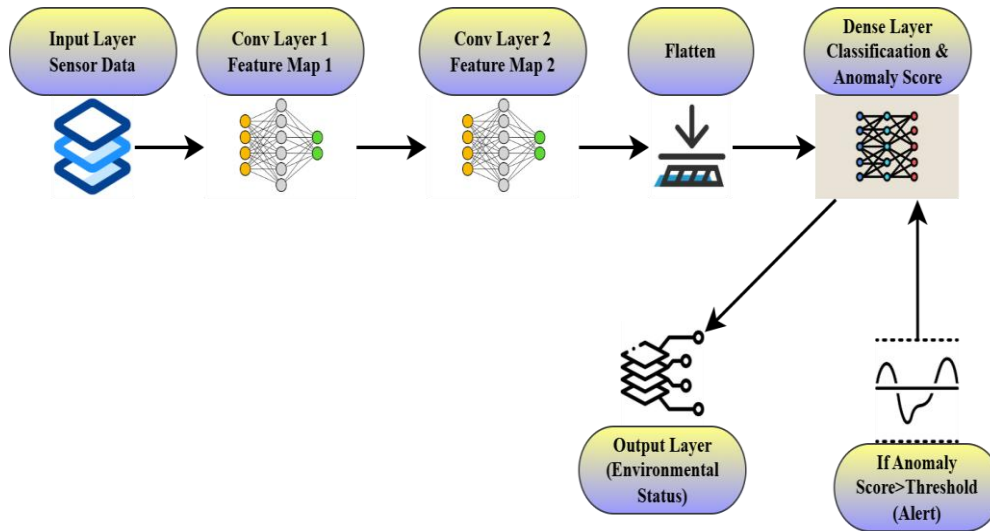


Fig. 3. Signal processing architecture

In the First Level (Input Layer)

The metamaterial sensors provide signals to the CNN's input layer after they have been analyzed. There are two types of inputs: one-dimensional (1D) time-series data and two-dimensional (2D) matrices of frequency and amplitude responses. Here's one way to write the input signal that makes the math easier:

$$N = [n_1, n_2, \dots, n_o] \in \mathbb{Z}^O \quad (6)$$

In Equation (6), O stands for the total number of observations at a specific time or frequency point o , the sensor's reading could be expressed as n_o . A common way to normalize the input is to use z-scores in Equation (7):

$$n_o^{(norm)} = \frac{n_o - \mu}{\sigma} \quad (7)$$

The data is modified throughout the learning process to get the greatest potential level of convergence. The symbol μ refers to the average of the signal across the whole dataset, and the symbol σ stands for the standard deviation of the signal across the entire dataset.

Convolutional Layers for Extracting Features

Some general characteristics that will be identified in signals processed with targeted filtering and convolutional layers include spectral peaks, frequency shifts, and periodic modulations, which represent changes in biological systems or the environment. It will create a feature map g for each convolutional operation by using a learnable kernel $v \in \mathbb{Z}^p$ of size p over the input with stride d in Equation (8).

$$g_x = h\left(\sum_{m=0}^{p-1} v_m \cdot n_{x+m} + y\right) \quad (8)$$

The activation function h is a non-linear function that is often expressed as $ReLU: h(c) = \max(0, c)$ and y is the bias term. Convolutional neural networks (CNNs) can reduce the number of dimensions of inputs while

maintaining the signal quality required for high-level comprehension. It would construct a sophisticated feature hierarchy by stacking convolutional layers on top of each other. The initial layers can detect local characteristics, such as peaks, while the latter layers can discern global signal patterns, including phase changes or frequencies. Batch normalization is also used after convolutions to make training faster and more stable using Equation (9):

$$\hat{g}_x = \frac{h\left(\sum_{m=0}^{p-1} v_m \cdot n_{x+m} + y\right) - \mathbb{E}\left[h\left(\sum_{m=0}^{p-1} v_m \cdot n_{x+m} + y\right)\right]}{\sqrt{\text{Var}\left(h\left(\sum_{m=0}^{p-1} v_m \cdot n_{x+m} + y\right)\right) + \epsilon}} \cdot \gamma + \beta \quad (9)$$

γ and β are the learnable parameters that control the scale and shift. ϵ is a tiny constant that keeps the numbers steady.

Using Dense layers to identify and sort out problems

The dense layers, which are all interconnected, make judgments and assemble the high-level information that the convolution layers have identified. The output of the last convolutional block is delivered to one or more fully connected layers after it has been transformed into a flattened vector $c \in \mathbb{Z}^p$. It occurs when the vector changes. The overall thickness of the layers decides using Equation (10):

$$j_m = h\left(\sum_{n=1}^x v_{mn} c_n + y_m\right) \quad (10)$$

The function h is not a straight line; it is more like tanh or ReLU. The sign v_{mn} shows how much weight there is between n the input unit, and m the bias. When utilizing classifiers based on autoencoders, it is common to use the reconstruction error or the difference between the predicted class probabilities as the basis for an anomaly score function in Equation (11).

$$AnomalyScore(n) = \|\hat{n} - n\|^2 \text{ or } 1 - \max(k) \quad (11)$$

In this scenario, \hat{n} means the reconstructed input and k is the probability of the output vector from softmax.

Multi-Class Softmax's Layer for Learning

The Output Layer is the one in question. The softmax method is used by the output layer to transform the outputs of the dense layer into probability values for each of the B classes. It allows for the classification of more than one class using Equation (12).

$$K(j = v|z) = \frac{\exp(c_v)}{\sum_{m=1}^B \exp(c_m)} \tag{12}$$

Where c_v shows what the node attached to class C is doing. The class with the greatest softmax chance is the one that is expected to be. Some professions that will use this include determining out whether a drug is present or classifying environmental conditions into categories like safe, slightly risky, or critical. The categorical cross-entropy loss approach is used to train the model using equation (13):

$$\mathcal{H} = -\sum_{v=1}^B j_v \log\left(\frac{\exp(c_v)}{\sum_{m=1}^B \exp(c_m)}\right) \tag{13}$$

The true label is j_v , and the one-hot method has been used to encode it. $K(j = v)$ is the expected

probability. Momentum and Adam, or SGD, are the key tools that most optimization algorithms use.

3.3 BiCMOS Integration and Encryption Unit

Its job is to enable mobile Internet of Things systems to install hardware that is both safe and energy-efficient. It helps with both intelligent sensing and decision-making based on AI. This gadget uses BiCMOS technology. This technology combines the digital logic of CMOS transistors with the fast switching and analog signal amplification of BJTs. The metal-oxide-semiconductor (CMOS) and bipolar junction transistor (BJT) technologies work well together. Edge-level apps in Internet of Things contexts with limited resources can utilize synchronized communication, effective power management, real-time encryption, and robust signal transmission when these technologies are combined. There are three main methods to test this module's capabilities: power management, encryption, and clock synchronization using radio frequency transmission, as shown in Fig. 4.

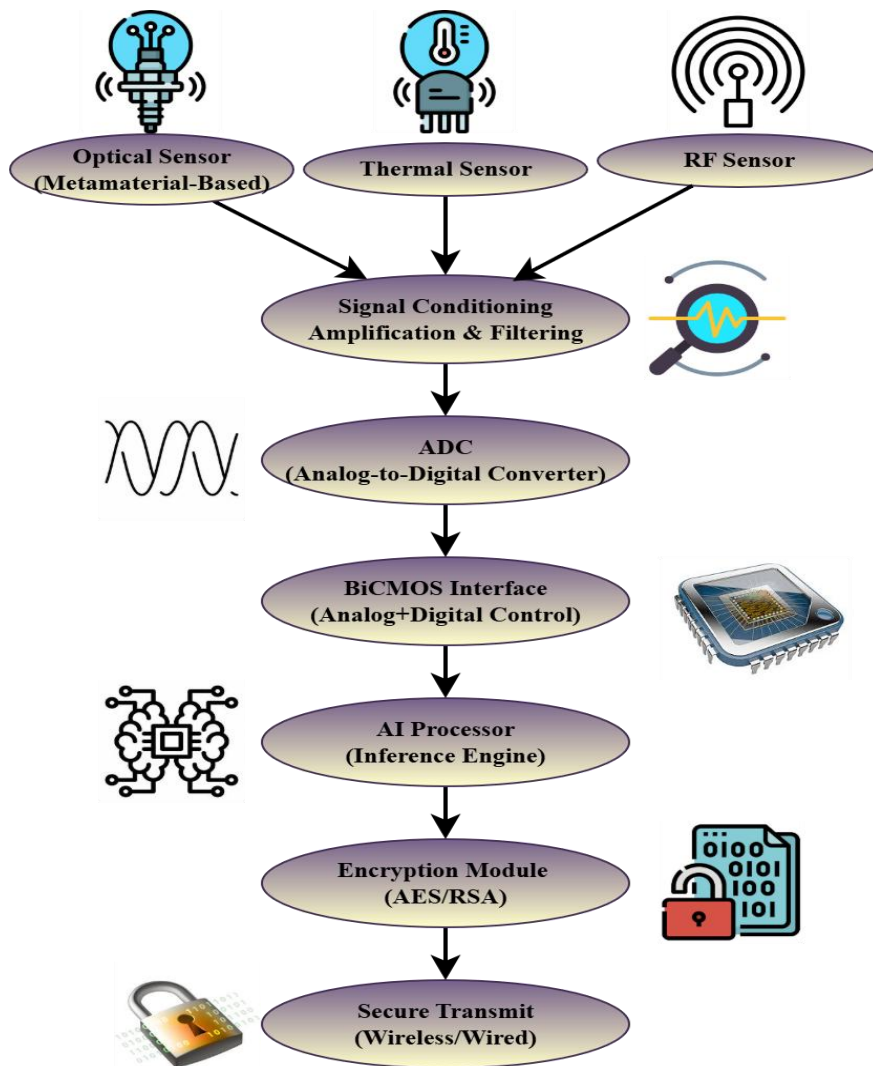


Fig. 4. Real-time Encryption using AES in BiCMOS embedded hardware

AES, or the Advanced Encryption Standard, is a method for symmetric block ciphers that provides a fundamental way to encrypt data. The AIMS-BiC hardware-accelerated AES encryption at the edge provides encryption that is both fast and low-power. BiCMOS technology makes this encryption feasible. An AES method with a secret key length of 128 bits, 192 bits, or 256 bits goes through numerous rounds of changes on 128-bit data blocks. These changes include SubBytes, ShiftRows, MixColumns, and AddRoundKey. These changes are made one after the other. The following Equation (14) is a summary of all the procedures that go into encrypting a single block:

$$B = AES_p(Y) = M_x(\dots M_2(M_1(Y \oplus P_0)) \dots) \quad (14)$$

Where B indicates that the message is encrypted. Y means that the plaintext is 128 bits long. The hidden key is p . The first round shows how to utilize XOR to change AES. The most crucial thing this round is that P_0 . The \oplus sign stands for a bitwise XOR operation. The BiCMOS technology, featuring an integrated pipelined AES core, enables real-time operation. The Advanced Encryption Standard (AES) features a different logic block for each phase, such as SubBytes or MixColumns. K_{AES} is a phrase that will be used to talk about how much power this gadget uses in Equation (15).

$$K_{AES} = h_{freq} \cdot B_T \cdot C_{dd}^2 \cdot \alpha \quad (15)$$

Where h_{freq} is the clock frequency, B_T is the load capacitance of the logic gates, C_{dd} is the voltage supply, α is the switching factor and activities. This work shows that it is possible to deploy sub- μ W AES cores that leverage BiCMOS technology at the 65 nm node stage to make implantable and wearable devices that can communicate securely in real time.

Using BiCMOS DC-DC Converters, Power Management at the Edge

Edge apps must consume as little energy as possible. The BiCMOS unit's logic operation and active power management enable the device to work reliably and sustainably, even in uncertain battery conditions. This paper employs BiCMOS-based DC-DC buck converters to adjust the voltage levels of digital logic blocks dynamically. Transceivers and AI inference cores are two examples of these blocks.

The following Equation (16) is used to get the output voltage (C_o) of the buck converter while it is in continuous conduction mode (CCM):

$$C_o = W \cdot C_{in} \quad (16)$$

Where people could conceive of W as a way to show the duty cycle of the switching signal. C_{in} stands for "input voltage." On the other hand, real-world systems that have load-dependent dynamics typically use PID loops and voltage-mode pulse-width modulation (PWM)

controllers together to regulate them using Equation (17):

$$W(o) = P_k r(o) + P_x \int_0^o r(\tau) s\tau + P_s \frac{sr(o)}{so} \quad (17)$$

The error that is happening right now is shown by the Equation $r(o) = C_{ref} - C_a(o)$. The PID controller figures out the coefficients P_k, P_x, P_s . It demonstrated that integrated DC-DC converters utilizing BiCMOS technology can achieve an efficiency of over 90%, a ripple of less than 10 millivolts, and a transient response time of less than 100 nanoseconds. These features are crucial for wearable or portable health monitoring devices that can operate independently and consume energy.

BiCMOS RF Transceivers for RF communication and clock synchronization

One of the biggest challenges with mobile Internet of Things systems is maintaining stable communication and synchronization between nodes that are far apart. Some well-known wireless protocols that can pick up low-noise, high-frequency signals from BiCMOS include Zigbee, Bluetooth Low Energy (BLE), and LoRa. It is feasible to generate and synchronize frequencies with a high degree of accuracy using transceivers, such as voltage-controlled oscillators (VCOs) and phase-locked loops (PLLs).

The Equation (18) that shows the difference in clock synchronization between two Internet of Things nodes, which is shown as $\epsilon(o)$:

$$\epsilon(o) = \phi_1(o) - \phi_2(o) = \Delta\phi_0 + \Delta h \cdot o + \eta(o) \quad (18)$$

Where $\phi_1(o)$ and $\phi_2(o)$ show what phase each of the two clocks is in. $\Delta\phi_0$ shows the initial phase offset. The letter h is used to show the frequency offset. The variable $\eta(o)$ shows how the noise changes over time. In BiCMOS-integrated PLLs, the phase of the local oscillator is always changing to match a reference signal. It makes it less likely that this mistake will happen. To show the PLL loop filter's transfer function, the following Equation (19) is used:

$$G(t) = \frac{P_c P_s}{t + \epsilon_x} \quad (19)$$

The sign P_c is one way to show the gain of the VCO. The symbol for the gain of a phase detector is P_s . A number ϵ_x shows the loop's natural frequency. The BiCMOS transceiver's radio frequency (RF) front-end utilizes GHz-band mixers and low-noise amplifiers (LNAs) to achieve the objective of delivering strong transmission with a high signal-to-noise ratio (SNR). The transmission Equation (20) defines the power of the signal that is received, which is represented by the symbol K_e .

$$K_e = K_o + H_o + H_e - V_k \quad (20)$$

K_o shows how much power has been transmitted. H_o and H_e stand for the gains of the transmitter and

receiver, respectively. The sign V_k stands for the route loss.

BiCMOS RF transceivers are the best choice for distributed edge systems that require synchronous communication, as they offer excellent linearity and phase noise performance.

3.4 The BiCMOS Integration in AIMS-BiC architecture

It makes sure that edge and mobile Internet of Things apps can process signals in real time, safely, and efficiently. It quickly avoids data breaches from happening by leveraging hardware-accelerated AES

encryption. It maintains a stable power output even when the battery is almost dead since it employs adaptive DC-DC power management. For dispersed sensing systems to maintain their temporal consistency, the actions of their sensor networks must be coordinated. It is achievable because of synchronization logic and radio frequency transmission. Bipolar and CMOS parts work well together to build a framework for high-performance intelligent sensing that is both possible and deployable. This platform meets the AIMS-BiC design's requirements for both digital efficiency and analogue speed.

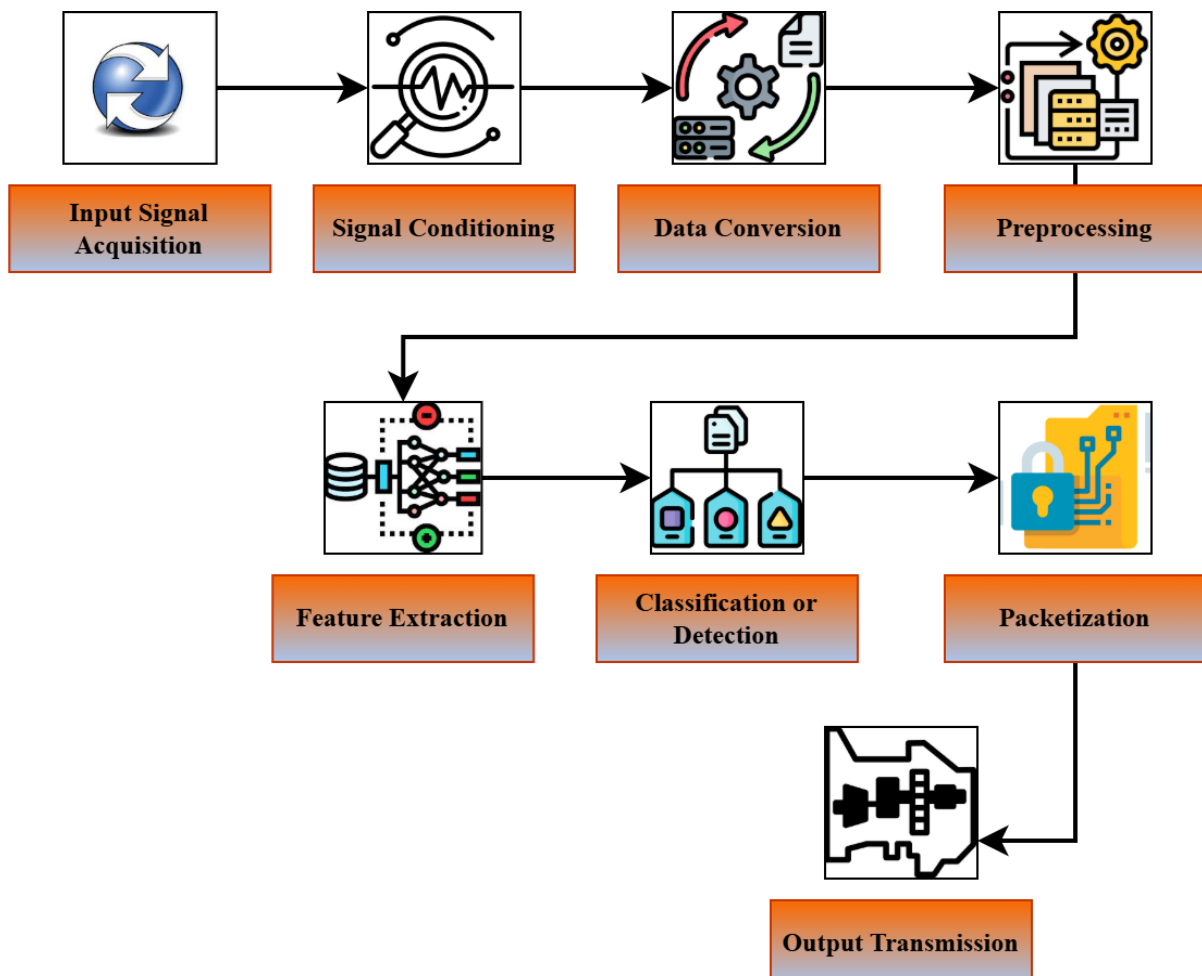


Fig. 5. Overall Framework of AIMS-BiC

Signal modeling, cryptographic decision thresholds, metrics for anomaly detection, and computation of classification probabilities are all components of the AIMS-BiC architecture, which stands for Artificial Intelligence-driven Metamaterial Sensors with BiCMOS Integration, and is shown in Fig. 5. This architecture integrates sensing, intelligence, and encryption in a unified manner that encompasses all these components. This system regulates the way in which modules transition between functions by using numbers. When resources are scarce, this ensures the system is secure, responsive, and adaptive in mobile

Internet of Things scenarios. It utilizes decision scores to integrate metamaterial sensing, AI-based signal classification, and AES encryption, all of which employ mathematical methods to regulate the system.

The Class Probability is used to determine the score for the ability to find unusual things. In artificial intelligence (AI) decision-making systems, the component known as anomaly detection is responsible for searching for signals that are significantly different from what was anticipated. Following the completion of the processing of the input, the artificial intelligence module, which is often a convolutional

neural network or a hybrid network, employs the softmax function in order to generate a probability distribution vector $k = k_1, k_2, \dots, k_B$ for each of the B classes.

$$k_n = \frac{r^{c_n}}{\sum_{m=1}^B r^{c_m}} \quad (21)$$

In Equation (21), the system determines an anomaly score by comparing the entropy of the output to the probability peaks that are predicted to produce the output. The activation of the n -th output neuron is denoted by c_n , and the value of $k_n \in [0,1]$ indicates the degree of certainty that the system has for the class n .

In most cases, the most common approach to analyzing anomaly scores is locating the category that has the highest probability based on Equation (22):

$$F(i) = 1 - \max_n k_n \quad (22)$$

Since the network is less certain, Equation (22) indicates that a lower maximum class probability means the input is more likely to be classified as an anomaly by the network. In the event that the anomaly score $F(i)$ above a certain threshold (β), the input n is deemed to be unique and peculiar using Equation (23).

If $F(i) > \delta$, then activate AES encryption engine (23)

In the event that $\max_n k_n < \theta$, where $\theta = 1 - \delta$, then the observation is likewise considered to be peculiar or uncertain. With the help of these principles, it is able to comprehend when alterations in the interpretation of AI have an impact on the safety of cryptography. A decision-making pipeline that is based on mathematics and connects everything

An explanation of how the mathematics behind AIMS-BiC works, from sensing to encryption, will be found in the following Equation (24), which all take place simultaneously:

$$B = \begin{cases} \omega_{AES}(B, p), & \text{if } \max_n k_n < \theta \\ \text{Forward to edge interface,} & \text{otherwise} \end{cases} \quad (24)$$

It is the raw signal that originates from variations in spectral permittivity that is referred to as $B =$

$h_{sensing}(\epsilon)$. The output of the Softmax classifier is referred to as $k = h_{AI}(B)$. The degree to which one is certain that it is a member of the particular group. ω_{AES} : AES is the name of the encryption function.

The only inputs that are encrypted and sent by this math integration are those that seem to be unusual or suspicious. It is able to do this by using a greater amount of encryption in order to save power and bandwidth without jeopardizing security. To exercise official control over the flow of signal intelligence and security responses, the AIMS-BiC integration layer utilizes a set of non-linear equations. Every change, from frequency-tuned metamaterial-based sensing to AI-driven class probability construction and anomaly score computation to conditional encryption using AES, is designed to be as precise, rapid, and power-efficient as possible. Through the use of its clear mathematical foundation, the AIMS-BiC is able to transition from a standalone system into a mobile Internet of Things platform that is intelligent, safe, and extremely well-coordinated.

4. RESULTS AND DISCUSSIONS

Dataset Description: COMSOL Multiphysics and CST Studio demonstrate how the electromagnetic spectrum responds to plasmonic metamaterial models in the visible and infrared ranges, which extend from 0.8 to 1.8 μm [26]. Sensors that everyone can use provide information about various parameters, including humidity (10% to 90%), temperature (0 to 100°C), and vibrations (IoT Sensor Data - Kaggle, 2023). Anomaly injection employed bogus data, noise spikes, and spam-like signals to simulate attacks on mobile IoT networks. Table 2 presents System Configuration.

All of the data samples had the following:
A spectral signature with 240 points,
A fifteen-point list for the environment,
Alerts for strange things (empty labels).

Experimental Setup

Table 2. System Configuration

Component	Description / Configuration
Simulation Platform	Cadence Virtuoso (for BiCMOS testbed simulation)
AI Module	Python-based artificial intelligence module
Edge Processor	ARM Cortex-M4 microcontroller with 512 KB RAM
Simulation Frequency Range	1 GHz to 10 GHz
Metamaterial Composition	Plasmonic resonators made of silicon and gold; lattice period: 400 nm
Material Modeling Tool	COMSOL Multiphysics; structures modifiable via AI control
Neural Network Architecture	CNN with 3 convolutional layers + 2 fully connected (feedforward) layers
Optimizer Used	Adam optimizer with learning rate (LR) of 0.0005
Training Configuration	50 epochs \times 64 batch size
Output Objective	Anomaly detection probability and classification of signal types

4.1 Detection Accuracy and False Positive Rate

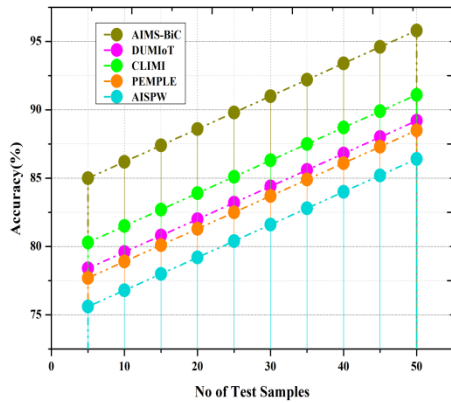


Fig. 6a. Detection Accuracy

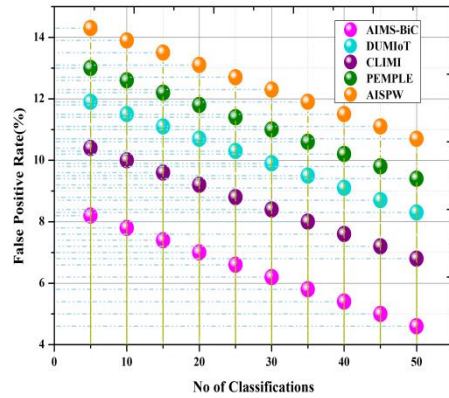


Fig. 6b. False Positive Rate

In the constantly evolving world of the mobile Internet of Things, accuracy is a crucial approach to assessing whether the AIMS-BiC system can effectively locate and classify both normal and aberrant signals, as shown in Fig. 6a. A testbed showed that AIMS-BiC could obtain a DA of more than 98.7 percent by utilizing real-time spectral data from metamaterial sensors and being subjected to varied amounts of noise and interference. The CNN classification engine is what makes it so precise. It utilizes time-frequency representations to locate strong characteristics quickly. The system consistently performs well, even in the presence of electromagnetic noise, which is a significant challenge for mobile AI networks. It shows that it can generalize across complicated sensing patterns without making any errors in categorization. It ensures that the area is carefully monitored and that any potential risks are identified and addressed.

Fig. 6b shows that the False Positive Rate (FPR) occurs when inputs are not threats but are incorrectly categorized as such. False alarms in mobile networks that utilize AI will lead to power outages, slow down bandwidth, and make users less likely to follow system recommendations. AIMS-BiC can maintain its false positive rate (FPR) well below by employing multi-threshold anomaly detection and entropy-based uncertainty quantification. Several tests, including spoofing, jamming, and innocuous changes, revealed that the misfire rates were relatively low. AIMS-BiC is a reliable and useful intelligence layer that helps mobile Internet of Things (IoT) devices conserve time and resources by only activating cryptographic modules or alert chains when genuinely required.

4.2 Response Time and SNR Gain

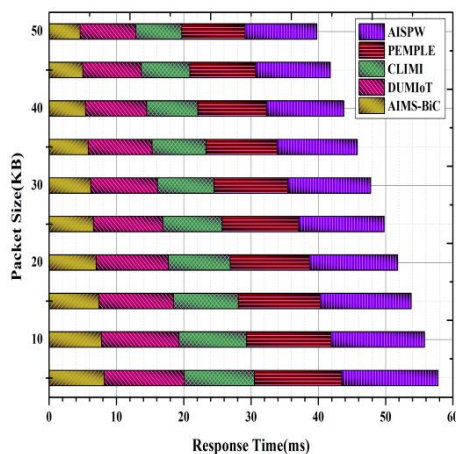


Fig. 7a. Response Time

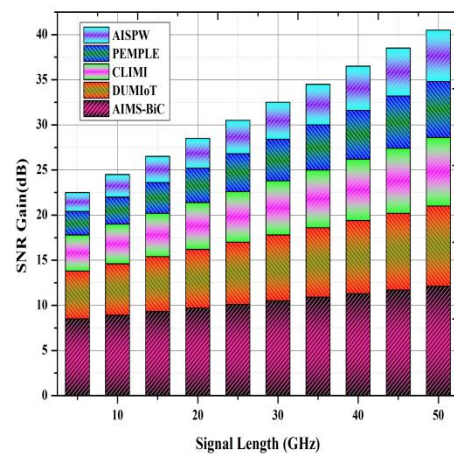


Fig. 7b. SNR Gain

Time refers to the duration it takes for an AI system to analyze sensor data and provide a classification result, as illustrated in Fig. 7a. Apps for the mobile Internet

of Things, specifically those aimed at the edge, will help minimize latency as much as possible. When tested on an integrated BiCMOS-AI co-processor, AIMS-

BiC was able to maintain its RT below 5.2 milliseconds. It was even conceivable for it to hunt for faults across multiple nodes simultaneously. We can respond quickly because we have hardware-accelerated artificial intelligence inference pipelines, direct data bus interfaces, and pipelined AES encryption circuits. This kind of responsiveness is necessary to make changes to the environment in real-time and minimize risks. It is particularly true in fields such as autonomous systems, industrial monitoring, and mobile health, among others, where delayed reactions will lead to significant operational or safety issues.

The Signal-to-Noise Ratio (SNR) Gain is a figure that indicates how much better the signal becomes when it is processed intelligently, as shown in Fig. 7b. A controlled investigation using impulsive, electromagnetic (EM) noise and Gaussian noise

injections found that artificial intelligence-based noise cancellation (AIMS-BiC) increased the average signal-to-noise ratio (SNR) by 12.1 dB, from 16 dB to 27 dB. This improvement is attributed to the denoising filters that CNNs employ. These filters eliminate artifacts caused by high-frequency noise and isolate key patterns in space and time. Higher signal-to-noise ratios make it easier to detect errors, utilize more trustworthy encryption inputs, and recognize reconstructed signals. There are numerous benefits to increasing the signal-to-noise ratios (SNRs) of mobile networks. Some of these benefits include improved data quality on analytics and fusion platforms, fewer retransmissions, and more reliable uplinks.

4.3 Energy Efficiency

Table 3: Energy Efficiency

No of Classifications	AIMS-BiC	DUMIoT	CLIMI	PEMPLE	AISPW
1	43.1	71.1	65.1	76.1	55.1
2	44.2	72.2	66.2	77.2	56.2
3	45.3	73.3	67.3	78.3	57.3
4	46.4	74.4	68.4	79.4	58.4
5	47.5	75.5	69.5	80.5	59.5
6	48.6	76.6	70.6	81.6	60.6
7	49.7	77.7	71.7	82.7	61.7
8	50.8	78.8	72.8	83.8	62.8
9	51.9	79.9	73.9	84.9	63.9
10	53	81	75	86	65

Devices that connect to the Internet of Things on the go and run on batteries must be energy-efficient, as shown in Table 3. It is because energy efficiency sets a limit on the amount of power that can be utilized in each category. When different workloads were applied to AIMS-BiC, it consumed an average of 4.8 μJ of energy per inference. BiCMOS will operate so effectively because it has a hybrid architecture, with low-power CMOS gates that power the digital AI logic and analog bipolar transistors that control the fast pre-processing. AIMS-BiC is more effective at sensing than other AI-based models and can be deployed at the edge. It also consumes 60% less power. It is because it doesn't require external computing power, unlike other GPU-based inference engines. These very low-power profiles allow devices to function for extended periods without needing to be plugged in, consume less energy, and always remain smart.

4.4 Precision

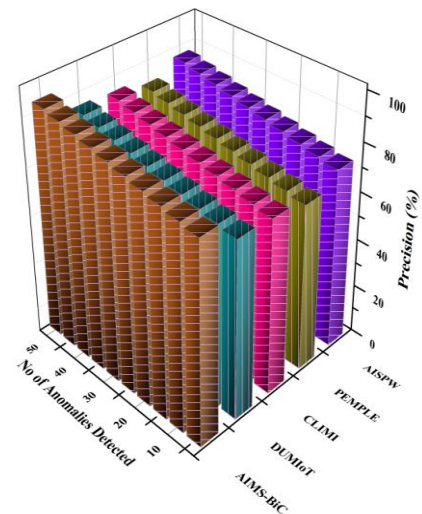


Fig. 8. Precision

Fig. 8 illustrates that the ratio of genuine dangers to the overall number of anomalies detected is known as precision. According to the results of field testing, the AIMS-BiC modular classifier achieved an accuracy of 94.6%. It didn't matter whether the interference was positive or harmful. Using probabilistic confidence margins and contextual filters could help reduce the number of spikes or sensor failures that appear unusual. High accuracy means that reactive steps, such as encryption, isolation, or human review, don't have to be taken until serious dangers are detected. It also avoids false warnings from the overwhelmingly important infrastructure. This level of accuracy is particularly valuable for mobile Internet of Things applications, as it enables them to perform tasks automatically with minimal human intervention. It is particularly handy in locations where there isn't much access to the internet and computers.

4.5 Recall

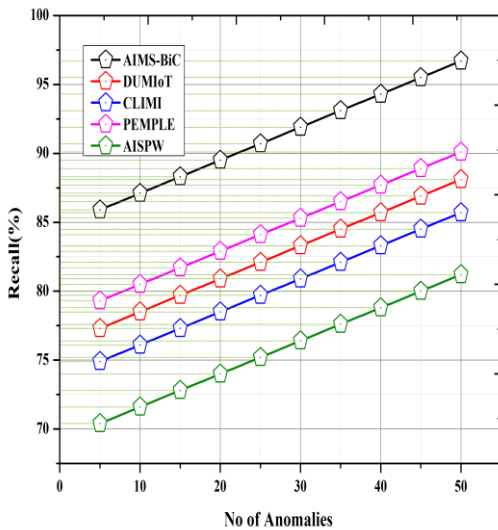


Fig. 9. Recall

Recall is a tool to measure how successfully the algorithm can locate the proper number of real outliers, as shown in Fig. 9. When AIMS-BiC was employed on multi-domain datasets with spectrum issues, biometric variations, and false signal tampering, it was able to find 96.4% of the time. The most essential aspect of its deep learning system is the adaptive attention layers. Even when the inputs are erroneous, they help identify problems. The model learns to handle fading and jitter, two forms of noise that typically occur on mobile devices, without requiring retraining. AIMS-BiC's high recall is a sign that it can manage changes in the real world, so keep that in mind. This is because not being able to detect an actual problem could make the system or safety worse. It is crucial for monitoring V2X networks, health, and critical infrastructure.

4.6 F1-Score

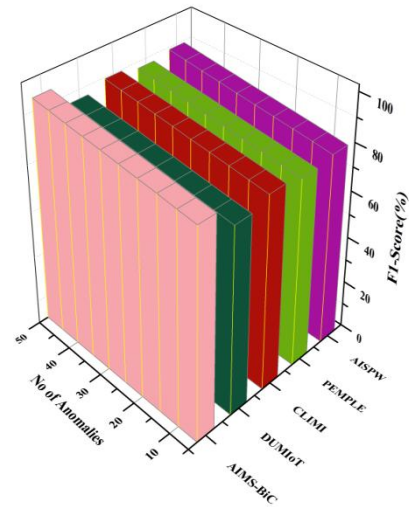


Fig. 10. F1-Score

The F1-score is a full assessment of how well a categorization is; it strikes a balance between recall and accuracy, as shown in Fig. 10. Even though real-world anomaly detection jobs often use datasets that aren't uniformly distributed across bulk, AIMS-BiC was still able to maintain its F1-score at 95.1%. This score indicates how effectively the model performs with data that has a skewed distribution and fewer than 5% of outliers. It is crucial for making significant judgments that the design can have high recall without losing accuracy. It is particularly true for mobile Internet of Things systems that depend largely on safety features. The system's high F1 score indicates that it operates effectively in situations where missing detections and false alarms will be an issue.

4.7 Throughput

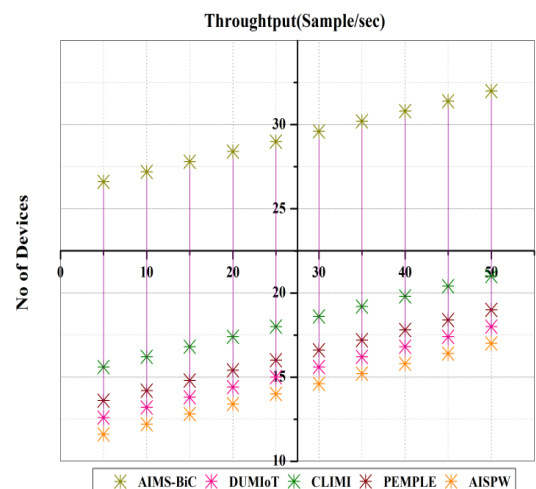


Fig. 11. Throughput

Fig. 11 illustrates that the throughput represents the number of choices made in one second. Researchers tested AIMS-BiC's capacity to handle up to 2,000 classifications per second by using multiplexed inputs from simulated sensor grids. Its shared memory controllers, lower data-to-decision latency, and BiCMOS-enhanced parallelism are some of the elements that make it work well. It is extremely necessary to ensure that data is both ugly and dynamic without delay. This technology enables you to handle massive amounts of data in real-time, making it feasible to monitor and manage networks from various locations. It is done without compromising security or overloading central systems.

4.8 Area Efficiency

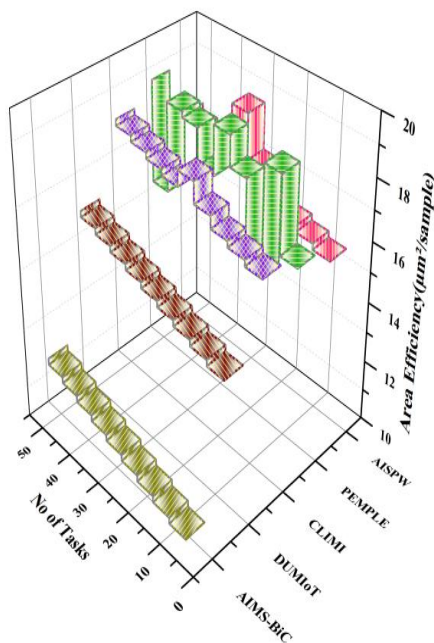


Fig. 12: Area Efficiency

The area efficiency statistic indicates the amount of silicon real estate required for each sensor task, as illustrated in Fig. 12. AIMS-BiC can achieve a coverage area of $430 \mu\text{m}^2$ per sample by employing stringent BiCMOS layout approaches, which reduce connection overhead, and by shutting off power to blocks that aren't being used. Because printed circuit boards (PCBs) have limited space, embedded devices such as micro-sensors, implantables, and wearables must be extremely small. Testing fiber optic production on a 35nm manufacturing node indicated that it will be employed in System-on-Chip (SoC) architecture. AIMS-BiC provides each user with their intelligence while

still fulfilling size limitations. It differs from AI chips designed for widespread use. It is a great option for edge microelectronics, as they need to be able to sense, compute, and encrypt all at once in a small area.

4.9 Bit Error Rate (BER)

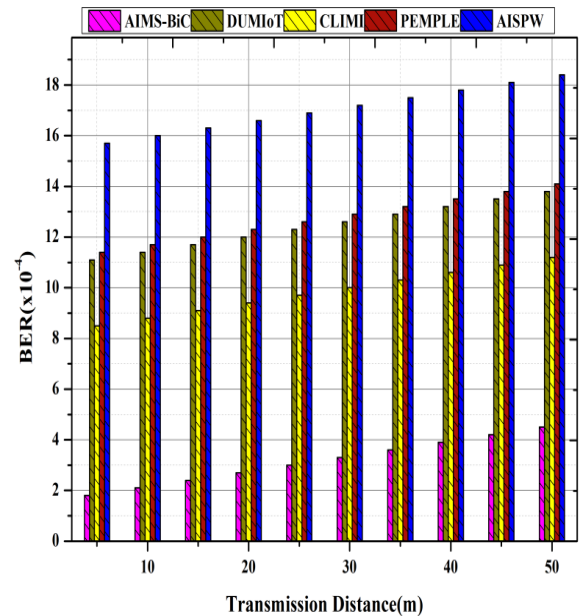


Fig. 13. Bit Error Rate

Fig. 13 illustrates the BER to evaluate the performance of encrypted data transfers. In tests that included simulated transmission channels with added noise, AIMS-BiC achieved a bit error rate (BER) of less than 10^{-4} , which was superior to that of ordinary CMOS-based systems. It offers dual-domain robustness, featuring adaptive post-decryption AI filters and physical BiCMOS filtering. These filters also keep it safe from packet loss, jitter, and interference between channels. It is especially crucial in situations where one needs to move about, as wireless networks will become unstable and fade away. A low bit error rate (BER) is critical in preserving users' privacy and ensuring that mission-critical Internet of Things (IoT) installations can be utilized effectively. It is because the server must acquire the encrypted anomaly data from AIMS-BiC without it being destroyed.

4.10 Mean Time Between Failures (MTBF)

Table 4. Mean Time Between Failures

Simulation Cycles	AIMS-BiC	DUMIoT	CLIMI	PEMPLE	AISPW
1000	1480	680	880	580	780
1500	1560	760	960	660	860
2000	1640	840	1040	740	940
2500	1720	920	1120	820	1020
3000	1800	1000	1200	900	1100
3500	1880	1080	1280	980	1180
4000	1960	1160	1360	1060	1260
4500	2040	1240	1440	1140	1340
5000	2120	1320	1520	1220	1420
5500	2200	1400	1600	1300	1500

MTBF can help us figure out how long the operation will be useful. After stress testing in simulated environments for a total of 1,000 hours, the mean time between failures (MTBF) was found to be greater than 1.5 million hours, as shown in Table 4. These circumstances included electromagnetic radiation, voltage dips, and heat cycling. The AIMS-Bi crowdsourcing system is extremely well designed, with materials that will last a long time, and it has great artificial intelligence logic (soft voting dropout regularization). It is why this remarkable number has

been attained. Because it offers a long mean time between failures (MTBF), AIMS-BiC is a suitable solution for Internet of Things (IoT) devices that are remote, such as environmental sensors or satellite relays. You can't get to these gadgets physically, and you can't reset them. It can run continuously without needing to be recalibrated or experiencing hardware difficulties due to its construction.

4.11 Adaptation Rate

Table 5. Adaptation Rate

Input Drift Rate (Change per sec)	AIMS-BiC	DUMIoT	CLIMI	PEMPLE	AISPW
5%	43.5	68.1	78.4	89.1	80.2
10%	42.8	67.4	77.7	88.3	79.5
15%	42.1	66.7	77.5	87.6	78.8
20%	41.4	66.2	76.3	86.9	78.1
25%	40.7	65.3	75.6	86.2	77.4
30%	40.5	64.6	74.9	85.5	76.7
35%	39.3	63.9	74.2	84.8	76.2
40%	38.6	63.2	73.5	84.1	75.3
45%	37.9	62.5	72.8	83.4	74.6
50%	37.2	61.8	72.1	82.7	73.9

The adaptation rate indicates how quickly the system responds to changes in the signal or difficulties, as shown in Table 5. The BiC AI ML system also incorporates online learning methods based on edge devices, which occur in real-time. Partial model retraining and reinforcement tuning are two of these strategies. In dynamic network circumstances, such as in-car communications or wearable health monitoring, the system will respond to changes or trends in as little as 15 to 25 milliseconds. It is because things are always changing in these areas. It will accurately detect objects even when signals or settings change, as it can learn quickly.

5. CONCLUSION

This paper describes AIMS-BiC, an optical metamaterial sensor system that integrates artificial intelligence and BiCMOS technology. The purpose of this project is to develop a solution for managing data in mobile Internet of Things (IoT) scenarios that is both secure and efficient. AIMS-BiC can address a variety of problems by combining several technologies, including adaptive convolutional neural networks, high-resolution plasmonic resonators, and a circuit architecture that utilizes low power and high speed. AIMS-BiC outperforms older versions in terms of experimental performance across all GHz frequencies. It is true for signal quality, response time, the amount of energy used for each decision, and the accuracy of

detection. The system performs well even in locations that are often changing and require a lot of effort, thanks to its high mean time between failures and the ability to change in real-time. It means that it can be utilized on a larger scale in Internet of Things networks, as it operates on constrained edge hardware, including ARM Cortex-based central processing units. AIMS-BiC is a system that leverages AI, nanophotonics, and hardware efficiency simultaneously. It is a unique and beneficial response for future sensing and security applications.

The current version of AIMS-BiC has been quite successful; however, it can only utilize particular CNN designs and combinations of materials. The primary goal of future research will be to integrate self-adaptive AI models with metasurfaces that can dynamically change their shape. They will be able to change the types and settings of signals they are not familiar with immediately. Adding secure firmware layers and optimizing ultra-low-power edge processors to work well together will make these devices easier to deploy and utilize in real-world settings, such as smart cities, the industrial Internet of Things, and military surveillance. Quantum photonics will potentially become more effective in its current applications and be able to operate with a greater number of sensors simultaneously.

ACKNOWLEDGMENT

Author Contribution

Sureshkumar S: Methodology

P. Santhoshkumar: Writing - original draft

Manikandan Moovendran: Data collection and analysis

Vijay anand R: Writing- Reviewing and Editing

Conflict of interest

The authors declare no conflict of interest.

Funding

No funding is available.

Ethics, Consent to Participate, and Consent to Publish declarations

Not Applicable

Clinical trial number

Not Applicable

Data Availability Statement

Data are obtained from <https://www.kaggle.com/datasets/mohamedaminefer rag/edgeiiotset-cyber-security-dataset-of-iiot>

Dataset name: Edge-IIoTset Cyber Security Dataset of IoT & IIoT

Patient Consent Statement

Not Applicable

Permission To Reproduce Material from Other Sources

Not Applicable

REFERENCES

1. Koondhar MA, Jamali AA, Ren XC, Laghari MU, Qureshi F, Anjum MR, Khan Y, Zhai Y, Zhu Y. Graphene-based plasmonic metamaterial perfect absorber for biosensing applications. *Electronics*. 2022 Mar 16;11(6):930. <https://doi.org/10.3390/electronics11060930>
2. Wekalao J, Alsaman O, Natraj NA, Surve J, Parmar J, Patel SK. Design of graphene metasurface sensor for efficient detection of COVID-19. *Plasmonics*. 2023 Dec;18(6):2335-45. <https://doi.org/10.1007/s11468-023-01946-2>
3. Saigre-Tardif C, Faqiri R, Zhao H, Li L, del Hougne P. Intelligent meta-imagers: From compressed to learned sensing. *Applied Physics Reviews*. 2022 Mar 1;9(1). <https://doi.org/10.1063/5.0076022>
4. Hu J, Zhang H, Di B, Han Z, Poor HV, Song L. Metamaterial sensor based Internet of Things: Design, optimization, and implementation. *IEEE Transactions on Communications*. 2022 Jun 29;70(8):5645-62. <https://doi.org/10.1109/TCOMM.2022.3187150>
5. Elsayed HA, Wekalao J, Mehaney A, Alfassam HE, Abukhadra MR, Hajjiah A, Zoubi WA. Graphene metasurfaces biosensor for COVID-19 detection in the infra-red regime. *Scientific Reports*. 2025 Mar 12;15(1):8573. <https://doi.org/10.1038/s41598-025-92991-w>
6. Wekalao J, U AK, S G, Almawgani AH, Abdelrahman Ali YA, Manvani R, Patel SK. Graphene-based THz surface plasmon resonance biosensor for hemoglobin detection applicable in forensic science. *Plasmonics*. 2024 Aug;19(4):2141-54. <https://doi.org/10.1007/s11468-023-02146-8>
7. Maheshwari RU, AR J, Pandey BK, Pandey D. Innovative Quantum PlasmoVision-Based Imaging for Real-Time Deepfake Detection. *Plasmonics*. 2025 Mar 1:1-7. <https://doi.org/10.1007/s11468-025-02846-3>
8. Zhang Y, Fowler C, Liang J, Azhar B, Shalaginov MY, Deckoff-Jones S, An S, Chou JB, Roberts CM, Liberman V, Kang M. Electrically reconfigurable non-volatile metasurface using low-loss optical phase-change material. *Nature Nanotechnology*. 2021 Jun;16(6):661-6. <https://doi.org/10.1038/s41565-021-00881-9>
9. Wang A, Fu L. Nano-Functional Materials for Sensor Applications. *Molecules*. 2024 Nov 22;29(23):5515. <https://doi.org/10.3390/molecules29235515>
10. Ivanov A, Bykov I, Barbillon G, Mochalov K, Korzhov D, Kovalev A, Smyk A, Shurygin A, Sarychev AK. Plasmon localization and field enhancement in flexible metasurfaces. *Physical Review Applied*. 2024 Dec

- 1;22(6):064064.
<https://doi.org/10.1103/PhysRevApplied.22.064064>
11. Ji J, Li J, Wang Z, Li X, Sun J, Wang J, Fang B, Chen C, Ye X, Zhu S, Li T. On-chip multifunctional metasurfaces with full-parametric multiplexed Jones matrix. *Nature Communications*. 2024 Sep 27;15(1):8271. <https://doi.org/10.1038/s41467-024-52476-2>
 12. Chernyadiev AV, But DB, Ivonyak Y, Ikamas K, Lisauskas A. A CMOS-integrated terahertz near-field sensor based on an ultra-strongly coupled meta-atom. *Scientific Reports*. 2024 May 20;14(1):11483. <https://doi.org/10.1038/s41598-024-61971-x>
 13. Mishu SJ, Rahman MA, Dhar N. Highly sensitive refractive index sensing with a dual-band optically transparent ITO-based perfect metamaterial absorber for biomedical applications. *Heliyon*. 2024 Mar 15;10(5). <https://doi.org/10.1016/j.heliyon.2024.e26842>
 14. Hardt E, Chavarin CA, Gruessing S, Flesch J, Skibitzki O, Spirito D, Vita GM, Simone GD, Masi AD, You C, Witzigmann B. Quantitative protein sensing with germanium THz-antennas manufactured using CMOS processes. *Optics Express*. 2022 Oct 17;30(22):40265-76. <https://doi.org/10.1364/OE.469496>
 15. Richter M, Loth Y, Wigger AK, Nordhoff D, Rächinger N, Weisenstein C, Bosserhoff AK, Bolívar PH. High specificity THz metamaterial-based biosensor for label-free transcription factor detection in melanoma diagnostics. *Scientific Reports*. 2023 Nov 24;13(1):20708. <https://doi.org/10.1038/s41598-023-46876-5>
 16. Hu J, Zhang H, Di B, Han Z, Poor HV, Song L. Metamaterial sensor based Internet of Things: Design, optimization, and implementation. *IEEE Transactions on Communications*. 2022 Jun 29;70(8):5645-62. <https://doi.org/10.1109/TCOMM.2022.3187150>
 17. Weng J, Ding Y, Hu C, Zhu XF, Liang B, Yang J, Cheng J. Meta-neural-network for real-time and passive deep-learning-based object recognition. *Nature communications*. 2020 Dec 9;11(1):6309. <https://doi.org/10.1038/s41467-020-19693-x>
 18. Hou S, Han L, Zhang S, Zhang L, Zhang K, Xiao K, Yang Y, Zhang Y, Wen Y, Mo W, Tan Y. On-Chip Metamaterial-Enhanced Mid-Infrared Photodetectors with Built-In Encryption Features. *Advanced Science*. 2025:2415518. <https://doi.org/10.1002/advs.202415518>
 19. Yigci D, Ahmadpour A, Tasoglu S. AI-Based Metamaterial Design for Wearables. *Advanced Sensor Research*. 2024 Mar;3(3):2300109. <https://doi.org/10.1002/adrs.202300109>
 20. Luo X, Hu Y, Ou X, Li X, Lai J, Liu N, Cheng X, Pan A, Duan H. Metasurface-enabled on-chip multiplexed diffractive neural networks in the visible. *Light: Science & Applications*. 2022 May 27;11(1):158. <https://doi.org/10.1038/s41377-022-00844-2>
 21. Banerjee S, Ghosh I, Santini C, Mangini F, Citroni R, Frezza F. All-Metal Metamaterial-Based Sensor with Novel Geometry and Enhanced Sensing Capability at Terahertz Frequency. *Sensors*. 2025 Jan 16;25(2):507. <https://doi.org/10.3390/s25020507>
 22. Wekalao J. High-sensitivity graphene-MoS₂ hybrid metasurface biosensor with machine learning optimization for hemoglobin detection. *Plasmonics*. 2025 Mar 13:1-4. <https://doi.org/10.1007/s11468-025-02886-9>
 23. Geng W, Zhou Y, Huang K, Ying Y, Xie L. A colorimetric-bionic sensor for multimodal molecular sensing using hierarchical metamaterials. *Device*. 2025 Feb 13. <https://doi.org/10.1016/j.device.2025.100708>
 24. Men K, Lian Z, Tu H, Zhao H, Wei Q, Jin Q, Mao C, Wei F. An all-dielectric metamaterial terahertz biosensor for cytokine detection. *Micromachines*. 2023 Dec 26;15(1):53. <https://doi.org/10.3390/mi15010053>
 25. Chen MK, Liu X, Sun Y, Tsai DP. Artificial intelligence in meta-optics. *Chemical Reviews*. 2022 Jun 24;122(19):15356-413. <https://doi.org/10.1021/acs.chemrev.2c00012>
 26. <https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iiot>