IoT SECURITY CAMERA

Mujammil Sheikh[*1], PranamKawale[*2], AbhijeetSonone[*3], RohitKale[*4], Ankush Gupta [*5], Prachiti Adghulkar[*6]

*[*1]Student,DepartmentofInformationTechnology,GovindraoWanjariCollegeof Engineering & Technology, Nagpur, Maharashtra, India*
muzammilsheikh139@gmail.com,
*[*2]Student,DepartmentofInformationTechnology,GovindraoWanjariCollegeof Engineering & Technology, Nagpur, Maharashtra, India*
pranamkawale@gmail.com,
*[*3]Student,DepartmentofInformationTechnology,GovindraoWanjariCollegeof Engineering & Technology, Nagpur, Maharashtra, India*
abhideva2105@gmail.com,
*[*4]Student,DepartmentofInformationTechnology,GovindraoWanjariCollegeof Engineering & Technology, Nagpur, Maharashtra, India*
rkale7946@gmail.com,,
*[*5]Student,DepartmentofInformationTechnology,GovindraoWanjariCollegeof Engineering & Technology, Nagpur, Maharashtra, India*
ankushgupta8421@gmail.com
*[*6]AssistantProfessorDepartmentofInformationTechnology,GovindraoWanjari College of Engineering & Technology, Nagpur, Maharashtra, India*
prachiti.ganorkar @gmail.com

Abstract
This research paper presents the design and development of an IoT-based smart security camera system that performs real-time monitoring and automated threat detection. Unlike conventional CCTV systemsthat only record video and require constant human supervision, the proposed system is capable ofanalysing live footage using computer vision techniques. It detects motion, captures images or video, and identifies individualsbycomparingtheirfaceswithastoreddatabase. Wheneveranunknown orsuspicious person is detected, the system automatically sends an alert to the concerned authority through email and logs the event for future tracking. By integrating Wi-Fi connectivity, face recognition, and automated notification, the system reduces manual effort, improves response time, and enhances overall security. The proposed solution demonstrates how intelligent surveillance can transform traditional monitoring into a proactive and efficient security mechanism suitable for modern environments.
Keywords: *IoT, Smart Surveillance, Face Recognition, Motion Detection, Computer Vision, Real-time Alerts.*

1. INTRODUCTION

In the modern era, the rapid growth of urbanization has made security a primary concern for bothresidential and commercial sectors. Traditional surveillance systems, while widely deployed, often act as passive recording devices that require constant human intervention to detect anomalies [1]. The main limitation of these conventional setups is their inability to distinguish between routine movements and actual security threats in real-time. With the advent of the Internet of Things (IoT) and Artificial Intelligence, there is a transformative shift towards autonomous monitoring solutions that can "think" and "react" without fatigue [3].

ThecoremotivationofthisresearchistodevelopanIOT-basedSmartSecurityCamerathatbridgesthegap between simple video recording and intelligent threat detection. By leveraging the YOLOv4-tiny (You OnlyLookOnce)deeplearningarchitecture,thesystemis designedtoachievehigh-speedobjectdetection with significant accuracy [2]. Unlike standard motion sensors that often trigger false alarms due to environmental changes, our proposed system utilizes the OpenCV library to perform sophisticated image processing, ensuring that alerts are only generated when a human presence or unauthorized activity is confirmed [5].

What sets this intelligent framework apart is its seamless integration of edge computing and cloud communication. When a potential breach is detected, the system does not merely log the event; it actively communicates [4]. Through the Twilio API, the system bridgesthe physical and digital worlds by sending instantaneousSMSandemailnotificationstotheuser'sregistereddevice[7].Thisensuresthattheproperty owner remains virtually present at their premises, regardless of their geographical location [6].

Byutilizinga robusthardware stack—includinganIntelCore i5processorand8GB ofRAM—thesystem manages complex mathematical computations locally to maintain real-time performance while using the cloud for remote alerts [8]. This research aims to provide a scalable, cost-effective, and highly reliable

securityframework[9].Ultimately,thegoalistomake"SmartSecurity"anaccessiblereality,empowering users with proactive awareness and peace of mind in an increasingly unpredictable world [10].

2. LITERATURE SURVEY

Title:ThroughtheLens:IPCameraSecurity &Privacy
Author:H.El-Tajetal.Year:2025
This research provides a comprehensive analysis of the security and privacy landscape of modern IP cameras. It highlights how lens- based vulnerabilities can lead to unauthorized access and data breaches. The paper suggests advanced encryption and firmware hardening as primary defenses against emerging privacy threats in IoT-connected surveillance devices.

Title:UnmaskingVulnerabilitiesofSmartIoTCameras
Author:S.Bhardwajetal.Year:2024
The study focuses on identifying hidden security flaws in popular smart IoT cameras. It discusses how weak authentication protocols allow attackers to gain control of camera feeds. The authors propose a securityframeworkthatincludesmulti-factorauthenticationandregularvulnerabilityscanningtoprotect end-users from cyber-attacks.

Title:Security &PrivacyEvaluationofIPCamerasonShodan
Author:K.NgandA.MehrnezhadYear:2024
This paper evaluates the exposure of unsecured IP cameras globally using the Shodan search engine. It revealsthatthousands ofcamerasremainaccessibleduetodefaultcredentialsandunpatchedsoftware.The study emphasizes the need for user awareness and automated security configuration tools to minimize public exposure.

Title:IoTCamerasExploitedinFinancialCrimes
Author:D.Siwakotietal.Year: 2024
This research explores the role of compromised IoT cameras in facilitating financial crimes, such as monitoring ATM PIN entries or unauthorized surveillance in banking sectors. It demonstrates how attackersusecameraexploitstogathersensitiveinformation,stressingtheimportanceofphysicaland digital security integration in financial institutions.

Title:PETIoT:PenetrationTesting IoT
Author:G.Bellaetal.Year:2023
The authors introduce a specialized penetration testing framework called PETIoT specifically for IoT devices.Thepaperappliesthisframeworktosmartcamerastotesttheirresilienceagainstcommonattack vectors like DDoS and Man- in-the-Middle (MitM) attacks. The findings suggest that many consumer-grade cameras lack basic penetration resistance.

Title:SurveyonIoT&EmbeddedFirmwareSecurity
Author:VariousAuthorsYear:2023
Thissurveyprovidesanextensiveoverviewofthesecuritychallengeswithintheembeddedfirmwareof IoTdevices.Itdetailshowoutdatedfirmwareversionsserveastheweakestlinkincamerasecurity.The paperadvocates forthe implementation of automatedfirmware update mechanismsto ensure long-term device safety.

Title:VulnerabilityAssessmentandPenetrationTestingonIP Cameras
Author:PietroBiondietal.Year: 2022
Thestudyperformsadetailedvulnerabilityassessmentandpenetrationtestingonspecificcameramodels, suchastheTP-LinkTapoC200.Itidentifiesseveralcriticalsecuritygapsandprovidesrecommendations for improving security defaults. Theresearch highlights the need for rigorous testing of diverse camera models before market release.

Title:IoT Security:End-to-EndView&Case Study
Author:Z.Lingetal.Year:2018
This work provides an end-to-end perspective on IoT security, using smart cameras as a primary case study.Ittracksthedatapathfromthecamerasensortothecloud,identifyingpotentialleakpointsateach stage. The

paper concludes that securing the entire ecosystem ismore effective than securing individual components in isolation.

Title:FacialRecognition &IoTCameraVulnerabilities
Author:A.Ravulaetal.Year: 2018
studiedtheintegrationofcloudAPIs.Researchin[6]and[7]showedhowtheTwilioAPIcouldbeused to bridge the gap between detection andaction.Their findings confirmed that sendinganinstant SMSor The paper discusses the intersection of facial recognition technology and IoT camera vulnerabilities. It exploreshowspoofingattackscanbypassrecognitionsystemsifthecamerahardwareiscompromised.The authors recommend the use of liveness detection and spatio-temporal filters to enhance the accuracy and security of recognition systems.

Title:AutomatedDynamicFirmwareAnalysisatScale
Author:A.Costinetal.Year: 2015
This foundational researchintroduces a method for automateddynamic analysis of firmware across a large number of IoT devices.Bytestingthousands offirmware samples, thestudy identifiedwidespreadsecurity issuesinIPcameras thathadbeenoverlookedforyears.Itremains akeyreferenceforunderstandinglarge-scale firmware auditing.

3.1 SystemArchitecture

1. SensingandDataAcquisitionLayer
The first stage of the architecture involves the continuous capture of the physical environment. An HD Cameramoduleis deployedastheprimarysensingunit,whichrecords alivevideostreamofthemonitored area. Unlike conventional systems that store raw footage without analysis, this layer provides a real-time data feed to the processing unit.

2. IntelligentProcessingLayer(YOLO&OpenCVModule)
This layer acts as the "brain" of the system. The captured video frames are processed locally on an Intel Corei5processingunit.First,theOpenCVlibraryisusedtopre-processtheframes,andthentheYOLOv4-tiny deep learning model scans the frames in real-time to identify human presence. This ensures that the system only reacts to genuine security threats.

3. IoTCommunicationandCloud Layer
Once a potential threat is detected, the system transitions to the communication phase. Using a WiFi/Internetgateway,thelocalprocessingunitconnectstothecloud.ThislayerinterfaceswiththeTwilio API, which handles the cloud-to-mobile communication, ensuring the notification reaches the user regardless of their location.

4. AutomatedResponseandLoggingMechanism
The final layeris responsible foroutput and record-keeping. The system automatically triggers an instant SMSandEmailnotificationtotheowner'sregisteredmobiledevice.Simultaneously,thesystemperforms dataloggingbysavingthe eventdetailsandvideosnippetstoa500GBHDD forfuture forensic evidence.

3.2 WorkingProcedure

- The system operates through a seamless flow that starts with the continuous capture of HD video frames, which are then pre-processed by OpenCV to ensure image clarity. These frames are analyzed in real-time by the YOLOv4-tiny deep learning model to accurately detect human presence and filter out false alarms. Once an intruder is confirmed, the system uses a WiFigateway to connect with the Twilio API, triggering instant SMS and email alerts to the owner's mobile device. Simultaneously, the event is logged and saved to a500GB HDD, providing the user with both immediate notification and a permanent record for future forensic evidence.

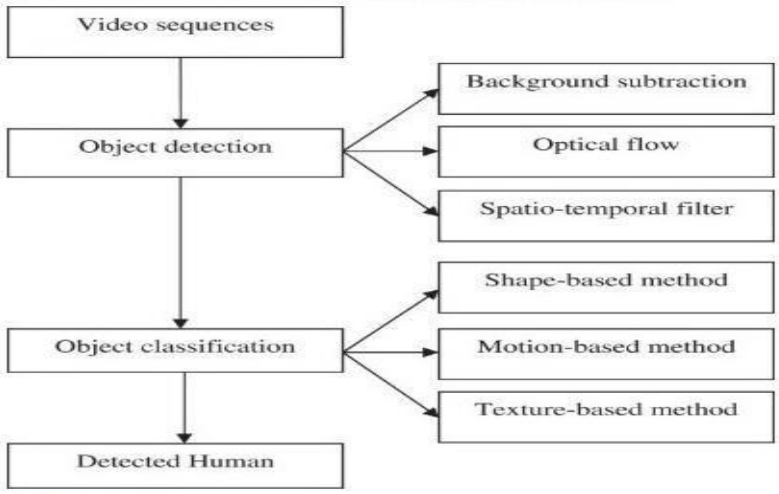
3.3 KeyFeaturesoftheProposedSystem

- Real-timelivesurveillance
- Intelligentpersondetection
- Reducedsecuritylaborcost
- Fasteremergencyresponse
- Securelocaldatastorage.

4. METHODOLOGY

The methodology begins with real-time video data collection using an HD camera module installed in the monitored area. The proposed system follows a modular design approach, allowing individual components such as sensing, edge intelligence, and cloud communication to operate independently. This modularity improves system scalability and simplifies maintenance and future upgrades. Data preprocessingtechniques such as noise removal and frame resizing via OpenCV are applied before analysis. The YOLOv4-tiny model generates an initial detection of objects based on motion and visual features. Deep learning layersfurtherrefine theclassification bylearningcomplex patternsfromspatialand temporal data. The final output triggers the automated notification system and logs the evidence locally.
Theflowdiagramillustratestheworkingofthe proposedIoT-basedsmartsecuritysystem.

Figure1.Methodology



TheVideosequencescapturedbythecameraserveastheprimaryinput.DuringtheObjectdetectionphase, techniques like background subtraction, optical flow, and spatio-temporal filters are utilized to identify moving entities. Once an object is isolated, it undergoes Object classification using shape-based, motion-based, and texture-based methods to distinguish between routine activity and a Detected Human. Based on this analyzed data, the system triggers the Twilio API to send real-time alerts. This automated process ensures precise threat identification, reduced false alarms, and improved home security.
Step1:Collectlivevideosequencesandenvironmentalvisualdatausingthe HDcamera. Step 2: Preprocess frames and apply filters for noise removal using OpenCV.
Step 3: Apply object detection methods like background subtraction to identify moving entities.
Step4:Useobjectclassification(YOLOv4)andtexture-basedmethodstoaccuratelyidentifyhuman presence.
Step5:Activatethenotificationandloggingmechanismbasedonthefinaldetection.

5. RESULTS

The proposed system demonstrates significant improvement in security monitoring efficiency compared to traditional surveillance methods. The experimental observations indicate that the system responds effectively to varying environmental conditions and lighting levels. Although the current implementation focuses on humandetection for home security, the same approach can be extended to industrial monitoring orrestrictedzonealertswithminor modifications.Automatedthreat detectionreducestheneedfor constant manual observation and ensures rapid response through instant mobile notifications. The integration of OpenCV and YOLOv4-tiny improves adaptability to different background noises and motion patterns. The system also reduces human labor dependency andsupports scalable smart city orprivate security solutions.

6. CONCLUSION

In conclusion, the proposed IoT-based smart security camera demonstrates how intelligent sensing anddata-driven decision-making can significantly enhance premises monitoring and threat management. By integrating an HD camera module with OpenCV and YOLOv4-tiny deep learning algorithms, the system enables precise, real-time human detection and automated cloud-based notifications through the TwilioAPI. This approach minimizes human error, reduces the reliance on constant manual surveillance, and ensures that owners receive alerts based onactual human detection rather than generalized motion triggers.

Furthermore, the automation of threat detection and instant alerting contributes to faster response times, improvedsafety,andreliableevidencecollectionona500GBHDD.Byoptimizingresourceutilizationand lowering the rate of false alarms, the system supports sustainable and smart security practices. The integration ofIoT with advanced predictive models represents ascalable andefficient solution formodern home surveillance, paving the way for smarter, technology-driven security systems in the future.

REFERENCES

1. H.El-Tajetal.,"ThroughtheLens:IPCamera Security&Privacy," 2025.
2. S.Bhardwajetal.,"UnmaskingVulnerabilitiesofSmartIoTCameras," 2024.
3. K.Ngand A.Mehrnezhad, "Security&PrivacyEvaluation ofIPCameras on Shodan,"2024.
4. D.Siwakotietal.,"IoTCamerasExploitedinFinancialCrimes," 2024.
5. G.Bellaetal.,"PETIoT:PenetrationTestingIoT," 2023.
6. Various,"SurveyonIoT &EmbeddedFirmwareSecurity,"2023.
7. VulnerabilityassessmentandpenetrationtestingonIPcamerasbyPietroBiondietal.2022
8. Z.Lingetal.,"IoTSecurity:End-to-EndView&Case Study," 2018.
9. A.Ravula etal.,"FacialRecognition&IoTCamera Vulnerabilities," 2018.
10. A.Costinetal.,"AutomatedDynamicFirmware AnalysisatScale,"2015