مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٤) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (4) 2025

تصميم واختبار نظام فعال لحماية الألواح الشمسية من السرقة باستخدام تقنية IOT

د. صفاء الاحمد*
م. رؤى عمران**

(تاريخ الإيداع ٢٠٢٤/١٢/٢٤ . قُبِل للنشر في ٢٠٢٥/٣/٢٣)

□ ملخّص □

تم في هذا البحث تصميم نظام لحماية الألواح الشمسية من السرقة بالاعتماد على تقنية إنترنت الأشياء (IOT). يتكون النظام المصمم من مكونين رئيسيين، وحدة ESP32-CAM، وهي قلب النظام ووحدة التحكم الأساسية فيه، والحساس المغناطيسي MC-38. اعتمد النظام المصمم على بروتوكول الاتصال M2M (MQTT)، من أجل ربط وحدة التحكم بالإنترنت مع منصة NODE-RED التي تدعم بروتوكول الاتصال MQTT من خلال خادم Adafruit IO، حيث توفر هذه المنصة العديد من المزايا الخاصة بإنترنت الأشياء، مما يمكننا من مراقبة النظام في الوقت الحقيقي، وبمجرد توفر الإنترنت يقوم النظام بإرسال التنبيه على شكل رسالة، بالإضافة إلى صور متتابعة للموقع، إما عبر Gmail أو تطبيق Telegram على الهاتف المحمول.

قمنا باختبار النظام المصمم على الألواح الشمسية الموجودة على سطح كلية الهندسة التقنية، بينت النتائج أن النظام المصمم فعال، كلفته منخفضة (بلغت حوالي 24$) وذو استهلاك منخفض للطاقة 500 mWh، كما حقق حماية جيدة جداً للألواح الشمسية المركبة على سطح الكلية من السرقة لما يتمتع به من سرعة استجابة وأداء عالي حيث يقوم بإصدار عدة أنواع من التنبيهات إنذار صوتي، إرسال ايميل أو رسالة بالإضافة إلى صور متتابعة للموقع على الـ Gmail وتطبيق الـ Telegram في الوقت الحقيقي. وأيضاً حقق بروتوكول MQTT جودة كبيرة وسرعة عالية في إرسال الرسائل حيث أظهر برنامج Wiresharkمن خلال تحليل بيانات الشبكة بالتقاط الـ IP للحزمة المرسلة زمن تأخير ضئيل جداً لوصول الرسائل وهو [msec] 66.559، ويعتبر متوسط التأخير هذا حسب تصنيف Tiphon "جيد جداً"، بالإضافة إلى أن فقدان الحزمة 5% وهي تعتبر قيمة وسط حسب التصنيف نفسه.

الكلمات المفتاحية: حماية من السرقة، IOT، ESP32-CAM، MQTT، NODE-RED، حساس MC-38، Wireshark.

*استاذ مساعد في كلية الهندسة التقنية، جامعة طرطوس، طرطوس-سوريا.
**طالبة دراسات عليا في كلية الهندسة التقنية، جامعة طرطوس، طرطوس-سوريا.

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (٤) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (4) 2025

Design and testing an effective system to protect solar panels from theft using IOT

Dr. Safaa Alahmad*
Eng. Roaa Omran**

(Received 24/12/2024 . Accepted 23/3/2025)

□ ABSTRACT □

In this research, a system was designed to protect solar panels from theft based on Internet of Things (IOT) technology. The designed system consists of two main components, the ESP32-CAM module, which is the heart of the system and its main control unit, and the MC-38 magnetic sensor. The designed system relied on the M2M (MQTT) communication protocol, in order to connect the control unit to the Internet with the NODE-RED platform that supports the MQTT communication protocol through the Adafruit IO server, as this platform provides many advantages related to the Internet of Things, which enables us to monitor the system in real time, and once the Internet is available, the system sends an alert in the form of a message, in addition to sequential images of the site, either via Gmail or the Telegram application on the mobile phone.

We tested the designed system on the solar panels on the roof of the College of Engineering Technology. The results showed that the designed system is effective, economical (its cost was about $24) and has low energy consumption of 500 mWh. It also achieved very good protection for the solar panels installed on the roof of the college from theft due to its high response speed and performance, as it issues several types of alerts, audio alarm, sending an email or message, in addition to sequential images of the site on Gmail and the Telegram application in real time. The MQTT protocol also achieved great quality and high speed in sending messages, as the Wireshark program showed, through analyzing the network data by capturing the IP of the sent packet, a very low delay time for the arrival of messages, which is 66.559 [msec], and this average delay is considered "very good" according to the Tiphon classification, in addition to the packet loss of 5%, which is considered an average value according to the same classification.

key words: Anti-Theft System, IOT, ESP32-CAM, MQTT, NODE-RED, MC-38 Sensor, Wireshark.

* Assistant Professor at Faculty of Technical Engineering, Tartous University, Syria.
**Postgraduate Student, Faculty of Technical Engineering, Tartous University, Syria.

١- مقدمة:

أدى انخفاض موارد الوقود الأحفوري على مستوى العالم إلى السعي العاجل لمصادر طاقة بديلة كمصادر الطاقة المتجددة. وقد كان النصيب الأكبر للطاقة الشمسية، حيث جذبت أنظمة الخلايا الكهروضوئية (PV) اهتماماً متزايداً في السنوات الأخيرة، فقد بلغ عددها في محافظة طرطوس 43 مشروع مربوطة على شبكة التوزيع ومتوزعة في أنحاء المحافظة.

ومع تزايد انتشار المنظومات الكهروضوئية في محيطنا الحالي، تزايدت عمليات السرقة حيث تم الإبلاغ عن كثير من حالات السرقة للألواح الشمسية في مختلف المحافظات السورية، مما سبب خسائر اقتصادية كبيرة وعرض أمن المنظومة للخطر، لذلك لجأ معظم مالكي المنظومات الكهروضوئية إلى العديد من الطرق أو التقنيات المختلفة لحمايتها من السرقة وتحقيق الأمن.

كانت أنظمة الأمان موجودة منذ فترة طويلة جدًا، حتى قبل إدخال وحدات التحكم الدقيقة، إلا أنها تطورت على مر الزمن وقطعت مراحل كثيرة. فقد انتقلت من كونها دوائر تناظرية بسيطة بمفاتيح (Switch) وأجراس ميكانيكية إلى كونها أنظمة رقمية متطورة يمكنها الإبلاغ تلقائيًا عن الإنذارات ومعلومات الحالة إلى مركز المراقبة [1].

أصبحت الطريقة الأفضل للإبلاغ عن الإنذارات مع التطور التكنولوجي هي الطريقة التي تعتمد على استخدام تقنية إنترنت الأشياء (IOT)، التي تقوم بربط الأجهزة مع بعضها البعض من خلال شبكة الإنترنت والـ IP، وتتيح للفرد التحكم بأجهزته عن بعد بالوقت الحقيقي فتوفر الوقت والجهد عند تطبيقها. الأمر الذي دفع الباحثين في الآونة الأخيرة إلى إجراء البحوث والدراسات حول كيفية حماية المنظومات الكهروضوئية من السرقة والاعتداءات بطريقة اقتصادية وفعالة اعتماداً على تقنية إنترنت الأشياء (IOT)، ومن هذه الدراسات:

- **قام الباحث Silvano Bertoldo وآخرين عام ٢٠١٢**، بتصميم شبكة التحسس اللاسلكية WSN التجريبي المخصص ليكون نظام إنذار ضد سرقة الألواح الكهروضوئية، حيث يتم تثبيت كل عقدة في الشبكة مباشرة تحت كل سلسلة PV وهي مجهزة بحساس التسارع القادر على اكتشاف الحد الأدنى من إزاحة اللوحة من موضعها الثابت. أثبت هذا النظام نجاحه في إرسال رسالة وإطلاق الإنذار عند اكتشاف أي دخيل مما قلل من فرص السرقة عن طريق تنبيه الأشخاص القريبين والمصرح لهم بالمعلومات المطلوبة حول وجود الدخيل في الوقت المحدد [2].

- **وفي بحث آخر للباحث Wasif Ali Khan وآخرين عام ٢٠١٧**، تم تطوير نظام لمكافحة سرقة الوحدات الكهروضوئية NODAS حيث تم اقتراح نظام إيقاف تشغيل تلقائي منخفض الطاقة وغير مدمر للوحدات الكهروضوئية(pv)، يتم من خلاله إغلاق وظيفة توليد الطاقة للوحدة الكهروضوئية داخلياً عند السرقة ولا يمكن إعادة تنشيطها بواسطة أفراد غير مصرح لهم. خلصت الدراسة إلى أنه تم اقتراح NODAS على مستوى الوحدة النمطية لحل مشكلة السرقة في الصناعة المتنامية لمحطات الطاقة الشمسية، مما يحقق أمان أكثر وتكلفة منخفضة مقارنة بالأجهزة المستخدمة في السوق باهظة الثمن[3] .

-**كما قام الباحث Reginald Ogu وآخرين عام ٢٠١٩**، بتصميم نظام مضاد للسرقة (STDS) لحماية البنى التحتية لإضاءة الشوارع التي تعمل بالطاقة الشمسية، يساعد النظام المقترح في منع السرقة المستمرة للبطاريات والمكونات الحيوية الأخرى باستخدام حساس PIR ووحدةArduino Uno . تم التوصل إلى أن هذا

النظام حقق هدفه الأساسي حيث أنه بمجرد اكتشاف اللص في النهار يصدر النظام إنذاراً لردع أنشطة السرقة وفي أثناء الليل يتم تنشيط دائرة الإنذار والوميض الضوئي لمنع اللصوص من الوصول إلى البنى التحتية [4].

-**أنشئ الباحث Filantropi Yusuf Aji Cahyono وآخرون عام ٢٠٢٢**، جهاز قادر على زيادة أمان غرفة من خلال استخدام Esp32-Cam وحساسي الحركة PIR، الحريق Ky-026. توصل الباحثون إلى أن حساس الحريق يعمل بشكل جيد بمتوسط قيمة تأخير تبلغ ١,٣٧ ثانية، كما يتم نقل البيانات عبر الإنترنت من خلال استخدام وحدة Esp32 Cam إلى تطبيق التلغرام على الهاتف بمتوسط تأخير هو ٠,٠٥٩٧ ثانية ويعتبر حسب التصنيفات جيد، بينما بالنسبة لاختبار فقدان الحزمة فإن القيمة التي تم الحصول عليها هي ٧,٠% وهي تعتبر أيضاً تصنيف جيد [5].

٢- مشكلة البحث وأهميته:

تكمن مشكلة البحث في أنه:

تشهد العديد من الشركات حول العالم سرقات مستمرة تتسبب بخسائر تفوق الأربعة عشر مليون يورو سنوياً حسب تقديرات المعهد الألماني للطاقة الشمسية، وأيضاً تتعرض بعض المحطات الكهروضوئية في محيطنا الحالي للسرقة (مثل سرقة الألواح الكهروضوئية في محطة السويداء مؤخراً وتبعه سرقة الألواح من مستوصف بلدة بسيرين بريف حماة الجنوبي حسب مصادر جريدة "الوطن"، وسرقة الألواح والبطاريات المستخدمة في إنارة الشوارع في مدينة طرطوس) والذي أدى إلى خسائر اقتصادية كبيرة بسبب فشل عمل المنظومة وتعرض أمنها للخطر، بالإضافة إلى أن أجهزة الحماية المتوفرة في الأسواق باهظة الثمن.

أما أهمية هذا البحث **تكمن** في إيجاد طرق مبتكرة واقتصادية لحل مشكلة سرقة الألواح الشمسية، كما أنها تعمل على زيادة أمن المنظومات الكهروضوئية وبالتالي التقليل من الخسائر الاقتصادية، بالإضافة إلى توطين التكنولوجيا لتصميم وتنفيذ أنظمة الحماية من السرقة.

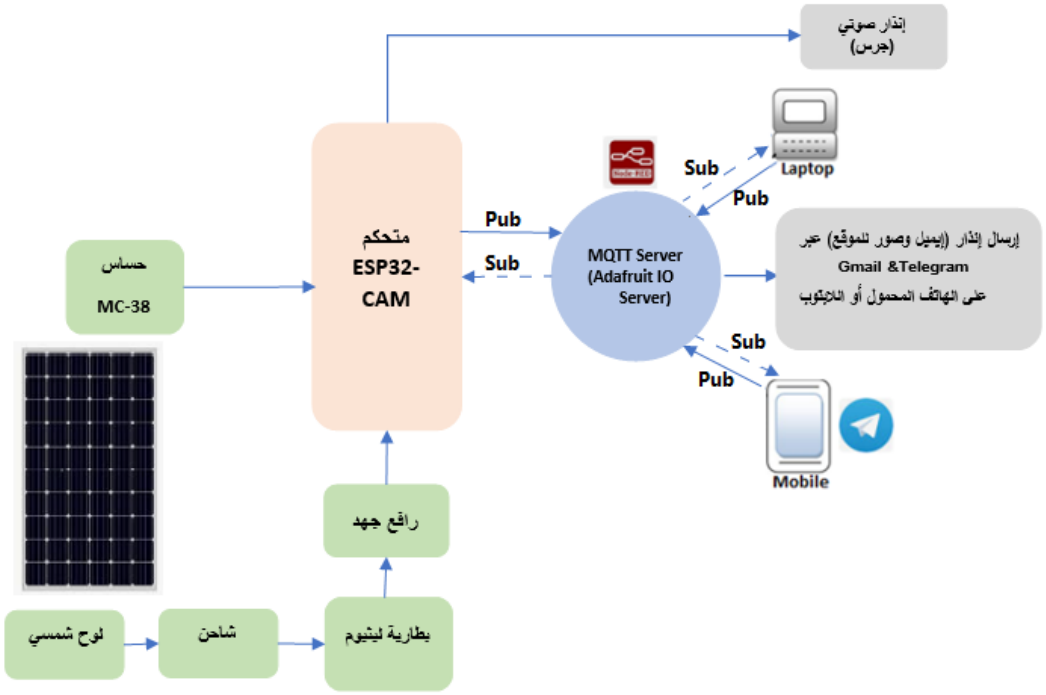
٣- هدف البحث:

يهدف البحث إلى تصميم نظام فعال لحماية الألواح من السرقة يعتمد على تقنية IOT (إنترنت الأشياء) منخفض التكلفة، يحقق استجابة سريعة في حال تعرض المنظومة الكهروضوئية للسرقة.

٤- طرائق البحث ومواده:

٤-١ المخطط الصندوقي لنظام الحماية من السرقة:

يبين الشكل (١) المخطط الصندوقي للنظام المصمم حيث يتألف النظام من ESP32-CAM Modual، والتي تعتبر قلب النظام والعقل الرئيسي له حيث تقرأ البيانات باستمرار من الحساس المغناطيسي MC-38 Sensor وتنقلها عبر بروتوكول MQTT وخادم Adafruit Server إلى منصة الـ Node-Red، التي تقوم بمعالجة البيانات الواردة إليها ومن ثم إرسال الأوامر إلى ESP32-CAM فترسل بدورها الإنذار في حال وجوده (رسالة وصور للموقع) عبر إيميل Gmail أو إلى تطبيق الهاتف المحمول Telegram.



الشكل (١): المخطط الصندوقي لعمل النظام

٤-٢ مكونات النظام المصمم:

٤-٢-١ الحساس المغناطيسي MC-38:

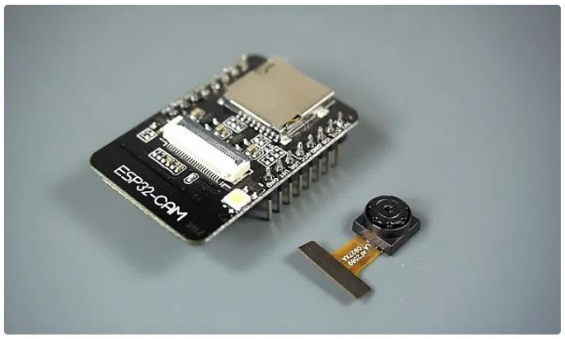
استخدامنا الحساس المغناطيسي MC-38 نظراً لموثوقيته، صغر حجمه، استهلاكه المنخفض للطاقة وأدائه العالي حيث أنه يتفادى حالات الإنذار الكاذبة، وهو عبارة عن حساس إنذار (مفتاح مغناطيسي)، يعمل وفق المبادئ الكهرومغناطيسية، يستخدم عادة للأبواب والنوافذ، يتكون الحساس من جزأين جزء هو المغناطيس الدائم والآخر متحرك، في هذا النوع من الحساسات تكون الدائرة مفتوحة في حالة عدم وجود مغناطيس (Normally open)، وعندما يقترب المغناطيس من الحساس تغلق الدارة (Normally close)، مما يسمح بمرور تيار وتنتج الإشارة.

في بحثنا تم تثبيت جزء على اللوح الأول والجزء الآخر على اللوح الثاني، بهذه الطريقة تمت حماية لوحين معاً، حيث يتم إطلاق الإنذار في حالة توقف تدفق التيار الكهربائي والتي تحدث في حالتين: إما نزع أحد اللوحين من مكانهما حيث يبتعد جزأ ي الحساس المغناطيسي عن بعضهما أو عند قطع سلك الحساس.

الشكل (٢): الحساس المغناطيسي MC-38

٤-٢-٢ متحكم ESP32-CAM:

وهي وحدة تحكم دقيقة مفتوحة المصدر مزودة بوظيفة WIFI متكاملة بالإضافة لـ Bluetooth، أطلقتها شركة Espressif System في الصين بعد شريحة ESP8266 ويتم استخدامها لتطوير تطبيقات أكثر في مجال انترنت الأشياء لكونها أسهل وعملية أكثر، وهي نفسهاESP32 مضاف إليها كاميرا كما يوضح الشكل (٣).



الشكل (٣): لوحة ESP32-CAM

تم اختيارها لرخص ثمنها وعدم الحاجة إلى جهد كبير لتأمين التغذية لها واستهلاكها المنخفض للطاقة الكهربائية، بالإضافة إلى سهولة التعامل معها وصغر حجمها وبساطة لغة البرمجة الخاصة بها، حيث يتم برمجتها عن طريق الحاسوب باستخدام البيئة البرمجية "Arduino IDE" المفتوحة المصدر، وقدرتها على الاتصال عبر تقنية الواي فاي (WI-FI)، بالإضافة إلى عدد المداخل والمخارج الكافية للنظام المصمم واحتوائها على كاميرا، أي أنها اختصرت أكثر من وظيفة في قطعة واحدة مما قلل من تكلفة النظام.

٤-٢-٣ الجرس Buzzer:

الجرس هو جهاز إرسال إشارات صوتية، نطاق التردد هو ٣٣٠٠ هرتز والتيار المغذي هو 15 mAوهو موضح بالشكل (٤).

الشكل (٤): الجرس Buzzer

٤-٢-٤ دارة تغذية النظام بالطاقة الكهربائية:

يتم تزويد دارة النظام المصمم بالتيار المستمر من خلال بطاريات الليثيوم أيون المشحونة بواسطة الألواح الشمسية حيث نحتاج لتغيير جهود التيار المستمر بطريقة سلسة وموفرة للطاقة لذلك تم تزويد النظام بدارة الشحن المبينة بالشكل (٩)، والتي تتكون مما يلي:

- **دارة LM2596:**

تستخدم كدارة تغذية حيث تقوم بتعديل الجهد الخارج عند مستوى معين وتخفيضه عن طريق مقاومة متغيرة موضحة في الشكل (٥)، (هنا نقوم بتخفيض الجهد القادم من اللوح الشمسي 18 V إلى جهد بطارية الليثيوم 3.7 V) ومن أهم مميزاتها انخفاض الاستطاعة المستهلكة وتبديد الحرارة.

الشكل (٥): دارة LM2596

- **دارة XL6009 E1:**

عبارة عن مبدل رافع جهد (BOOST)، تقوم برفع الجهد عند مستوى معين مع تيار تحويل 4 A (حيث تقوم برفع الجهد من جهد بطارية الليثيوم 3.7 V إلى جهد تغذية ESP-32 CAM وهو 5 V)، تستخدم هذه الدارة الجيل الثاني من تقنية التبديل عالي التردد XL6009E1كرقاقة أساسية، بتكلفة أقل وأداء أكثر تميزًا وهي موضحة بالشكل (٦).

الشكل (٦): دارة XL6009 E1

- **منظم جهد لبطارية ليثيوم آيون ٠٣٩٦٢A:**

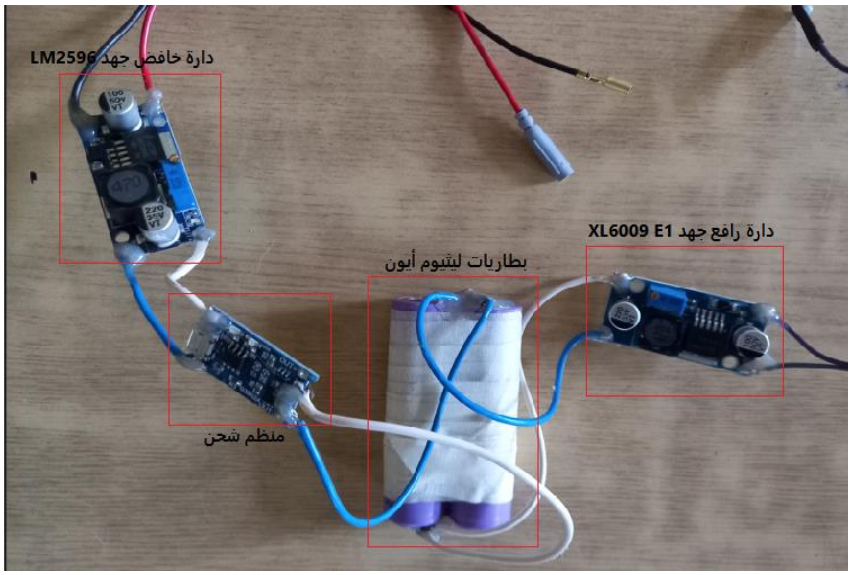
هي دارة تستخدم في الدوائر الإلكترونية كما يوضح الشكل (٧)، لتنظيم الجهد الكهربائي في حالة دارة شحن بطارية ليثيوم أيون حيث يقوم المنظم بتحويل الجهد المدخل إلى جهد ثابت ومناسب لشحن بطارية ليثيوم أيون.

الشكل (٧): منظم جهد ٠٣٩٦٢A

الشكل (٨): بطارية ليثيوم ايون 18650

▪ **بطارية ليثيوم ايون ١٨٦٥٠:**

هي بطارية قابلة لإعادة الشحن بجهد ٣,٧ فولت وسعة 2000 mAh يمكن أن تعطي تياراً يصل حتى 2A بالإضافة إلى حجمها الصغير كما هو موضح بالشكل (٨)، تحتوي هذه البطارية على دائرة حماية مدمجة تمنعها من التفريغ الزائد. أيضا تمتاز بقدرتها على تحمل الشحن، تعد بطارية ليثيوم ايون القابلة لإعادة الشحن هذه خيارًا مثاليًا لتشغيل الأجهزة.



الشكل (٩): دارة الشحن ووصلها مع Esp32-Cam

٤-٢-٥ بروتوكول الاتصال MQTT (Message Queue Telemetry Transport) ومنصة Node-RED:

من أجل تحقيق الاتصال وربط المتحكم مع منصة Node-Red نحتاج إلى بروتوكول محدد يقوم بعملية الربط والاتصال المطلوبة، لذلك استخدمنا بروتوكول MQTT وهو بروتوكول مراسلة قائم على معايير أو مجموعة من القواعد يستخدم للاتصال من آلة إلى أخرى (M2M)، يعتمد على نظام نشر/اشتراك ويستخدم مكدس TCP/IP كأساس للاتصال [6][7]. تتكون بنيه اتصال MQTT من وسيط (MQTT Broker) المركزي وعدد من عملاء MQTT الذين هم أجهزة انترنت الأشياء، يتكون الوسيط من العديد من "صناديق البريد" التي تسمى الموضوعات (Topics) حيث يمكن لكل عميل الاشتراك ونشر الرسائل (Pub-Sub).

في نظامنا المصمم تم استخدام الخادم الوسيط Adafruit server حيث أنه المسؤول في المرتبة الأولى عن تلقّي كل الرسائل، وفرزها، ليقرّر الأجهزة المهتمة بها، ثم ينشرها لجميع العملاء المشتركين بها [10,11].

سبب اختيار هذا البروتوكول لنظامنا كونه مفتوح المصدر، بسيط وسهل التنفيذ، يتطلب نطاق ترددي منخفض والذي يعتبر أمر مفيد في الشبكات اللاسلكية، فضلاً عن استخدامه لمكدس الاتصال البسيط (TCP/IP)

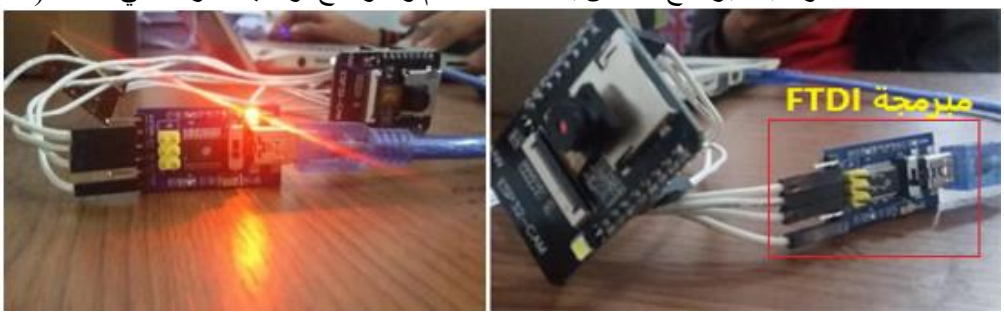
الذي يقلل الأعباء على الشبكة، بالإضافة إلى أنه يتطلب معالجة أقل وبالتالي يكون المعالج أقل تطلباً وهذا يجعله مثالياً للتطبيقات التي يتم فيها استخدام أجهزة ذات طاقة معالجة منخفضة مما يؤدي إلى استهلاك أقل للطاقة، وهذا ضروري للأجهزة التي تعمل طوال الوقت وخاصة تلك التي تعمل بالبطاريات [7,8].

كما تم استخدام منصة Node-RED والتي تُعدّ بيئة افتراضية (منصة للوصل) بين الأجهزة المادية وواجهات برمجة التطبيقات APIs وخدمات Online بطرق جديدة ومثيرة للاهتمام، كما أنها مفتوحة المصدر، وهي أداة برمجة تعتمد على مفهوم البرمجة القائمة على التدفق حيث تُوفّر تدفُّقٍ قائماً على متصفّح ومما يسهّل هذا التدفُّق استخدام عُقَد واسعة النطاق في لوحة Node-Red وهي تدعم بروتوكول MQTT المستخدم وتعتمد على بيئة تشغيل Node.js الخفيفة الوزن [9].

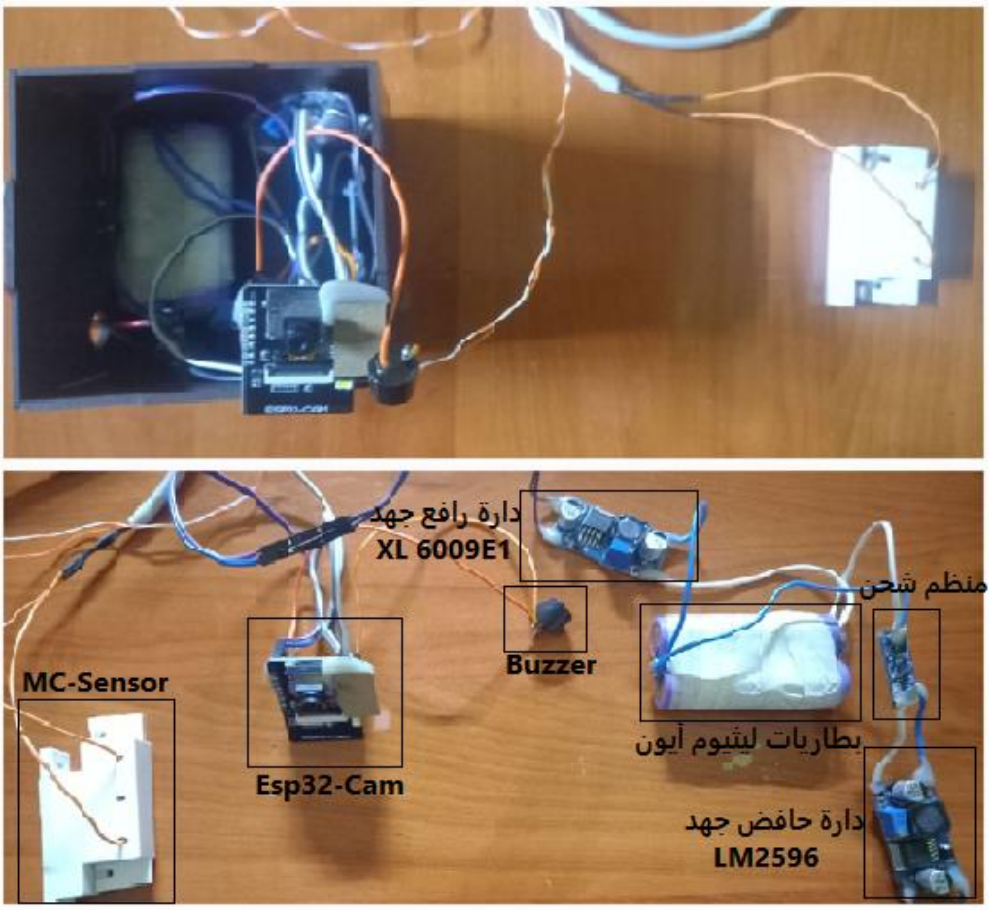
٤-٣ الجزء البرمجي للنظام:

٤-٣-١ برمجة لوحة ESP32-CAM:

تم برمجة لوحة ESP32-CAM بمبرمجة خاصة FTDI المبينة في الشكل (١٠) باستخدام البيئة البرمجية Arduino IDE وكتابة البرنامج الخاص بنظامنا المصمم والموضح توصيل مكوناته في الشكل (١١).



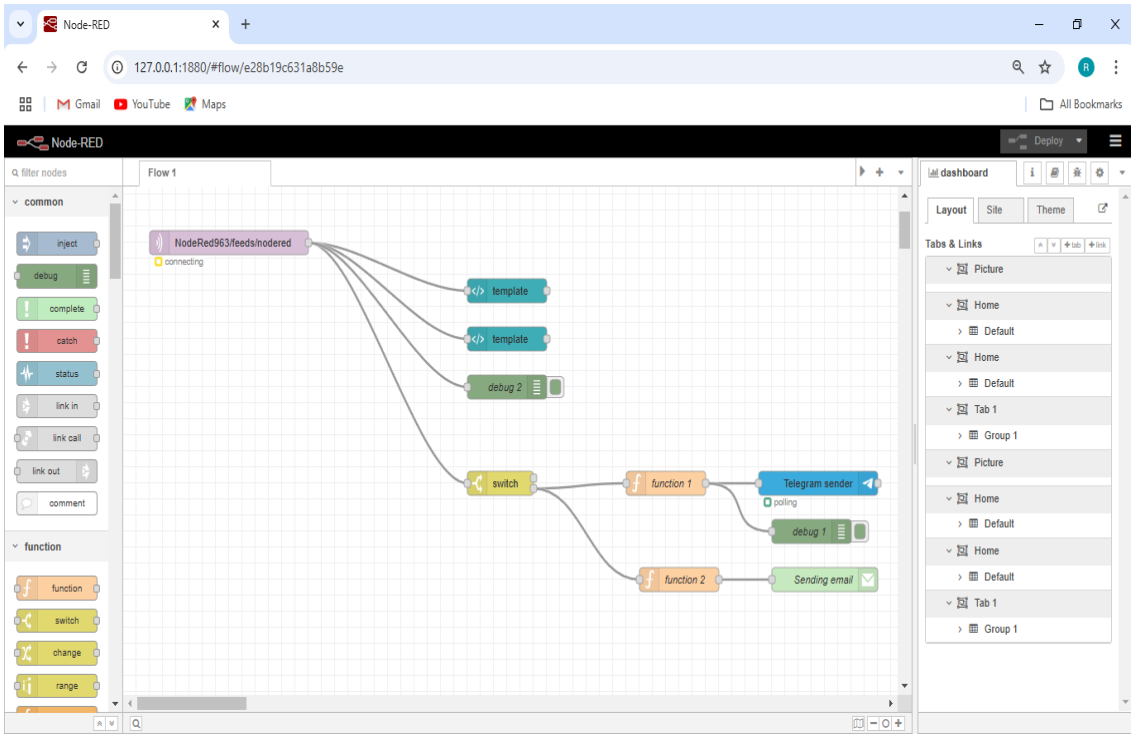
الشكل (١٠): برمجة ESP32-CAM عن طريق مبرمجة FTDI



الشكل (١١): توصيل مكونات النظام وبرمجته

٤-٣-٢ تصميم واجهة Node-Red الخاصة بنظامنا:

تم تصميم واجهة الـ Node-Red الخاصة بنظامنا من خلال تنسيق وترتيب لوحة المعلومات والتحكم في واجهة المنصة. وبعدها قمنا بإنشاء سلسلة التعليمات البرمجية وذلك من خلال اختيار العقد المناسبة للنظام مثل (Mqtt in، Template, Switch, Function, Sending Email, Telegram Sender) والربط بينها كما يوضح الشكل (١٢)، ولأجل الربط بين المتحكم والمنصة أدخلنا المعلومات البرمجية مثل الـ IP و Base64 الخاص بالصورة و Chat Id لإرسال الرسائل على التلغرام وغيرها من المعلومات التي يجب أن تكون متوافقة بين المتحكم والمنصة لإرسال الصورة والتنبيه في حال وجوده، ومن ثم إجراء تدفق بينها لمعالجة البيانات واتخاذ الإجراء المناسب.



الشكل (١٢): واجهة Node-Red البرمجية لنظامنا المصمم

٤-٣-٣ إنشاء بوت (Bot) على Telegram:

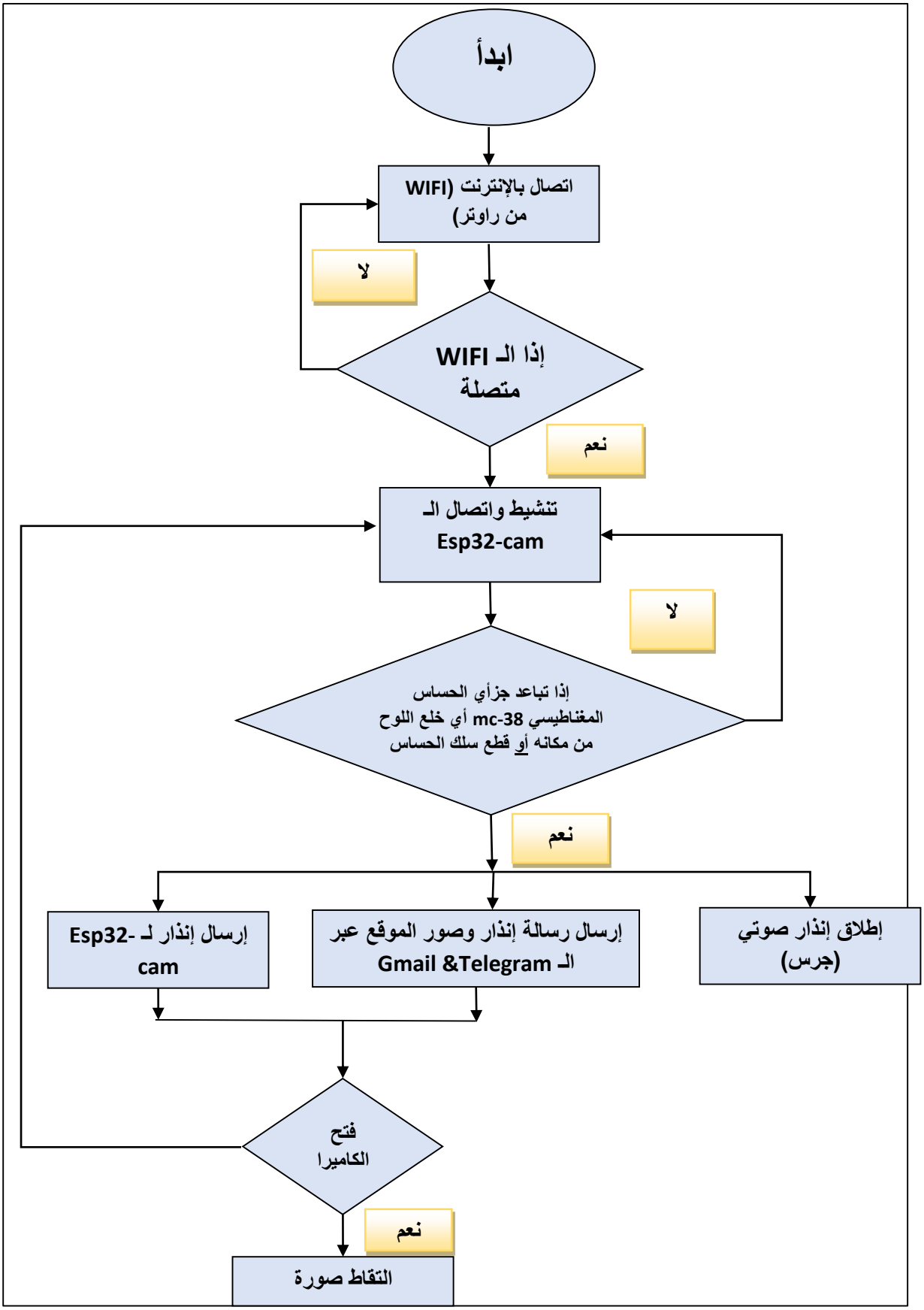
تم إنشاء بوت جديد على التلغرام باستخدام خدمة BotFather كما في الشكل (١٣)، وتحديد رمز الـ Bot وChat ID (معرف الدردشة) من أجل الربط مع عقدة تلغرام التي تم اختيارها سابقا في واجهة Node-Red.

تم إنشاء Bot لتلغرام الخاص بنظام الحماية من السرقة وتسميته Esp-Cam، نتلقى عليه رسالة الإنذار ورابط للصور الملتقطة للسارق وموقع الألواح. وفيه رمز معرف الدردشة ChatID: 797666345.

الشكل (١٣): إنشاء بوت (Bot) تلغرام

٤-4 خوارزمية عمل النظام:

يبين الشكل (١٤) خوارزمية نظام حماية الألواح الشمسية من السرقة المنفذ، التي تتيح الفهم السريع لعمل النظام والتعديل عليه حسب الحاجة. حيث يقوم النظام بداية بالتحقق من الاتصال بشبكة الإنترنت، فإذا كان النظام غير متصل بالإنترنت يقوم بتكرار العملية حتى تتم عملية الاتصال، بعد التأكد من توفر الإنترنت يتم الاتصال بين ESP32-Cam والشبكة وتنشيط عملها، ففي حال نزع اللوح من مكانه أي ابتعاد جزأي الحساس المغناطيسي عن بعضهما أو عند قطع سلك الحساس، تقوم الـ Esp32 وعبر منصة الـ Node-Red بإطلاق عدة أنواع من التنبيهات كإصدار إنذار صوتي(جرس)، وإرسال رسائل متتابعة على Gmail&Telegram على الهاتف المحمول أو الحاسوب مضمونها أن "اللوح الشمسي يسرق "وصور متتابعة للموقع يتم التقاطها من خلال كاميرا الـ Esp32.



الشكل (١٤): خوارزمية عمل نظام الحماية

٥- اختبار النظام ومناقشة النتائج:

٥-١ اختبار الحساس المغناطيسي MC-38:

✓ تم اختبار الحساس المغناطيسي لمعرفة مسافة التحسس التي يمكن أن يتحسسها، حيث يبين الشكل (١٥) طريقة تركيب الحساس على الألواح الموجودة على سطح كلية الهندسة التقنية. وبالاختبار توصلنا إلى النتائج الموضحة في الجدول (١).

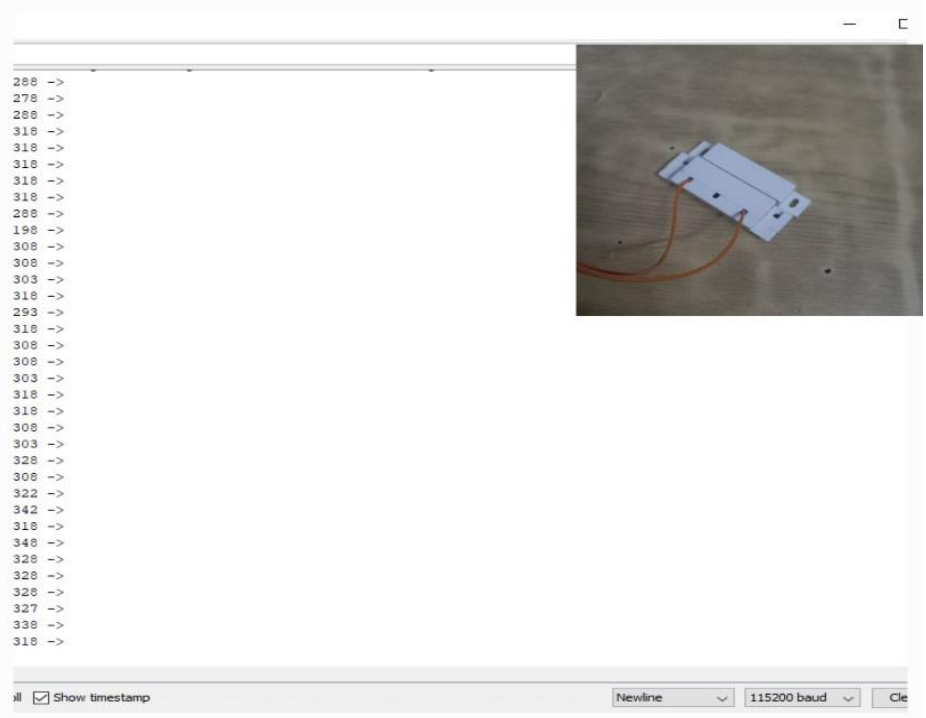
الشكل (١٥): توضع الحساس MC-38 على اللوح الشمسي الموجود على سطح كلية الهندسة التقنية

الجدول (١) يوضح حالات عمل الحساس

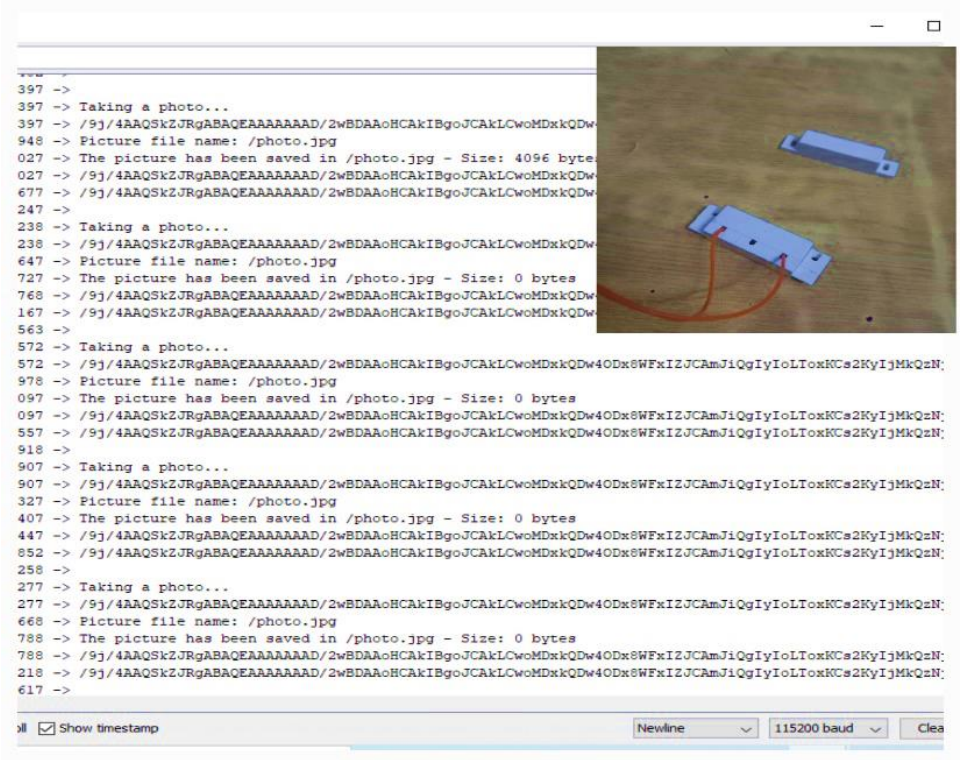
المسافة	MC-38 Sensor	ESP32-CAM
1 cm	Normally Close	لا يتم التقاط صور وإرسال رسالة
1.5 cm	Normally Close	لا يتم التقاط صور وإرسال رسالة
2 cm	Normally Close	لا يتم التقاط صور وإرسال رسالة
2.5 cm	Normally Close	لا يتم التقاط صور وإرسال رسالة
3 cm	Normally Close	لا يتم التقاط صور وإرسال رسالة
3.5 cm	Normally Open	يتم التقاط صور وإرسال رسالة
4 cm	Normally Open	يتم التقاط صور وإرسال رسالة
5 cm	Normally Open	يتم التقاط صور وإرسال رسالة

يبين الجدول نتائج اختبار الحساس المغناطيسي MC-38 لوحظ وجود وضعين للعمل:

- الوضع الأول (Normally Close) عندما يكون الجزأين المكون منهما الحساس معا أو على مسافة أقل من 3 cm فإن الحساس يوفر دخل منخفض لوحدة التحكم كما في الشكل (١٦) وبالتالي لا يحدث إنذار.
- الوضع الثاني (Normally Open) عندما يكون الجزأين المكون منهما الحساس بعيدين عن بعضهما أو على مسافة أكبر من 3 cm فإن الحساس يوفر دخل مرتفع لوحدة التحكم كما في الشكل (١٧) وبالتالي يحدث الإنذار.



الشكل (١٦): وضع الحساسNormally Close

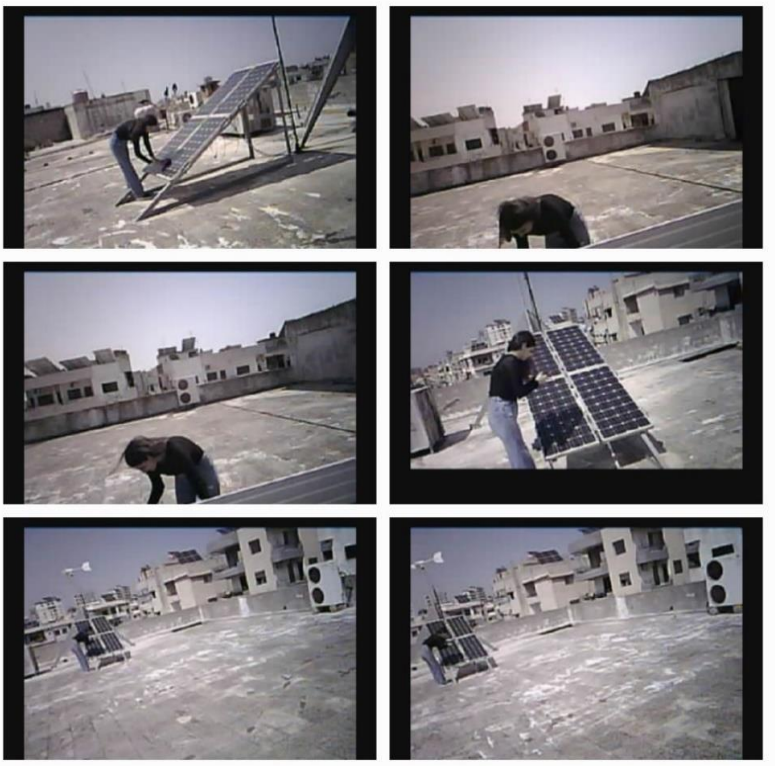


الشكل (١٧): وضع الحساس Normally Open

✓ كما تم اختبار مدى تأثير طول سلك الحساس على استجابته فوجدنا أن الحساس قام بوظيفته حتى طول سلك حوالي ٤ أمتار، وأدى وظيفته بنجاح.

٥-2 اختبار كاميرا الـ Esp32-Cam:

تم اختبار مدى وضوح الصورة التي تلتقطها كاميرا الـ ESP32 على أبعاد مختلفة، النتائج موضحة بالشكل (١٨) و (١٩) حيث تم تلقي رسالة على إيميل الـ Gmailوعلى تطبيق التلغرام Telegram على الهاتف المحمول بأن "اللوح يسرق" ورابط صور متتابعة لموقع الألواح مع إطلاق إنذار صوتي في الموقع عند تحرك اللوح من مكانه.

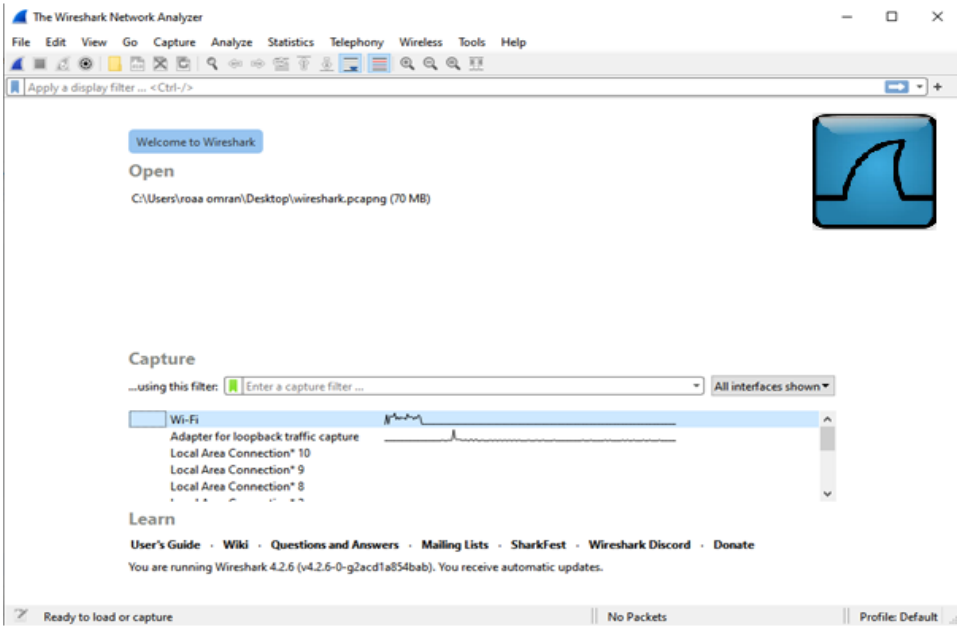


الشكل (١٨): الصور الملتقطة من esp32-cam عند الإنذار عن حالة السرقة

الشكل (١٩): رسائل البريد الإلكتروني والتلغرام للإنذار بوجود سرقة للألواح

٥-٣ اختبار جودة النظام:

لاختبار جودة النظام المصمم قمنا بقياس التأخير الزمني وزمن فقدان الحزمة باستخدام برنامج Wireshark، وهو برنامج مفتوح المصدر للتنصت على الشبكة وتحليل الحزم، يستخدم لاكتشاف الأخطاء في الشبكة، وتحليل الشبكات وكذلك للأغراض التعليمية. يعرض محلل حزم الشبكة Wireshark بيانات الحزمة الملتقطة بأكبر قدر ممكن من التفاصيل، ويعتبر الـ Wireshark من أفضل برامج تحليل الحزم(البروتوكولات) في شبكة الإنترنت ويبين الشكل (٢٠) واجهة برنامج الـ Wireshark.

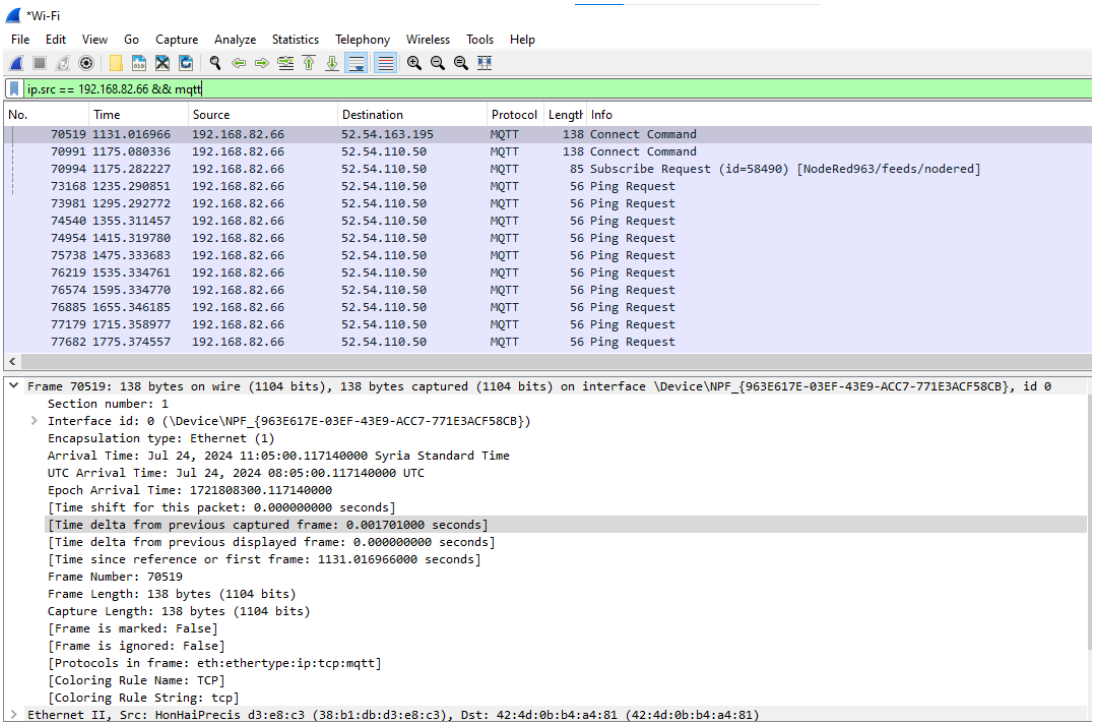


الشكل (٢٠): واجهة برنامج Wireshark

٥-٣-١ قياس التأخير على برنامج Wireshark:

يمكن استخدام واير شارك لفحص تفاصيل حركة المرور على مستويات متنوعة تتراوح من المعلومات على مستوى الاتصال إلى البتات التي تشكل حزمة واحدة، يمكن أن يوفر التقاط الحزمة لمسؤول الشبكة معلومات حول الحزم الفردية مثل وقت الإرسال والمصدر والوجهة ونوع البروتوكول وبيانات الرأس. وتكون هذه المعلومات مفيدة لتقييم أحداث الأمان واستكشاف مشكلات جهاز أمان الشبكة وإصلاحها ويمكن التقاط كلمات المرور وكل شيء يمر داخل الشبكة الخاصة بك.

يكون البرنامج قادرًا على معالجة البيانات الخاصة بالاتصالات التي تم إنشاؤها من هذا النظام، من خلال النظر إلى عنوان IP الخاص بالوجهة المستخدمة. ولأجل حساب التأخير الزمني لنظامنا المصمم اعتمدنا على الـ IP الخاص بالحزمة الملتقطة وقت إرسال التنبيه وهو ١٩٢,١٦٨,٨٢,٦٦ فحصلنا على البيانات الموضحة في الشكل (٢١).



الشكل (٢١): تحليل حزمة البيانات على برنامج Wireshark

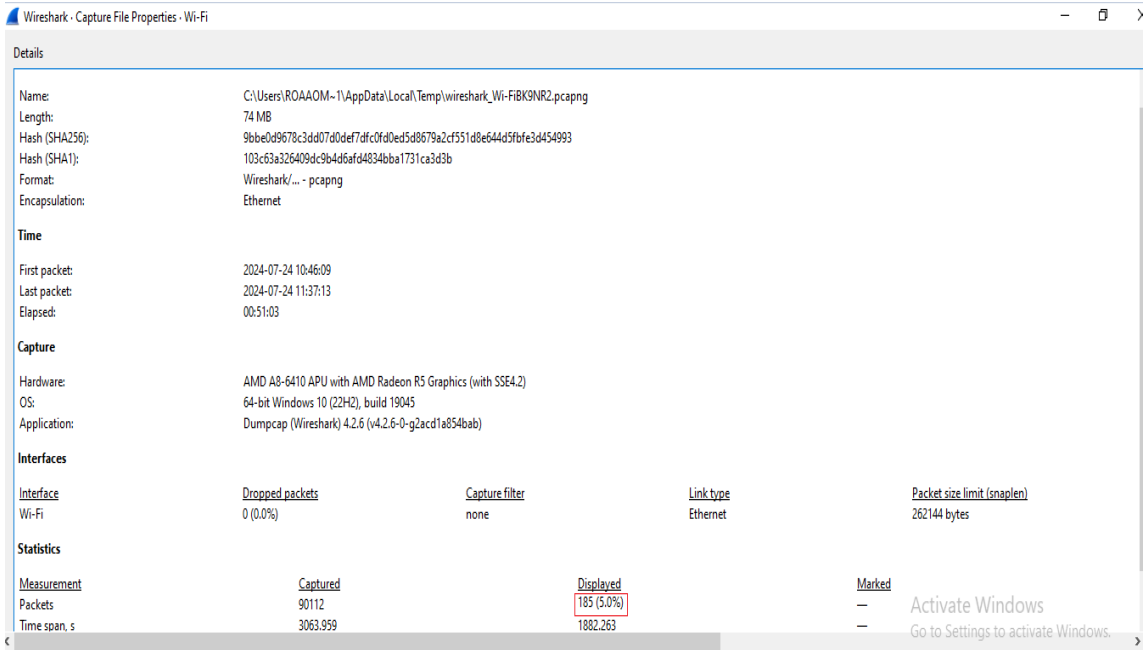
الجدول (٢) بيانات حزمة الإرسال

Source	Destination	Protocol	Length	Time
192.168.82.66	52.54.163.195	MQTT	138	0.001701
192.168.82.66	52.54.110.50	MQTT	138	0.000837
192.168.82.66	52.54.110.50	MQTT	85	0.011252
192.168.82.66	52.54.110.50	MQTT	56	0.455074
192.168.82.66	52.54.110.50	MQTT	56	0.032402
192.168.82.66	52.54.110.50	MQTT	56	0.157504
192.168.82.66	52.54.110.50	MQTT	56	0.598317
192.168.82.66	52.54.110.50	MQTT	56	0.03228
192.168.82.66	52.54.110.50	MQTT	56	0.016776
192.168.82.66	52.54.110.50	MQTT	56	0.204216
192.168.82.66	52.54.110.50	MQTT	56	0.431847
192.168.82.66	52.54.110.50	MQTT	56	0.094681
192.168.82.66	52.54.110.50	MQTT	56	0.187973
192.168.82.66	52.54.110.50	MQTT	56	0.006427
192.168.82.66	52.54.110.50	MQTT	56	0.055651
192.168.82.66	52.54.163.195	MQTT	138	0.000686
Average				٠,٠٦٦٥٥٩ seconds

يبين الجدول (٢) التأخير الزمني لنظامنا وقدره66.559 mS . بناءً على تصنيف التأخير الحالي، يمكن استنتاج أن متوسط التأخير هو مؤشر "جيد جداً" وذلك حسب تصنيف TIPHON (Telecommunications and Internet Protocol Harmonization over Network) [12,13].

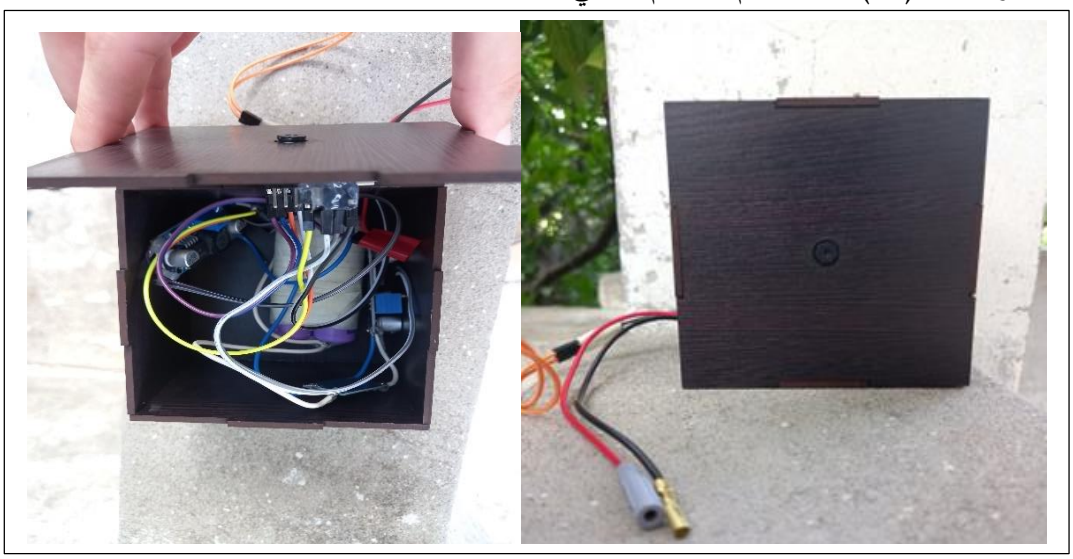
٥-٣-٢ اختبار فقدان الحزمة على برنامج Wireshark:

فقدان الحزمة هو عدد الحزم المفقودة على الشبكة والتي لا تصل إلى الوجهة وتنجم عن الاصطدامات وسعة الشبكة الكاملة وانقطاعات الحزم الناجمة عن نهاية الحزم TTL (Time to Live)، وعند اختبارنا لفقدان الحزمة لنظامنا المصمم باستخدام برنامج Wireshark واعتماداً على (الـ ip الخاص بالحزمة الملتقطة وعدد الحزم الملتقط وغير الملتقط المبين في الشكل (٢٢))، حصلنا على فقدان حزمة ٥,٠% كما هو مبين في الشكل (٢٢) [12,13].



الشكل (٢٢): اختبار فقدان الحزمة على برنامج Wireshark

يظهر الشكل (٢٣) شكل النظام المصمم النهائي:



الشكل (٢٣): الشكل النهائي لصندوق نظام الحماية وحجمه

٦-الاستنتاجات والتوصيات:

الاستنتاجات:

- جودة النظام من حيث تفادي حالات الإنذار الخاطئة وأدائه وظيفته بنجاح بشكل متكرر، حيث بلغ متوسط التأخير الزمني [msec] 66.559 وهو يعتبر "جيد جداً" حسب تصنيف Tiphon، بالإضافة إلى أن فقدان الحزمة 5% وهو يعتبر وسط حسب تصنيف Tiphon أيضاً.
- مكّنت منصة Node-Red من توفير واجهة مرئية لعرض ومراقبة الموقع في الزمن الحقيقي (من أي كمبيوتر أو هاتف محمول)، كما أن استخدام بروتوكول MQTT حقق سرعة كبيرة في نقل الرسائل بين العملاء Client.
- يمتاز نظام الحماية المصمم باستهلاكه المنخفض للطاقةmWh 500، وبتكلفته المنخفضة نظراً لأن مكوناته من متحكمات وحساسات وغيرها رخيصة الثمن ومتوفرة في السوق المحلية وتؤدي الوظيفة المطلوبة بسرعة وكفاءة عالية حيث بلغت 24$ وهي تكلفة منخفضة جداً مقارنة بالأجهزة المتوفرة في الأسواق.

التوصيات:

من أجل الأعمال المستقبلية، نوصي بما يلي:

- استخدام تقنية معالجة الصورة واستخدامها للتعرف على وجوه العمال أو الحراس أو الأشخاص المخول لهم بالدخول إلى محطات الطاقة الشمسية.
- دراسة إمكانية تزويد اللوح بتقنية GPS لتحديد موقع اللوح بعد السرقة واستعادته.
- استخدام متحكم الراسبيري ومقارنة النتائج مع تلك التي حصلنا عليها.

المراجع References:

[1] Mohammed,Nora.(2017). Design Control System to Protect The Solar Cell from Theft. Al Neelain University.

[2] Bertoldo, S., Rorato, O., Lucianaz, C., & Allegretti, M. (2012). A Wireless Sensor Network Ad-Hoc Designed as Anti-Theft Alarm System for Photovoltaic Panels, Wireless Sensor Network, 4, 107-112. Scientific Research.

[3] Khan, W. A., Lim, B. H., Lai, A. C., & Chong, K. K. (2017, April). A novel anti-theft security system for photovoltaic modules. In AIP Conference Proceedings (Vol. 1828, No. 1). AIP Publishing.

[4] Ogu, R. E., Agwu, D. D., & Ezenugu, I. A. (2019). Anti-Theft System for the Protection of Solar Street Lighting Infrastructure. In 2nd International Engineering Conference (pp. 254-261).

[5] Cahyono, F. Y. A., Suharto, N., & Mustafa, L. D. (2022). Design and build a home security system based on an esp32 cam microcontroller with telegram notification. Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi), 12(2), 58-64.

[6] Soni, D., & Makwana, A. (2017, April). A survey on mqtt: a protocol of internet of things (iot). In International conference on telecommunication, power analysis and computing techniques (ICTPACT-2017) (Vol. 20, pp. 173-177).

[7] Nalin, G. (2014). Orchestration of smart objects with MQTT for the Internet of Things.

[8] Singh, M., Rajan, M. A., Shivraj, V. L., & Balamuralidhar, P. (2015, April). Secure mqtt for internet of things (iot). In 2015 fifth international conference on communication systems and network technologies (pp. 746-751). IEEE.

[9] Hagino, T. (2021). Practical Node-RED Programming: Learn powerful visual programming techniques and best practices for the web and IoT. Packt Publishing Ltd.

[10] Aimaschana Niruntasukrat, Chavee Issariyapat, Panita Pongpaibool, Koonlachat Meesublak, Pramrudee Aiumsupucgul, Anun Panya, Authorization Mechanism for MQTT-based Internet of Things, IEEE ICC2016-Workshops: W07-Workshop on Convergent Internet of Things.

[11] Satyavrat Wagle,Semantic Data Extraction over MQTT for IoTcentric Wireless Sensor Networks, 2016 International Conference on Internet of Things and Applications (IOTA) Maharashtra Institute of Technology, Pune, India 22 Jan - 24 Jan, 2016.

[12] Nurhaida, I., Pratama, D. W. P., Zen, R. A., & Wei, H. (2020). Interior Gateway Protocol Routing Performance Comparison Of The Virtual Private Network Based On MultiProtocol Label Switching And Direct-Link Backupsed On Mpls And Direct-Link Backup. Sinergi,24(1), 1-10.

[13] Fatimah, A. W., Kurniawan, M. T., & Hediyanto, U. Y. K. S. (2020). Network Traffic Data Center Based on TIA-942 Standard: A Case Study in Bogor Government Office. Journal of Advances in Computer Networks, 8(1).