**MapSec: A unified platform to monitor your IoT devices**

Mohd Anas, Anuran Roy, and Aman Sharma

mohd.anas2020@vitstudent.ac.in, anuran.roy2020@vitstudent.ac.in, aman.sharma2020b@vitstudent.ac.in

20BCT0350, 20BT0343, 20BCT0267

VIT –Vellore Institute of Technology

**Abstract**

IoT, by nature, is insecure- IoT devices are dependent on external resources for data-intensive operations. This opens up a huge potential attack surface for real-time IoT devices, which can be seen from the numerous leaks in recent times. Imagine opening your smart watch with fingerprint, just before you go out for a stroll. The sun's shining bright, and a cool breeze is blowing. Sounds just like the weather you want to take a walk under, right? After half an hour, your bank messages you. "There has been a withdrawal of $100k from your bank account numbered XXXXXXXXX" You're stumped. You never went to the bank. Who was it? Someone impersonated you using your fingerprint by intercepting your fingerprint lock traffic and card details, and withdrew all your life savings. That's how easy it is - just one bad day. This is more than enough to show how critical security is for IoT-based devices, especially the ones that are always connected to you - ingesting sensitive personal data 24x7, and processing it in real-time for insights (think smart watches).

**Keywords**

Internet of Things, Port Scanning, Wireless Sensor Network, Cyber attacks

1. **Introduction**

MapSec serves as an indispensable solution for fortifying your IoT ecosystem against lurking vulnerabilities, ensuring that you are never caught off guard by unforeseen threats. These vulnerabilities encompass a spectrum of potential risks, and while the following points shed light on the core aspects, they merely scratch the surface of MapSec's multifaceted capabilities.

In Exposed Credentials, in IoT landscape, it's disconcerting how frequently default login credentials are left unchanged, making them a prime target for malicious actors [6]. MapSec steps in as your vigilant guardian, meticulously identifying default credentials within the devices populating your network. More than just detection, it provides you with comprehensive guidance on altering these credentials swiftly. By pre-emptively addressing this common issue, MapSec ensures that attackers are kept at bay, shielding your IoT infrastructure from potential breaches.

In Exposed Ports, IoT devices maintain constant connectivity with cloud resources, typically through real-time or near-real-time Pub-Sub models [7]. As a result, certain ports must remain exposed to facilitate seamless communication. However, this very exposure opens the door to exploitation by legitimate applications and, more worryingly, malicious entities. MapSec takes on the responsibility of scrutinizing these exposed ports with unwavering vigilance. Its advanced scanning capabilities meticulously monitor for any signs of malicious activity. In the event of a threat, MapSec promptly notifies you, empowering you to take immediate action to secure your network.

In Open-Source Intelligence (OSINT), Even if you've taken every precaution to secure your credentials, there's an inherent risk that they may have been compromised and leaked on the internet [8]. MapSec extends its protective umbrella by actively scouring various Open-Source Intelligence (OSINT) services. This exhaustive search aims to verify whether your credentials have surfaced in any data breaches or leaked online. By staying attuned to these external threats, MapSec ensures that you are not blindsided by credential compromises.

What sets MapSec apart is its user-centric approach, making network security accessible and hassle-free. Gone are the days of laboriously setting up audit schedules via complex command-line operations. With MapSec, safeguarding your IoT ecosystem is as easy as a single click. This streamlined process not only saves you precious productivity hours but also ensures that security log analysis, which can be a time-consuming chore, becomes a thing of the past. MapSec diligently extracts and processes these logs, distilling them into actionable insights that are readily available at your fingertips.

Furthermore, MapSec recognizes the value of convenience and accessibility in today's fast-paced world. Its user-friendly interface guarantees that you can access scan logs and their insights swiftly, from anywhere and at any time. In essence, MapSec emerges as your trusted ally in navigating the intricate landscape of IoT security. It simplifies the arduous task of safeguarding your network while providing you with peace of mind that your IoT ecosystem remains resilient against the ever-evolving realm of threats.

1. **Literature Review**

***2.1. Artorias: IoT Security Testing Framework***

To raise the standard of security, companies need more ways to automate testing of the most commonly found issues with IoT devices against their products. The creation of an automated security testing framework, such as Artorias, allows companies to automate the process of finding easy to identify problems, saving time for more advanced and manual processes of security and functional testing on a product. To show the framework's stability and reliability, things such as proper coding standards should be adhered to, proper management of the project should be present, and unit-tests or code coverage of the framework should be created and maintained. This ongoing project bridges together the principles of security and proper planning and development of a larger programming effort.

IoT Security Testing Framework Artorias, and present an extensible framework that interested research community members can extend for more coverage on privacy and security issues of IoT devices [1].

***2.2. Automated IoT security testing with SecLab***

IoT security breaches are a dangerous reality. Cost pressure and complexity of security tests for embedded systems and networked infrastructure are often the excuse for skipping them completely. SecLab is security test lab to overcome that problem. Based on a flexible and lightweight architecture, SecLab allows developers and IoT security specialists to harden their systems with a low entry hurdle.

The open architecture supports the reuse of current external security test libraries and scalability for the assessment of complex IoT Systems. A reference implementation of security tests in a realistic IoT application scenario proves the approach [2].

***2.3. Design and implementation of automated IoT security testbed[3]***

The arrival of technology connected with the Internet of Things (IoT) is reshaping our lives, while simultaneously raising many issues due to their low level of security, which attackers can exploit for malicious purposes. This research paper conducts a comprehensive analysis of previous studies on IoT device security with a focus on the various tools used to test IoT devices and the vulnerabilities that were found [3].

Additionally, IoT based security testbeds in the research literature. Here introduce an open-source platform for identifying weaknesses in IoT networks and communications. The platform is easily modifiable and extendible to enable the addition of new security assessment tests and functionalities. It automates security evaluation, allowing for testing without human intervention. The testbed reports the security problems of the tested devices and can detect all attacks made against the devices. It is also designed to monitor communications within the testbed and with connected devices, enabling the system to abort if malicious activity is detected. To demonstrate the capabilities of the proposed IoT security testbed, it is used to examine the vulnerabilities of two IoT devices: a wireless camera and a smart bulb[3].

***2.4. A Secure Platform for IoT Devices based on ARM Platform Security Architecture***

Recent IoT services are being used in various fields such as smart homes, smart factories, smart cars and industrial systems. These various IoT services are implemented through hyper-connected IoT devices, and accordingly, security requirements of these devices are being highlighted. In order to satisfy the security requirements of IoT devices, various studies have been conducted such as HSM, Security SoC, and TrustZone. In particular, ARM proposed Platform Security Architecture (PSA), which is a security architecture that provide execution isolation to safely manage and protect the computing resources of low- end IoT devices. PSA can ensure confidentiality and integrity of IoT devices based on its structural features, but conversely, it has the problem of increasing development difficulty in using the security functions of PSA [4]. To solve this problem, this paper analyses the security requirements of an IoT platform and proposes secure platform based on PSA. To evaluate the proposed secure platform, a PoC implementation is provided based on hardware prototype consisting of FPGA. Our experiments with the PoC implementation verify that the proposed secure platform offers not only high security but also convenience of application development for IoT devices [4].

***2.5. IoT Testing-as-a-Service: A New Dimension of Automation***

Internet of Things (IoT) systems has become a global trend enhancing the capabilities smart computing era involving a variety of distributed end-devices and multi- scalable applications. The collaborative nature of IoT systems connected through the Internet increases the heterogeneity of coming data streams that need to be processed for correct decision making in a real-time environment. The processing of huge data streams for remotely distributed IoT systems create loops for data breaches and open new challenges for security and scalability of system testing. Thus, the testing of IoT systems is becoming the necessity, requires automated testing framework due to the amount of IoT devices and processing of data events is prone to error by traditional software testing. An automated IoT testing service-based framework is purposed in this paper, to test the distributed IoT systems by reducing cost and scalability issues of software testing. The infrastructure of IoT systems demands a large number of platforms be developed which requires systematic testing approach. Therefore, the purposed automated IoT testing as a service model performs distributed interoperability testing, oneM2M based conformance testing, security testing of distributed systems and validating semantics/syntactic testing of IoT devices in a systematic approach. Lastly, to provide more strength to the work we discussed and analyse existing IoT testing models to evaluate our proposed model [5].

**2.6. IoT network monitor**

The IoT Organization Screen is an easy-to-use device intended to help people distinguish and address weaknesses in their home IoT gadgets. It works on a Raspberry Pi designed as a switch and utilizes three vital strategies to investigate associated gadgets. In the first place, it distinguishes gadgets with default passwords that might have been compromised in past assaults, like the Mirai Botnet. To upgrade security, it consequently changes these default passwords to arbitrarily created 12-character strings and educates the client regarding the refreshed qualifications. Also, the IoT Organization Screen performs profound parcel investigation on the organization information of each associated gadget. It makes clients aware of possible dangers by distinguishing occurrences where delicate individual data is sent without encryption. This assists clients with going to proactive lengths to get their information.

Ultimately, the instrument is prepared to distinguish botnet traffic beginning from an IoT gadget on the organization. In the event that a gadget is compromised, the client is advised and encouraged to detach the impacted gadget, forestalling further security breaks. The general objective of the IoT Organization Screen is to engage mortgage holders to proactively deal with the security of their home organizations. By giving clear bits of knowledge into possible weaknesses and offering significant stages, this easy-to-use device intends to improve the general security of buyer IoT organizations. The engineers guess that inescapable reception of this instrument will add to a safer climate for home IoT gadgets [9].

**2.7. Securing the Internet of Things**

The coming of the Web of Things (IoT) has presented a plenty of new innovations into both private and business settings, coordinating them into IP networks that were initially not intended to help such a different exhibit of gadgets enough. Already, networks essentially obliged PCs and printers; however, today they have a collection of gadgets like instalment frameworks, Wi-Fi and versatile/wearable gadgets, VoIP telephones, candy machines, sensors, alert frameworks, servers, surveillance cameras, indoor regulators, entryway locks, and different structure controls. This section digs into the assessment of current accepted procedures for getting PC organizations, stressing the difficulties presented by IoT reconciliation. It examines remarkable episodes in IoT security, featuring chosen major digital assaults as verifications of idea. Moreover, the section frames a structure intended to direct the protected sending of IoT gadgets in both venture and home conditions. By tending to these viewpoints, the point is to give bits of knowledge into the special security contemplations and potential weaknesses related with IoT, offering useful direction for moderating dangers and guaranteeing a safer organization of IoT gadgets [10].

**2.8. Systematically Evaluating Security and Privacy for Consumer IoT Devices**

Web of-Things (IoT) gadgets, like brilliant bulbs, cameras, and wellbeing screens, are acquiring far and wide reception among shoppers, with projections showing an ascent into the billions. In spite of their prevalence, these gadgets are helpless to assaults and can be taken advantage of for a huge scope and with expanding recurrence. This examination means to lay out a deliberate methodology for distinguishing security and protection weaknesses in different IoT gadgets, planning to caution buyers, producers, and controllers to expected gambles. The paper orders dangers into four aspects: secrecy of private information traded by the IoT gadget, trustworthiness of information communicated from the IoT gadget to inside or outer elements, access control instruments of the IoT gadget, and intelligent assaults that an IoT gadget could send off. To assess these aspects, the analysts foster scripts that robotize security testing. Twenty market-prepared customer IoT gadgets are exposed to this test suite, prompting discoveries that give a thorough outline of the security and protection stance of these gadgets.

The proposed technique can possibly act as the establishment for a star-based security evaluations framework for IoT gadgets entering the market. This framework could offer important bits of knowledge to shoppers, makers, and controllers, assisting them with arriving at informed conclusions about the security levels of IoT gadgets and empowering the improvement of safer items in the quickly extending IoT scene [11].

**2.9. How Secure Having IoT Devices in Our Homes**

In the contemporary time, innovation has flawlessly coordinated into our day to day routines, offering help and comfort. The coming of savvy home gadgets has altogether mitigated the weights of homegrown life, giving productivity and control. Nonetheless, the comfort includes some significant pitfalls — our own lives are progressively powerless against outside access. This paper dives into the security parts of shrewd home gadgets and their correspondence, drawing support from scholastic writing. It investigates the functionalities of these gadgets, distinguishes potential security chances, and expects future patterns in security assaults. By integrating data from different insightful sources, this examination expects to give an extensive comprehension of the security scene encompassing savvy home gadgets. It is basic to survey how well our homes are protected in the advanced domain. The paper will enlighten the functional parts of these gadgets, revealing insight into weaknesses that could be taken advantage of by malignant entertainers. In perceiving the likely dangers and showing the way that programmers can think twice about security of our savvy homes, this examination tries to bring issues to light about the requirement for defensive measures. Similar as we secure our actual homes with locked ways to battle off gatecrashes, it is similarly vital for brace ourselves against digital dangers. The paper finishes up by offering functional answers for safeguard our homes from security assaults, accentuating the significance of proactive measures to guarantee the respectability of our own advanced spaces [12].

**2.10. Towards Privacy-Preserving Local Monitoring and Evaluation of Network Traffic from IoT Devices and Corresponding Mobile Phone Applications**

The primary thought of this paper is to present a structure that permits clients to acquire bits of knowledge into the correspondence examples of their Web of Things (IoT) gadgets. The essential goal is to empower clients to comprehend and look at the genuine correspondence stream of these gadgets with their planned purposes. The structure enables clients to arrive at educated conclusions about the authenticity regarding the traffic produced by their IoT gadgets. In contrast to existing security occurrence occasion the executives (SIEM) arrangements that continually gather all data about a client's traffic, the proposed system guarantees that no extra information leaves the client's premises except if the client concludes that specific traffic is undesirable. In such cases, the client can wilfully move chosen portions to an outsider for additional examination, in this way restricting information spillage. The paper presents a bunch of devices for nearby examination and easy to understand perceptions, stressing schooling for the neighbourhood client or administrator of the IoT sending. This approach plans to cultivate more straightforwardness and informed decision-production at the neighbourhood level. The vital commitment of the paper is to exhibit that security safeguarding and GDPR-agreeable observing of IoT-related network traffic is achievable, giving clients command over their information and displaying how this checking system would work practically speaking [13

1. **Procedures for Proposed Method with an Algorithm**

We propose the mechanism of MapSec to be proactive in nature, instead of commonplace reactive security methodology. Scheduling preventive measures, along with backups and disaster recovery plans are key to a proactive strategy. The various modules in MapSec are designed especially keeping those in mind.

**Algorithm Steps:**

1. Initialize MapSec Platform:

* Set up the MapSec platform with modular components: Account, Controller, Credentials, Dashboard, and Scans.

2. Schedule Regular Scans:

* Input: Network details, scan frequency (e.g., every 6 hours or daily).
* Initiate a network scan at the scheduled frequency.
* Identify all devices connected to the network.
* Retrieve device details such as IP addresses and device types.

3. Discover Unused Open Ports:

* Input: Device details from the scan.
* Perform a port scan on each device to identify open ports.
* Keep a record of all open ports for each device.
* Identify ports that are unused or unnecessary for the device's functionality.

4. Scan Credentials for Online Leakages:

* Input: Device details, user credentials.
* Check each device's default login credentials.
* Scan online sources for potential leaks of these credentials.
* Utilize APIs from monitoring services like HaveIBeenPwned and BreachDirectory.

5. Map Credential Scan Data with Device Credentials:

* Input: Credential scan results, device details.
* Match credential scan data with the credentials of devices connected to the network.
* If a match is found, prompt the user to change the credentials.
* Ensure that the new credentials are strong and not easily guessable.

6. User Interaction and Data Storage:

* Input: User responses, updated device information.
* Store user details in the Account module for synchronization across devices.
* Store device information in the Controller module and enable synchronization via account sync.
* Securely store sensitive information in the Credentials module in a zero-knowledge format.
* Maintain a historical record of device scan data in the Scans module.

7. Dashboard Module

* Input: Device information, security insights.
* Serve as a centralized hub for user information.
* Provide a quick overview of critical details for an enhanced user experience.

8. NodeMCU and RaspberryPi connection

* Camera module is connected to nodeMCU
* Which is scanned through raspberryPi
* MapSec will show the analysis in computer

MapSec is purposefully designed as a loosely coupled platform, combining various modules to form a cohesive and comprehensive IoT security solution. The Account module, which serves as a repository for user details and allows data synchronization across devices, is one of the key modules. The Controller module is essential to MapSec, storing device information and enabling synchronization via the account sync feature. In terms of user data security, the Credentials module secures sensitive information in a zero-knowledge format and actively monitors for potential breaches via APIs from monitoring services. The Dashboard module, which is currently in development, is intended to serve as a centralized hub for user information, providing a quick and organized overview of critical details. Lastly, the Scans module maintains a historical record of device scan data, offering valuable insights into the security status of devices over time. Together, these modules contribute to MapSec's effectiveness in providing a proactive and user-friendly approach to IoT security.

These modules form a cohesive unit plan for a proactive IoT Security Plan. As for the internal service architecture, it consists of a 3 tier architecture consisting of independent units of Frontend, Backend and Database. The Backend is in FastAPI running on a Uvicorn server. The Frontend is in React + TypeScript. And we use a TinyDB [14] JSON Database to store the data, for easier transfer of data across different devices.

1. **Work Flow – proposed method**

The controller plays an important role in the MapSec project by initiating the execution of a ports scanner while also managing a credentials scanner. In addition, the MapSec platform includes a number of other modules, each of which performs a specific function within the overall security framework. The MapSec platform is intricately linked to the user's server, which can be a desktop or laptop computer. The system extends its reach to a Wireless Sensor Network (WSN), which includes sensor devices like the Raspberry Pi, NodeMCU [17], and cameras. This WSN is an important part of the project because these sensor devices continuously gather and transmit data. The MapSec controller orchestrates the scanning process of these sensors within the WSN in the project's workflow. The MapSec platform uses ports and credentials scanners to proactively assess the security status of sensor devices via this mechanism. The connection between the MapSec platform and the user's server allows for seamless network monitoring and management. This comprehensive approach ensures that potential vulnerabilities in the WSN are identified and addressed in a systematic manner, contributing to a higher level of security within the Internet of Things (IoT) ecosystem.

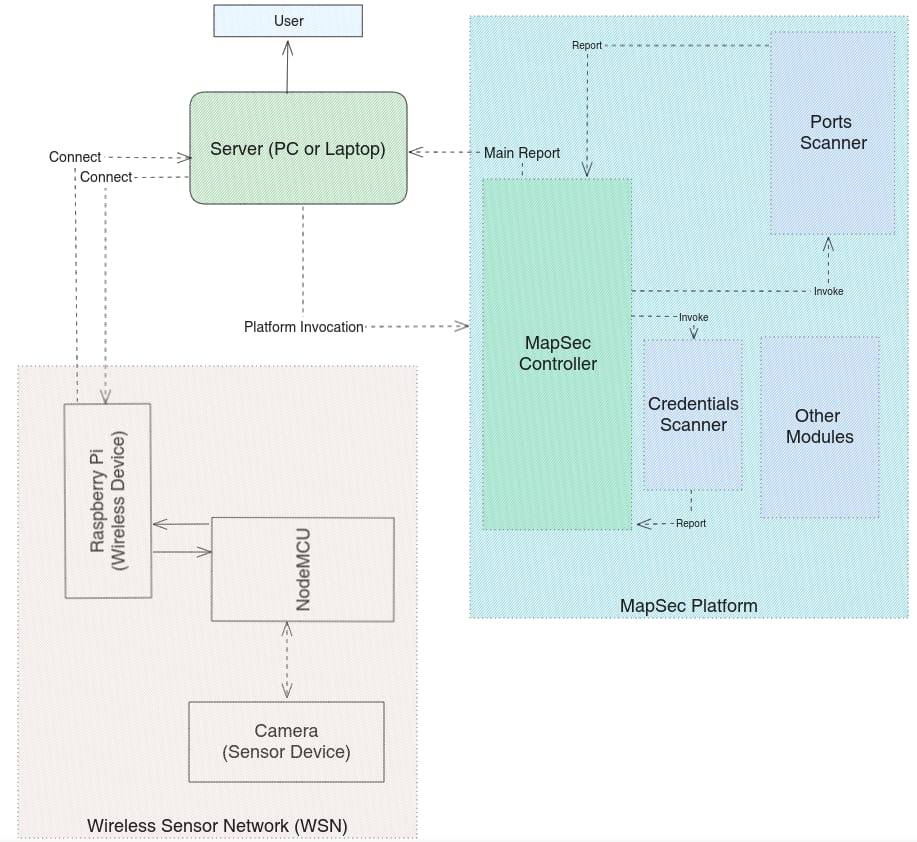


Figure 1 Workflow of the proposed work

MapSec envelops a few key modules, each assuming a critical role in its complete way to deal with IoT security. The Account module fills in as a store for client subtleties, offering the comfort for clients to download their MapSec information and synchronize it with different gadgets. The designers have likely made arrangements to carry out a live exchange, including further upgrading client adaptability. The Controllers module, albeit right now under development, is ready to become the foundation of the MapSec structure. It is intended to store insights concerning gadgets working as regulators inside the MapSec environment. These regulators, each having separate data sets, can be synchronized through the record sync highlight, giving a durable and coordinated construction to the whole framework. In the domain of client information security, the Credentials module, likewise under development, takes a proactive position. It safely stores messages and passwords in a zero-information design inside a JSON data set. Customary observing of messages and non-delicate subtleties utilizing APIs from checking administrations, for example, HaveIBeenPwned and BreachDirectory, guarantees ideal identification and reaction to expected breaks. The Dashboard module, right now being developed, vows to be an incorporated center point of data for clients. It is imagined as a catalog where a weak course of events, brief realities, and other basic subtleties are coordinated into a speedy dashboard. This plan means to work with clients in engrossing fundamental data initially, upgrading the general client experience. The Devices module, however under development, is intended to store insights regarding gadgets that have gone through checking by MapSec. This data can be synchronized across regulator gadgets, guaranteeing consistency and openness in the administration of filtered gadgets inside the IoT biological system.

The hardware implementation of the project is given in the figure 4. Which have Raspberry-Pi, NodeMCU, and computer. Figure 2 is Camera Module and Figure 3 shows Raspberry-Pi module. And full setup is shown in the figure 4.

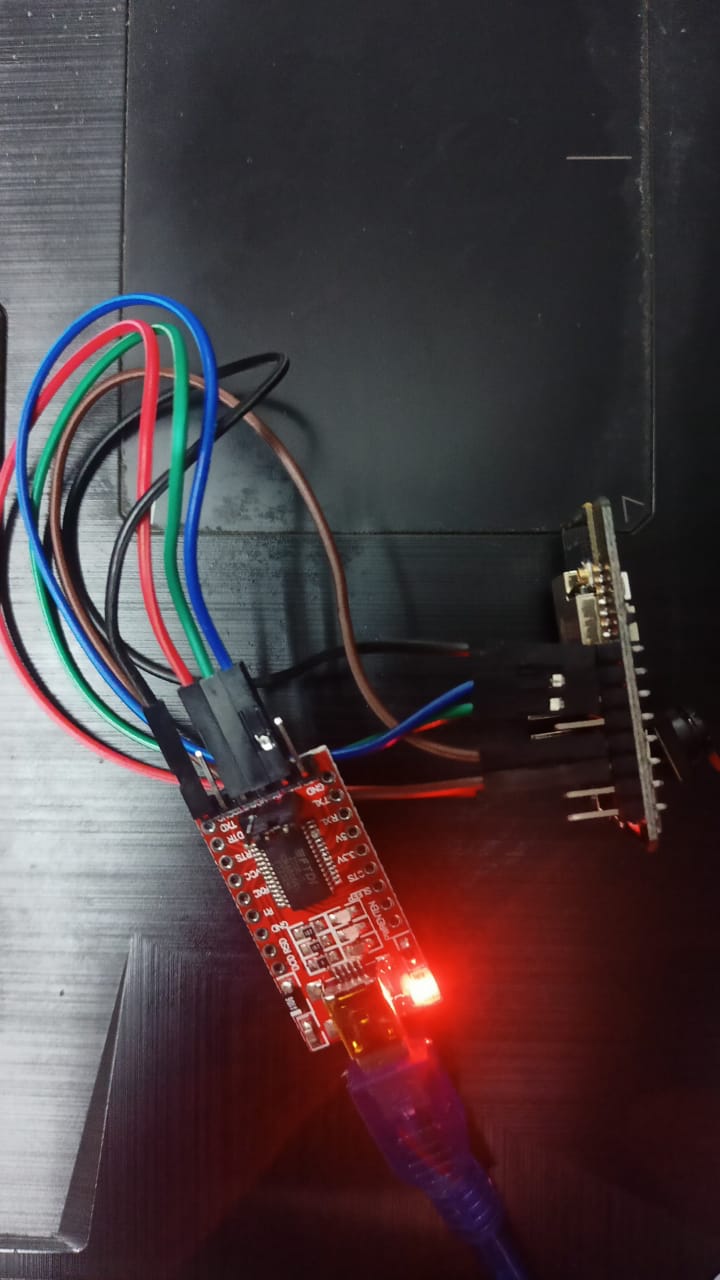
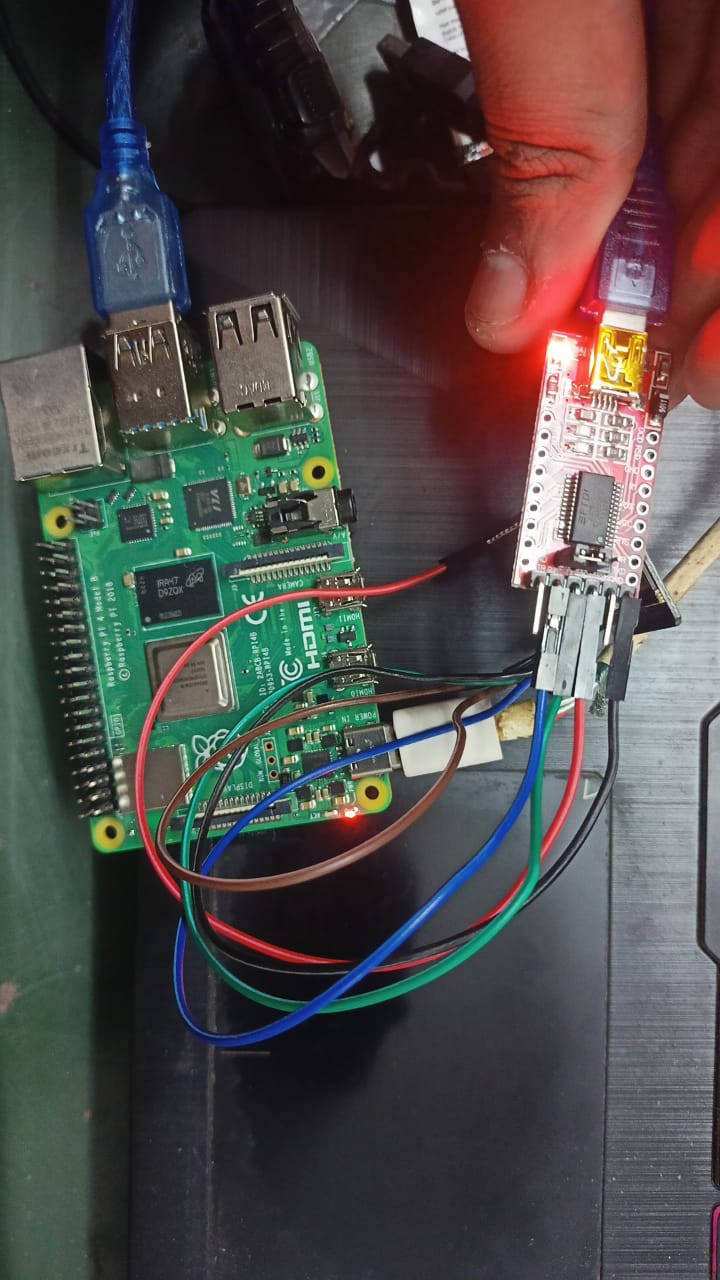
 

Figure 2 Camera Module Figure 3 Camera module connected with Raspberry Pi

In conclusion, the Scans module keeps a record of the output history for various gadgets associated with similar organizations as the regulator gadgets. This authentic information gives significant bits of knowledge about the security status of gadgets over the long run, helping clients follow changes and recognize expected patterns or examples connected with security weaknesses.

**5. Result and Discussion**

The presented paper underscores the inherent insecurity of IoT devices due to their dependency on external resources, posing a significant attack surface for real-time IoT devices. The narrative vividly illustrates a potential security breach scenario, emphasizing the critical need for robust security measures in the IoT landscape. The focus is on MapSec as a solution, positioned to fortify IoT ecosystems against vulnerabilities and unforeseen threats. The introduction outlines MapSec's multifaceted capabilities, with a specific emphasis on its role in addressing common vulnerabilities in IoT devices. The discussion on exposed credentials highlights the prevalence of default login credentials in IoT devices and how MapSec serves as a vigilant guardian by identifying and guiding users to change default credentials promptly. The section on exposed ports delves into the necessity of scrutinizing open ports for potential exploitation, with MapSec's advanced scanning capabilities offering timely notifications to empower users to secure their networks.

The integration of Open-Source Intelligence (OSINT) into MapSec's protective measures is discussed, underlining the importance of monitoring external threats and credential compromises [15]. The user-centric approach of MapSec is highlighted, emphasizing its ease of use and accessibility, positioning it as a valuable ally in simplifying the complex task of securing IoT networks. The literature review section provides context by referencing existing frameworks and solutions, showcasing Artorias, SecLab [16], and an automated IoT security testbed. While these frameworks contribute to automated security testing and evaluation, MapSec distinguishes itself with a focus on user-friendly features and proactive security measures. The proposed mechanism of MapSec is presented as a proactive security solution, scheduling preventive measures and providing a step-by-step workflow. The modular structure of MapSec, consisting of Account, Controller, Credentials, Dashboard, and Scans, is explained, highlighting their roles in a cohesive and proactive IoT security plan.

In summary, the paper effectively communicates the critical need for enhanced security in the IoT landscape, presenting MapSec as a comprehensive and user-friendly solution. The emphasis on proactive security measures, ease of use, and the integration of Open-Source Intelligence sets MapSec apart in the realm of IoT security frameworks. The proposed workflow and modular structure provide a clear roadmap for users to fortify their IoT ecosystems and make informed decisions about the security of their devices.

1. **Conclusion**

In conclusion, this paper has underscored the inherent security challenges within the Internet of Things (IoT) landscape, emphasizing the critical need for robust solutions to fortify IoT ecosystems against potential vulnerabilities. The vividly portrayed scenario of a security breach serves as a stark reminder of the real-world consequences of inadequate security measures, particularly for devices constantly connected and processing sensitive data. MapSec, introduced as a solution in this paper, emerges as a comprehensive and user-centric tool to address the multifaceted security issues plaguing IoT devices. The discussion has highlighted MapSec's unique features, including its proactive nature, ease of use, and a modular structure encompassing essential components like Account, Controller, Credentials, Dashboard, and Scans. The user-friendly approach of MapSec sets it apart from existing frameworks, as it simplifies the complex task of securing IoT networks, making it accessible to a broader user base. By focusing on exposed credentials, ports, and incorporating Open-Source Intelligence, MapSec provides a holistic security solution, allowing users to proactively manage and fortify their IoT ecosystems. The literature review contextualized MapSec within the broader landscape of IoT security frameworks, showcasing its distinctive features in comparison to Artorias, SecLab, and automated IoT security testbeds. While these frameworks contribute to automated testing, MapSec's emphasis on user-friendliness and proactive security measures positions it as a valuable and unique asset in the realm of IoT security. The proposed workflow and modular structure of MapSec offer a clear and practical roadmap for users to strengthen the security of their IoT devices. The paper's overall contribution lies in presenting a solution that not only addresses existing vulnerabilities but does so in a way that is accessible, proactive, and user-centric. In essence, MapSec stands as a promising and comprehensive answer to the pressing security concerns surrounding IoT devices, providing users with the tools and insights needed to make informed decisions and fortify their IoT ecosystems against evolving threats. The paper anticipates that the adoption of MapSec will contribute significantly to a more secure and resilient environment for IoT devices in homes and beyond.

**Reference**

[1] 1. B. Jeannotte and A. Tekeoglu, "Artorias: IoT Security Testing Framework," 2019 26th International Conference on Telecommunications (ICT), 2019, pp. 233-237, doi: 10.1109/ICT.2019.8798846

[2] P. Schwaiger, D. Simopoulos and A. Wolf, "Automated IoT security testing with SecLab," NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 2022, pp. 1-6, doi: 10.1109/NOMS54207.2022.9789797.

[3] Omnia Abu Waraga, Meriem Bettayeb, Qassim Nasir, Manar Abu Talib, Design and implementation of automated IoT security testbed, Computers & Security, Volume 88, 2020, 101648, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101648. (https://www.sciencedirect.com/science/article/pii/ S0167404819301920)

[4] J. Jung, J. Cho and B. Lee, "A Secure Platform for IoT Devices based on ARM Platform Security Architecture," 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2020, pp. 1-4, doi: 10.1109/IMCOM48794.2020.9001713.

[5] . Malik, B. H., Khalid, M., Maryam, M., Ali, M. N., Yousaf, S., Mehmood, M., & Saleem, H. (2019). IoT Testing-as-a-Service: A new dimension of automation. International Journal of Advanced Computer Science and Applications, 10(5).

[6] Alharbi, R., & Aspinall, D. (2018). An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities.

[7] Sivanathan, A., Gharakheili, H. H., & Sivaraman, V. (2018, December). Can we classify an iot device using tcp port scan?. In *2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS)* (pp. 1-4). IEEE.

[8] Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673-682.

[9] Jonsdottir, G., Wood, D., & Doshi, R. (2017, November). IoT network monitor. In *2017 IEEE MIT Undergraduate Research Technology Conference (URTC)* (pp. 1-5). IEEE.

[10] Payne, B. R., & Abegaz, T. T. (2018). Securing the Internet of Things: best practices for deploying IoT devices. *Computer and Network Security Essentials*, 493-506.

[11] Loi, F., Sivanathan, A., Gharakheili, H. H., Radford, A., & Sivaraman, V. (2017, November). Systematically evaluating security and privacy for consumer IoT devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 1-6).

[12] Estrada, D., Tawalbeh, L. A. A., & Vinaja, R. (2020). How secure having IoT devices in our homes?.

[13] Klement, F., Pöhls, H. C., & Spielvogel, K. (2020, June). Towards privacy-preserving local monitoring and evaluation of network traffic from IoT devices and corresponding mobile phone applications. In *2020 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

[14] Madden, S. R., Franklin, M. J., Hellerstein, J. M., & Hong, W. (2005). TinyDB: an acquisitional query processing system for sensor networks. *ACM Transactions on database systems (TODS)*, *30*(1), 122-173.

[15] Williams, Heather J., and Ilana Blum. *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Santa Monica: Rand Corporation, 2018.

[16] Ghiglieri, M., & Stopczynski, M. (2016, September). Seclab: an innovative approach to learn and understand current security and privacy issues. In *Proceedings of the 17th Annual Conference on Information Technology Education* (pp. 67-72).

[17] Parihar, Y. S. (2019). Internet of things and nodemcu. *journal of emerging technologies and innovative research*, *6*(6), 1085.