Towards the reliability of PRNU based scanner identification for securing authentication in IIoT

Prabith GS, Chandrakiran J
Computer Science and Engineering)
Amrita School of Computing, Amrita Vishwa Vidyapeetham.)
Amritapuri, India
prabith7.g.s@gmail.com, chandrakiran03@hotmail.com

***Abstract*—In the recent times, cyber attacks on the IoT and IIoT industry has increased rapidly. IIoT devices are everywhere, so IIoT attacks are on the rise. The vulnerability of IIoT comes from risks inherent both in the devices themselves and in the ways they interact with the rest of an organization's systems. Thousands of cyber attacks were recorder in 2021 itself. Since the IoT and IIoT devices are more valuable and used frequently, securing those devices to protect against IoT and IIoT attacks is a critical step for every security team. In this paper we aim at checking the reliability of the remote user authentication that combines Photo Response Non-Uniformity (PRNU) and fingerprint biometrics [3] by creating a tool for the authentication using Python.**

***Index Terms*—PRNU, Scanner Identification, IIoT**

I. Introduction

Biometric authentication generally proves more secure than traditional methods of authentication but still, hacking into a biometric authenticated system is possible. Securing the devices using another layer of protection along with biometric authentication and PRNU makes it more secure. Photo Response Non Uniformity (PRNU) is the difference between a sensor's actual response and the uniform response when uniform light is falling on it.

The cyberattacks against the Ukrainian power utilities in December 2015 were unusual in that actual harm was done. However, there is a lot of proof that organisations' operating systems have been infiltrated widely. [9]

Following a series of cyberattacks on three local energy firms, significant portions of the Ukrainian populace experienced power outages over the 2015 holiday season. The identity of the hackers is still unknown despite being commonly believed to be from Russia because identification in these cases is difficult. However, the primary attack vector – a well-known trojan called Black Energy – has been definitively established.

The specifics of how the operational systems of the Ukrainian power firms were penetrated serve as an informative case study highlighting the complexity of today's cyberattacks and the susceptibility of organisations participating in the Industrial Internet of Things (IIoT).

II. Related Work

In accordance with the thesis written by Jan Lukáš, Jessica Fridrich, and Miroslav Goljan [1], Which proposes the authentication of the image using PRNU, In a court setting, identifying the source of photos given as evidence would be extremely helpful if the equipment used to capture a specific digital image could be accurately identified. This research paper discusses a new approach to the issue of digital camera identification from its images based on the sensor's pattern noise. The photo-response non-uniformity noise and the fixed pattern noise (FPN) are the two primary elements of the pattern noise (PRNU). FPN refers to a certain noise pattern on digital imaging sensors that is frequently seen during longer exposure shots and occurs when some pixels are prone to producing greater intensities than the average intensity. Only a minor portion of the pattern noise is the fixed pattern noise. The pixel non-uniformity noise brought on by varied pixel light sensitivity is another, much stronger, component that better withstands processing [2]. Ambient temperature or humidity have no impact on PNU noise. The output from the scanner is represented as

$$I_R = I^0 + I^0 P + \theta \tag{1}$$

where I^0 is the noise-free version of the output image I_R, P is the camera PRNU fingerprint and θ independent random noises.

This study also discusses several flaws that inevitably enter the image acquisition process and provides a brief description of the processing processes inside a typical digital camera. Analyse the pattern noise and its characteristics to determine which elements are most likely to be helpful in identifying cameras.

A technique known as flat fielding, which involves first correcting the pixel values for the additive FPN and then dividing them by a flat field frame, can be used to reduce the pattern noise.

The noise is then achieved using a denoising filter F to the image I_R,

$$Q = I_R - F(I_R) \tag{2}$$

The author have used the wavelet-based denoising filter. The PRNU fingerprint,$\hat{P}$ is generated by computing maximum likelihood estimate

$$\hat{P} = \sum_{i=1}^{N} Q_i I_{Ri} / \sum_{i=1}^{N} (I_{Ri})^2 \tag{3}$$

where N is the number of images.

We compute the correlation C between the camera reference pattern and the noise residual n = p - F(p) to determine if an image p was captured by camera C.

$$\rho_C(p) = \operatorname{corr}(n, P_C) = \frac{(n - \bar{n}) \cdot \left(P_C - \bar{P}_C\right)}{\|n - \bar{n}\| \left\|P_C - \overline{\boldsymbol{P}}_C\right\|}, \quad (4)$$

According to the thesis, "Securing Remote User Authentication in Industrial Internet of Things ", User authentication is crucial to Industrial Internet of Things security. Many of the current authentication methods, however, are open to numerous attacks. In the referenced paper, They presented a strong user authentication scheme that uses fingerprint recognition and photo response non-uniformity to secure IIoT. PRNU-based authentication minimizes the attack surfaces by assisting in the demonstration of the user's device's ownership. The proposed method uses hardware and user fingerprints to successfully thwart phishing and spoofing attacks. Even though they only ran a small-scale experiment to demonstrate PRNU's effectiveness, we still managed to get results that have the potential to greatly enhance IIoT security. [3] [4]

The study suggests a pixel PRNU-based unified framework for both device identification and integrity verification. Both tasks begin with estimating the PRNU using a maximum-likelihood estimator that is created from a condensed model of the sensor data. The maximum likelihood estimator for the PRNU is derived, and the results highlight the need for pre-processing the estimated signal to get rid of some systematic patterns that could increase the number of false alarms in device identification and the number of missed detections in integrity verification. Some malicious changes in the image may preserve the PRNU, such as changing the colour of a stain to a blood stain. Such manipulations will not be detected using this method.

III. Solution Approach

To guarantee that linked IoT devices can be trusted to be who they say they are, strong IoT device authentication is needed. As a result, each IoT device requires a special identity that can be verified during connection attempts to a gateway or central server. [8]

Whether we realise it or not, biometrics are becoming more and more crucial to how we perform daily chores. As time goes on, the use of biometrics will increase and many of us will utilise them automatically to access a variety of goods and services that we use on a regular basis. [10]

In today's era, Cyber Authentication enables organizations to keep their networks secure by permitting only authenticated users or processes to gain access to their protected resources.

There are many different cyber security techniques, and each has its own difficulties. We need to develop a solution that overcomes the limitations of existing approaches. The raw data is encrypted before being delivered over the channel in order to guarantee the authentication of the authorised user. Therefore, there ought to be specialised techniques that can stop attacks like 3D spoofing.

Issues include:

(1) the resistance to impersonation attacks;

(2) the irrevocability of biometric templates; and

(3) guarantee that personal information remains private

We need to make the IIot (Industrial Internet of Things) applications more secure when it comes to authentication and security to safeguard the critical information.

TABLE I
BIO-METRICS COMPARISON

Biometric Characteristics	**Table Column Head**						
	Finger	***Facial***	***Iris***	***Hand***	***Retina***	***Sign***	***Password***
Universality	High	High	High	Mid	High	Low	Low
Distinctiveness	High	Low	High	Mid	High	Low	Low
Permanence	High	MId	High	Mid	Mid	Low	Low
Collectability	Mid	High	Mid	High	Low	High	Low
Performance	High	Low	High	Mid	High	Low	Low
Acceptability	High	High	Low	Mid	Low	High	Low
Circumvention	Mid	High	Low	Mid	Low	High	Low

- Security – security-wise, it is a vast improvement on passwords and identity cards. Fingerprints are much harder to fake, they also change very little over a lifetime, so the data remains current for much longer than photos and passwords. They are simple and straightforward to utilise for the user. No more having trouble recalling your previous password or getting locked out because you forgot your photo ID at home. Your fingerprints are always with you. [5]
- Non-transferable – fingerprints are non-transferrable, ruling out the sharing of passwords or 'clocking in' on behalf of another colleague. This allows for more accurate tracking of workforce and provides additional security against the theft of sensitive materials. Increased accountability at work is another benefit of utilising fingerprint recognition. Biometric evidence that you were present when a scenario or occurrence occurred is difficult to dispute and can be used as proof, if necessary.
- Cost effective – from a technology management perspective, fingerprint recognition is now a cost-effective security solution.Small, portable scanners provide a high degree of precision and are simple to set up.

With regards to our analysis from the above table [6], We had come to a conclusion that fingerprint authentication can be the best bio-metric authentication suitable to integrate with PRNU as cited in [3]

Security experts have been particularly worried about the risks associated with fingerprint authentication. So, a new tool to identify fake images has lately been introduced: the Photo-Response Non-Uniformity [1]. Significant research has been done and is being done in the area of bio-metric authentication security.

Here we aim at checking the reliability of the authentication by integrating PRNU and fingerprint authentication with a larger database. So we've developed a Python tool for checking

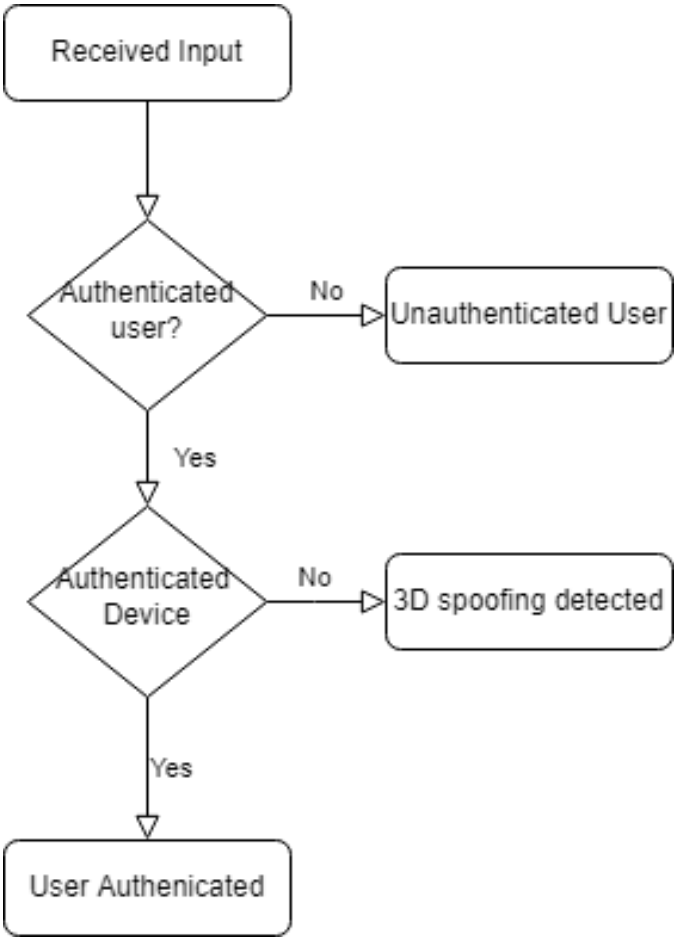

Fig. 1. Flow Chart.

the authenticity of the fingerprint and device using PRNU. That is, If the fingerprint matching score (y)

$$x > 60$$

, It checks for the PRNU PCE (y) value. If

$$y > 60$$

, then the user gets authenticated else the tool denies access.

A. Experiment Set-up

The experiment setup includes a biometric fingerprint sensor module connected to Raspberry Pi 3 Model B using PL2303HX 3.3v/5v TTL (Transistor-Transistor Logic) Logic Level USB Serial Port Adapter. We use the source identification algorithm presented in "Determining Image Origin and Integrity Using Sensor Noise" to test the fingerprint images. Peak to Correlation Energy(PCE) which is a ratio that is the squared correlation divided by the sample variance of the circular cross-correlations is used as the similarity metric for identifying the source scanner or biometric fingerprint scanner in the Python source code.

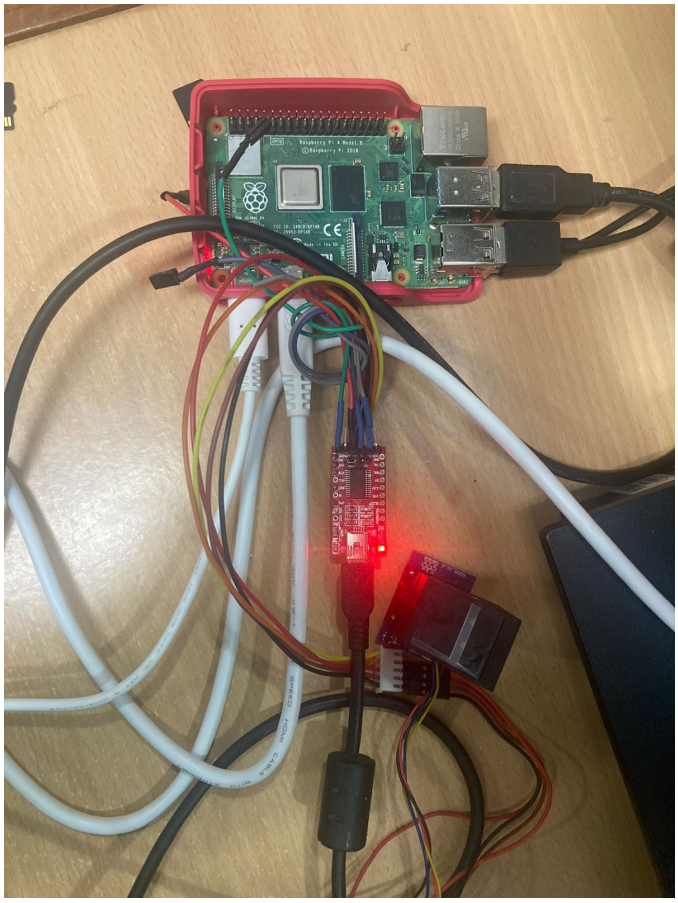

Fig. 2. Experimental Setup.

IV. Experiment and Performance Evaluation

To verify the reliability of an existing method which combines PRNU with Biometric fingerprint . First to verify the fingerprint, the fingerprint scanner capture an image of the fingerprint being scanned and make sure the pattern matches the one in the database. To verify if a fingerprint picture belongs to a particular scanner, we correlate the image's PRNU in opposition to that scanner's reference fingerprint extracted from at least six images. When two separate sources are compared, PCE values are close to zero for unauthentic photos. The PRNU matching is carried out principally based totally on a PCE threshold charge of forty. Authentic devices could be identified from the fingerprint image. We made the setup and verified the reliability of the PRNU and fingerprint authentication tool.

V. Conclusion

Despite numerous user authentication techniques, attackers continue to find a way. To sharpen the security we put forward usage of PRNU based scanner identification. In this paper, by carrying out the experiment we have verified the reliability of the technique which combines Photo Response Non-Uniformity and fingerprint biometrics. This technique

prevents several types of attacks such as 3D spoofing and also helps to verify the device thus providing more security.

REFERENCES

[1] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, 2006.

[2] M. Chen, J. Fridrich, M. Goljan, and J. Luk´as, "Determining image origin and integrity using sensor noise," IEEE Transactions on information forensics and security, vol. 3, no. 1, pp. 74–90, 2008.

[3] K. Nimmy, S. Sankaran, K. Achuthan and P. Calyam, "Securing Remote User Authentication in Industrial Internet of Things," 2022 IEEE 19th Annual Consumer Communications Networking Conference (CCNC), 2022, pp. 244-247, doi: 10.1109/CCNC49033.2022.9700512.

[4] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "User authentication via prnu-based physical unclonable functions," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1941–1956, 2017.

[5] M. Casey, M. Manulis, C. J. Newton, R. Savage, and H. Treharne, "An interoperable architecture for usable password-less authentication," in International Workshop on Emerging Technologies for Authorization and Authentication. Springer, 2020, pp. 16–32.

[6] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of multi-factor authentication for securing advanced iot applications," IEEE Network, vol. 33, no. 2, pp. 82–88, 2019.

[7] K. Nimmy, S. Sankaran, and K. Achuthan, "A novel multi-factor authentication protocol for smart home environments," in International Conference on Information Systems Security. Springer, 2018, pp. 44–63.

[8] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724–4734, 2018.

[9] BBC, "Ukraine power cut 'was cyber-attack'," 2017. [Online]. Available: https://www.bbc.com/news/technology-38573074

[10] P. Kumar and G. S. Gaba, "Biometric-based robust access control model for industrial internet of things applications," IoT Security: Advances in Authentication, pp. 133–142, 2020.