PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 06 • June 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

The Smart Home Cybersecurity Paradox: Is Your Raspberry Pi Secure Enough to Protect against Attacks?

A $35 computer can be a lifesaver or a life-threatener to your smart home and new Pakistani and other research indicates that the difference is reduced to the way you establish it.

By **Fizah Iman** | University Of Agriculture | Published: Thursday June, 2026
imanfizah28@email.com | Position: Student

Introduction

Walk Within the Karachi and Lahore Raspberry Pi has become a building block to smart home hobbyists. This very low-cost and energy saving microcomputer has exceptional versatility. Nevertheless cybersecurity researchers point out a very serious two-sidedness, The very hardware used to automate household tasks can also be a very serious network vulnerability. Global research indicates that an optimally secured Raspberry Pi is capable of intercepting 99.9% of domestic cyber intrusions. On the other hand conference talks such as those at DEF CON 33 have demonstrated how poorly secured commercial products based on Pi architecture. such as high end smart smoke detectors can be hacked to enable covert audio surveillance. This comes as a major challenge in the fast changing technological environment of Pakistan whereby the incorporation of smart devices often outcompetes the adoption of sound security measures. The very cheap hardware that drives local innovation can also become an unintentional network vulnerability. According to researchers who combine real time threat intelligence with a Raspberry Pi, a 99% success rate in identifying and neutralizing denial of service and brute force attacks can be achieved.

> ***"In a study, the researchers obtained a rate of 99.% detection and prevention of brute- force attack and denial of service attack with a Raspberry Pi and real-time intelligence on threats."***

Technology Overview

So The Raspberry Pi is a fully fledged computing platform with memory, processing, internet connectivity and USB ports all fitted into a board that is about the size of a credit card.. Costing only 35 dollars and using only five watts, it can be easily interoperated with various other peripherals such as GPS trackers, motion sensors and environmental monitors. This flexibility has made it one of the major tools in developing smart homes in the world and in Pakistan. University students in the Islamic world, including Islamabad to Faisalabad, are busily using these devices to design energy monitoring systems, security surveillance systems and automated agricultural irrigation systems. This hardware has two diametrically different security functions depending on its configuration. The process of open source software integration (UFW firewall, WireGuard to tunnel an encrypted VPN and Suricata to detect intrusions) into a defense will make the Pi a powerful network guardian. It constantly monitors the packet traffic to counter aberrant traffic and also helps in enabling the safe remote access to the internal systems without putting the entire network at the mercy of the external internet. On the contrary a poorly maintained Pi is an extremely appealing target to attackers. Poor cryptographic policies, old

and out of date software and default credential settings provide easy access points. Analysis of a commercial Pi based smart smoke detector in 2025 identified these risks as showing no basic authentication and secure boot procedures.

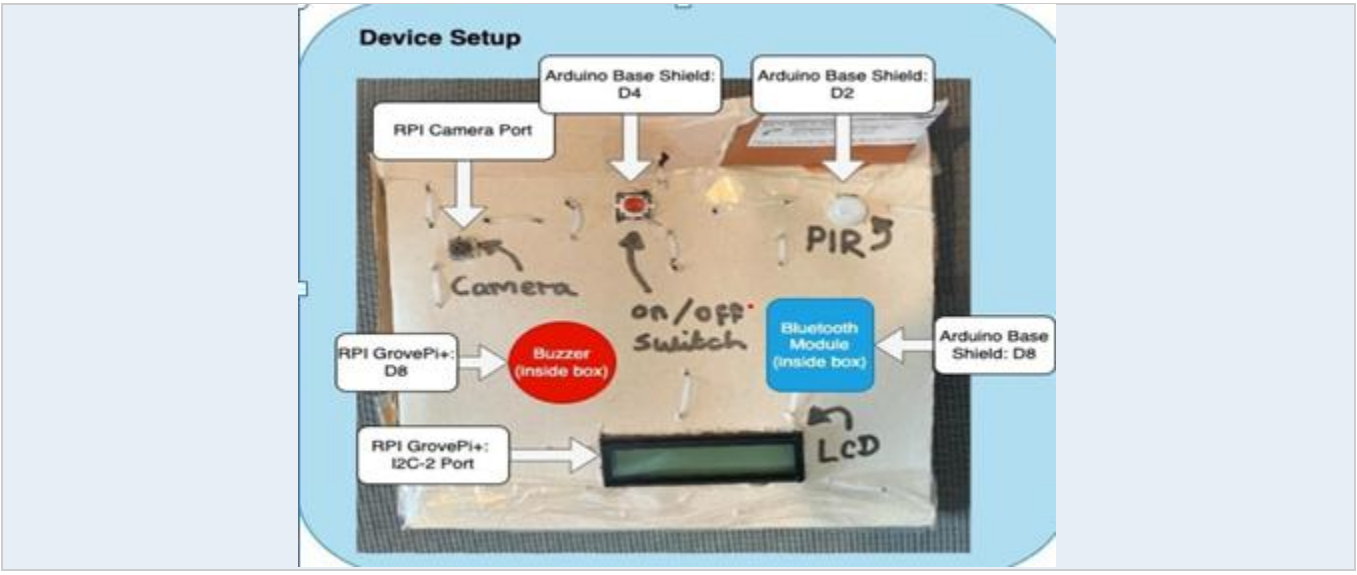

Figure 1: Image : Physical wiring diagram showing Raspberry Pi connected to Grove sensors, Arduino, and camera module. Credit: Kieran Williams / Source: CM2306 Security System IoT Project , Cardiff University GitLab Repository

Key Findings & Impact

The study of empirical research that will be held at the beginning of 2025 will give solid information about the effectiveness of Raspberry Pi security implementations. A combination of the Malware Information Sharing Platform (MISP) and the Suricata intrusion detection platform on Pi hardware the system was able to intercept 99.9% of traditional cyber threats such as malware distributions, denial of service flooding and brute force intrusions. This degree of all but perfect enterprise grade defense is afforded on hardware that is truly extraordinarily cheap.

Moreover the fact that strong encryption is slowing down the low power processors has been refuted. The use of the Dynamic Session Enhanced Key Protocol (DSEKP) incurs only a 10 percent overhead in data packet, and an initial 27 percent spike in latency only when establishing a session. Users are therefore able to enjoy high network throughput and enjoy military grade encrypted sessions.

Local users are still concerned with physical security. Unless the complete disk encryption procedure is applied using LUKS, an attacker with physical access to the device or SD card can easily acquire all the information stored on it. The fact that the secure boot is not provided in most business versions also enables attackers to reverse engineer the operating system by dumping the memory of the device.

In the fast advancing technology industry of Pakistan these weaknesses highlight a significant neglect. security measures are often seen as after the fact measures as opposed to pre-deployment considerations. Simple security measures like adding two factor authentication, turning off password-based SSH access and changing default passwords should not take a lot of time and help to counteract the overwhelming majority of automated attacks. To regional businesses making an entrance into the IoT arena this is indicative that affordable hardware will easily support real time threat detection and lightweight encryption without hurting the budget or performance of the system.

What's Next?

The next generation of Raspberry Pi security will probably incorporate machine learning and artificial intelligence to self-autonomously.

Detect deviant network behaviors instead of using fixed rule sets. The expected hardware developments should normalise trusted execution environments and secure boot features thus closing the gap between enterprise grade protection and hobbyist infrastructure. Pakistan has a unique opportunity in this development with a growing tech literate population that the country can afford to avoid the security mistakes made by the more developed markets. Academic institutions should integrate the concept of IoT security in their curriculum and local startups need to focus on secure by default engineering. Moreover this transition can be enabled by the strong open source community through the spread of best practices and configuration manuals in both English and Urdu.

User awareness is the main challenge since most people do not realize that such devices need proactive and continuous defense measures. Users have to be aware of the natural dangers of static passwords and the importance of network partitioning and confirmed software updates. As an active defense strategy to standard users, adjusting default passwords before going online and implementing a restrictive firewall such as UFW, changing password-based SSH to ed25519 cryptographic keys, automatic critical security patches and fail2ban to stop unnecessary access points. These procedures are performed within less than half an hour and are effective in reducing more than 99% of automated cyberattacks.

Commercial developers are also subject to stricter requirements such as the requirement to use secure boot verified and encrypted root filesystems the disabling of production level physical debug interfaces (such as UART and JTAG) and cryptographic signatures of all firmware updates. These advanced features are natively supported by hardware such as the Raspberry Pi Compute Modules 4 and 5. In the end it is up to the user and developer and the hardware is just a programmed machine.

About the Author

I am Fizah Iman currently puruing the degree of Bachelor of Computer Science. I can be reached at imanfizah28@gmail.com.

Keywords: Raspberry Pi; Smart Home Security; Cybersecurity; IoT; Pakistan Technology; Intrusion Detection; Encryption

References

[1] Addison, S. K., Mohammad, T., & Isoaho, J. (2025) Experimental Implementation of a Low Cost Real-Time Threat Intelligence Solution for Smart Home Security, ScienceDirect / UTUPub.

[2] Džankić, R., Bulatović, Z., & Bauk, S. (2025) Improving Security and Privacy with Raspberry Pi Devices, Signals and Communication Technology, Springer.

[3] Pereyra, S. (2025) Next-gen school smoke detector sparks privacy concerns with embedded microphones, News (DEF CON 33 coverage).

[4] Rakshit, H., Bhandari, R., & Banerjee, S. (2025) Lightweight Session-Key Rekeying Framework for Secure IoT-Edge Communication, arXiv:2511.02924.

[5] Tsyrfa, V. (2025) You can eavesdrop on people through a vape detector, Gagadget