International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM03973
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Ransomware Prevention System using Python and IoT

Dr. T. Amalraj Victoire[1] Mrs. M. Vasuki[2] B. Prasanth[3]
[1]Professor, Department of Computer Applications, Sri Manakula Vinayagar Engineering College
[2]Associate Professor, Department of Computer Applications, Sri Manakula Vinayagar Engineering College
[3]PG Student, Department of Computer Applications, Sri Manakula Vinayagar Engineering College
amalrajvictoire@gmail.com[1], dheshna@gmail.com[2], tbkprashant@gmail.com[3]

Abstract: Ransomware attacks are a critical threat to data integrity by file encryption and ransom payment for decryption. Conventional cybersecurity mechanisms are ineffective against zero-day ransomware attacks, and hence a forward-looking mitigation solution is required. This project proposes a Ransomware Mitigation System that scans file system activity in real-time through Python to identify ransomware attack patterns through file encryption activity.

During a ransomware attack, the encryption process changes file extensions, which Python identifies and notifies a .NET Windows Forms application. When identified, the application automatically activates an ESP8266-based IoT relay to physically remove the infected device from the network to prevent further decryption. The system also disables network drivers to prevent further propagation of the attack.

Once isolated from the network, the system will prompt the user to start recovery procedures, recovering compromised files back to their previous safe state. To provide added data resilience, the project additionally employs an hourly or daily automated backup procedure that ensures constant protection of data against ransomware attacks. Proactively reducing data loss and preventing the spread of ransomware, this implementation also integrates well with current cybersecurity systems for added system protection.

Objectives:

1) Comprehend the need of anti-ransomware system in the first place basically, how it can keep your precious data safe and stop hackers from wrecking your day.
2) Dig into what's happening with ransomware trends. What's new, and just how bad it can affect the data and your system.
3) Figure out why it's so difficult to spot and shut down these attacks. Examine the real time monitoring, network segmentation, and data recovery.

Keywords: Ransomware Prevention, Cybersecurity, File Monitoring, Python, IoT Security, ESP8266, Network Isolation, Data Protection, Backup and Recovery.

1. Literature Review

Ransomware is basically the digital threat right now everywhere you look in cybersecurity, people are talking about it. It's not just hitting big corporations; home users get wrecked by it too. Thieves toss their nasty code around, scramble files, and then demand you cough up cash or Bitcoin, usually for the decryption key.

Anyway, tons of smart people have been breaking their brains trying to crack the code on how ransomware acts, how to spot it early, and, of course, how to keep your stuff safe. That's kind of what this survey is about just zooming out and seeing which tricks actually work for stopping these attacks, especially since we're all-in on building our own Python and IoT-based anti-ransomware setup.

Oleg Skulkin wrote this incident in 2022 that's honestly a lifesaver. He lays out everything: monitoring things as they happen, doing forensics once things go sideways, yanking infected devices off the network ASAP. This dovetails with what we're building: catch files misbehaving with Python, then flip the ESP8266 switch to axe internet connections if needed. The sooner you notice and isolate, the better. It makes our idea of auto-network-throttling with IoT look even smarter.

Now, check out Khowla Khaliq and crew's 2024 research they dig into the nitty-gritty of detection. It turns out, the classic antivirus you're paying for, it kind of blows at catching sneaky, never-seen ransomware. They talk about how you got to watch for weird file changes and suspicious behavior on the fly, lending props to our whole file monitoring angle using Python. They even shout out anomaly-based detection, which, by the way, is right in our wheelhouse if files suddenly start getting encrypted out of nowhere, something's fishy.

Then there's one from Se-Beom Cheon et al. they basically written about whitelist-only protection. Hackers just dress up their evil software as "safe" apps and stroll right in. This is why we don't treat whitelisting like gospel. Our approach is to watch what files actually do instead of relying on a pre-approved list. If a "trusted" process starts mangling files, it's getting flagged.

Atul Kumar and Ishu Sharma put Android ransomware under the microscope using a bunch of real phone data. While our project's mostly Windows-focused, their findings spill over. Turns out, the same kind of monitoring magic works across platforms. Plus, their work makes us look smart for eyeing network isolation via IoT as a way to shield everything including phones and smaller gadgets down the line.

Roger Grimes (2022). He breaks down how ransomware keeps evolving now you've got fileless attacks, shape-shifting malware, and ransom notes tailored just for you. He says what everyone's thinking: automate backups and try stuffing AI in your defenses because cybercrooks are moving fast. We're onboard with all that; our system's got a backup-and-restore module already, and plugging in some AI could crank it up a notch.

All in all, these papers show ransomware is leveling up, so you can't stick to old-school defenses. Watching files in real time, slamming the internet door when needed, and backing up everything. That's the stuff that actually works. Our system pulls pieces from all these studies Python scripts for file watching, ESP8266s that stop connections, and backup smarts on tap.

2. Research Methodology

Instead of running experiments or bothering people for interviews, I dove straight into the info that's already out there. We're talking endless hours spent knee-deep in cybersecurity reports, flipping through academic journals that only nerds like me seem to read, and scrolling some seriously sketchy corners of malware forums. Most of my data came from these security threat intelligence reports. The big cybersecurity companies like CrowdStrike and Palo Alto Networks yeah, those guys plus a mishmash of research papers, and some really wild case studies about ransomware attacks gone sideways. I checked what's trending in ransomware, how hackers actually pull off their attacks, and get this the gaping holes most current solutions leave wide open. That's how we got ideas for the Ransomware Prevention System: to get ahead of the game, catch threats early, lock down the network, and recover your stuff before some cyber attackers can make the day even worse.

3. Current Scenario of Ransomware Threats

Ransomware is just everywhere now. It's like the cockroach of the cyber world. Doesn't matter if you're some random college kid, a hospital, or the bloody government, these cyber-crooks don't discriminate. They bust in, lock up all your files, and then hit you up for crypto like it's some twisted version of Monopoly. If the user wants to get the data back, they have to pay up, and oh, good luck figuring out who just mugged you, because those Bitcoin wallets are harder to track than your shoes after a wild night out. And the worst part is that attackers keep leveling up. There's this whole Ransomware-as-a-Service gig going on, like Netflix, but instead of movies, it's digital blackmail for rent. Now, anyone with a bad attitude and Wi-Fi can play villain. Honestly, your old security software is probably crying in the corner at this point. Numbers are wild too.

Cybersecurity Ventures says damages might hit $265 billion yearly by 2031. That's billionaire-level cash every year. And reportedly, there's a ransomware hit every two seconds, so by the time you've read this, someone else's Monday just went down the toilet. IBM is over there talking about the average hit costing $4.54 million, and get this, that's without even paying the ransom. That's just cleaning up the mess. Most places dealing with this stuff wind up offline, which, you know, is super handy if you're, say, a hospital or government.

India's not escaping either. Ransomware attacks there shot up 53% last year. It's getting nasty in hospitals, banks, government offices, you name it. CERT-In (Indian Computer Emergency Response Team) says hackers are doing double extortion now, so if you don't pony up, they'll just leak your embarrassing files on the internet for everyone to see.

With 300,000+ new ransomware viruses popping up every year, it's tough to keep up. That's why you need all the fancy new toys: real-time detection, instant network lock-downs, magic self-healing files whatever you've got. The good old "don't click sketchy emails" isn't enough anymore. It's like bringing a butter knife to a gunfight.

4. Challenges in Ransomware Prevention

Although ransomware prevention systems have safeguard features protecting from escalating cyber threats, certain issues need to be resolved to enhance their functionality, usability and adoption on a wider scale.

Security Risks: Ransomware attackers design new ways of bypassing traditional preventive mechanisms. Detection becomes problematic in zero-day ransomware attacks because there exists no prior signature. Polymorphic malware, which changes its code to evade detection and keep reappearing, further complicate the situation. Avoiding solely signature-based methods ensures a robust anomaly-based detection system.

Trust Factor: Automated ransomware preventive systems are rejected by many corporations because of the automatic detecting mechanisms that are sensitive to interrupts of normal activities. The network disconnection containment strategies involving separation of the infected systems from the network must be accurate to the high degree so that erroneous downtime is not experienced. Besides, users need to trust that the ransomware detection system will not jeopardize privacy through data collection surveillance.

Technological Integration: Operating system interfaces, monitoring stations, and security gateways need to integrate seamlessly with ransomware prevention. The usability across different existing and emerging file systems, cloud storages, and security frameworks of the enterprise is the greatest challenge. Additionally, IoT based network isolation has to secure unabated access across diverse networking environment so that disconnection from the network cannot be noticed by other uninfected devices.

Privacy Concerns: Organizations worry that monitoring activities in a file system will leak sensitive information or even create new gaps in their already fragile cybersecurity infrastructure. File monitoring must be performed in a manner that user privacy is protected, but threats can be detected as early as possible. If we are not nailing down how you handle data and sticking to your own security rules, you're just begging for trouble.

Legal and Regulatory Risks: Depending on where you're working and what field you're in, you've got to juggle a ton of different rules. Think about GDPR in Europe, HIPAA for health care in the U.S., and PCI-DSS if you're dealing with credit cards. These things do NOT play around mess up and suddenly monitoring your network or locking sections down gets way harder, because you're walking on eggshells with user data. Balancing what your business needs and what's legally required.

Infrastructure Gaps: Too many companies are still dragging along ancient computers and crummy security setups, hoping for the best. Real-time threat alerts are barely known by the employees and what ransomware even is, let alone how to avoid it. Basically, if your infrastructure's not good and your team's clueless, you're rolling the dice with ransomware every single day.

User Adaptation: Most users do not have any background information about automated ransomware mitigation procedures. As with any anti-virus program, a ransomware prevention system must monitor for file activity, encryption, and suspicious alteration in files on a proactive basis. User education on recovery steps post-file restoration is essential along with an understanding of why network segmentation is a prerequisite to fully harness the technology and ensure comprehensive protection.

5. Existing System

Most organizations still just rely on the usual suspects for fighting ransomware: basic antivirus, something fancier like EDR, and your regular old backups. It's nothing groundbreaking, honestly. These tools pretty much just scan for stuff they already recognize because of signatures, maybe worry when a file acts wrong, or descend in with backup copies when things go sideways

EDR and antivirus are not good since the attackers watch over your files for anything that matches their blacklist of signatures. Oldest trick in the book. Backup routines try to roll things back if ransomware messes with your files, sometimes they'll just tweak the data back to how it was before you got hosed. Between saving stuff on a local drive or tossing it up to the cloud, your data got a fighting chance. Not bulletproof, but better than nothing.

However, there are some issues with the current ways organizations try to fight ransomware:

1. *Ineffective Against Zero-Day Attacks*: If you're using that old-school, signature-based antivirus. It's not suitable anymore. It's great at catching the obvious stuff, but it can't catch zero-day ransomware or polymorphic viruses. They just bypass right past. The software's blind to anything it hasn't seen before.
2. *Delayed Detection and Response:* Honestly, most systems find the ransomware only after your files are locked or encrypted. By the time you know something's up, it's already too late. All the data is lost and recovery is impossible without a existing backup.
3. *Lack of Network Isolation:* It's wild how many defenses don't just isolate or disconnect an infected machine. Instead, they sort of sit there watching the malware hop from one device to another, spreading virus throughout the system.
4. *Dependence on Backups:* Sure, backups are supposed to save the day, but they don't stop the attack in the first place. Plus, some of the latest ransomware variants are smart enough to find your backups and smash them too. All the backup data can be corrupted too.
5. *Privacy and Compliance Challenges:* Lot of solutions are basically constantly collecting or watching everything user does to catch threats, which besides being invading user privacy, it can get issues with stuff like GDPR or HIPAA. So often they might decide your totally legit work is suspicious and block it.

6. Proposed System

Ransomware is just getting more and more by every second. Standard cybersecurity tools cannot protect the files and fails stop the ransomware attack. Once the attack has occurred it's very hard to reverse the process and recover from it. So, here's the plan: a Ransomware Prevention System using Python and some IoT that doesn't wait until your data's locked. Instead, it jumps in, spots trouble in real time, and protects the data so that ransomware cannot attack the system.

The proposed system consists of the following key components:

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM03973
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

1. *Real-time Ransomware Detection:* The Python custom library monitors the file system in real time, keeping an eye on files like all the time. Once the attack occurs the file extensions start changing and the Ransomware Prevention System spots the pattern immediately and instantly it will trigger the .NET Windows Forms app, so you don't have to play detective after the heist.
2. *IoT-Based Network Isolation:* As soon as ransomware is caught in the act, there's no time for negotiation. The system will trigger the ESP8266 IoT by using the VB.NET application isolates the device off the network. Doesn't stop there either, the Ransomware Prevention System disables the network drivers for multi-layer protection, just in case, so that virus doesn't drag the rest of your devices down with it.
3. *Automated Backup and Recovery:* Nobody wants to lose their data which they have worked so hard on. That's why the system is always working in the background, making backups on the regular basis. Once you're isolated from the network after a attack, it asks if you want to roll back and we can just restore and watch your files come back.
4. *Integration with Existing Cybersecurity Measures:* No need to remove your antivirus or whatever's already running. This system can co-exist with an extra layer, behavioral detection plus that mean network cutoff to make ransomware's life miserable. Basically, this setup is like a extra layer for your data, ready to remove any ransomware before it can corrupt the files. No more watching your files get hijacked while your antivirus does its best goldfish impression. Game on.

7. Architectural Design

The architecture of Ransomware Prevention System is built with some actual thought. It integrates the real time monitoring, IOT and Backup and Restore Modules. Everything is inter connected by keeping the purpose of protecting the data without system lag and faster prevention system.

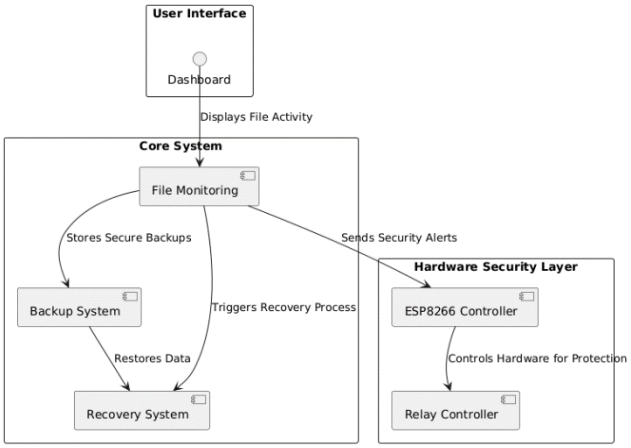

Fig. 1: Architecture Diagram

The user interface it's built in VB.NET on Windows since it is very light weight so it won't cause any system lag and it will be compatible with almost all the Windows Systems. It is made with functionality in mind. The dashboard lets the user examine the multiple settings like protection status, Monitoring Log, Backup and Restore settings and Relay Controlling. Plus, you can dig into threat reports, tweak file monitoring, and set alerts. Almost all the basic functionalities are covered in the user interface for easier usage of antivirus.

The file monitoring layer is digital security that is always on. It's always scanning around the file system with this custom Python toolkit or library. So, if files start vanishing suddenly, or if the files getting renamed or encrypted faster than we think. That's means probably ransomware up to its attack. This system's watching the the really important folders that don't want messed with. Anything suspicious sets off alarms. Then it basically stops everything and alerts the system and VB.NET application.

The IoT-based security layer using an ESP8266 module. If File Monitoring layers finds out that something suspicious is going on in the system then the IoT layer automatically cut off system from the network so that the attack does not spread across that system any further. Keeps the ransomware from system without causing further attack. Plus, meanwhile, it sends alert messages to a remote dashboard, so admins or users can jump in before things really hit the fan.

Ransomware show fake dialog box messages or alert messages to the users for scamming money from the user, The OpenCV layer tracks the dialog boxes or alert messages to prevent the users from sending money to scammers or attacks since most of time the files or data won't be recovered by paying the money.

The security and response layer the does the main process of tracking which ever data is encrypted and recovers it from the backup system for fast recovery process. It also shutdowns all the suspicious activities or process related to the ransomware. This layer is connected with the IoT layer

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 06 | June – 2025 DOI: 10.55041/ISJEM03973
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

make the system isolated from the network to prevent the spread of further attack.

So, the whole architecture is integrated with real time file monitoring, network isolation, backup and restore process to safeguard the files and data of the user. All the layers and inter connected in a unified dashboard to make user experience easier for the user. Plus, the dashboard also shows the status of the monitoring and logs of the data scanned.

8. Modules

The Ransomware Prevention System isn't just another security tool it's made of multiple layers for security modules. The modules work together to safeguard the files by using monitoring, network isolation and various modules. Let's break down all the modules one by one:

1) Dashboard Module

The Dashboard Module is the central point of the Ransomware Prevention System where all the modules are combined and showed to the user for easier user experience. This module provides the details of the system files monitoring logs, monitoring status and all the settings related to the application. The module also contains the features of backups and restores to faster recover and systematic backup process.

2) File Monitoring Module

This module constantly monitors or watches the files and folders for any changes like renaming, encryption, for any modifications done to the files by a virus or ransomware especially. When something suspicious occurs, this module will trigger the IoT module for network isolation process. This module is very important because this module is the starting point of finding the ransomware and safe guarding the files or data.

3) IoT Security Response Module

This Module is used for the network isolation of the affected system to stop the spreading of the ransomware attack. The network will be cut in both hardware and software wise. IoT module is responsible for hardware network isolation by cutting the connection between the router or modem or server and the connected computer system. It uses ESP8226 IoT which controls a relay which will be in the middle of system and network after attack occurs the relay will be triggered to cut of the network.

4) Security and Backup Module

A ransomware application cannot be complete without the backup and restore module since the files encrypted cannot be decrypted easily and the decryption process will take a lot of time so using the systematic or automated timed backups, we can easily restore the files which were affected by the ransomware. This module has features like automated backups for local and cloud-based access.

Altogether, this thing's got layers like a fortress with way too many doors and locks. All the modules ensure the one purpose of safe guarding or protecting the data of the users by using real time monitoring, network isolation, backup and restore modules.

9. Screenshots

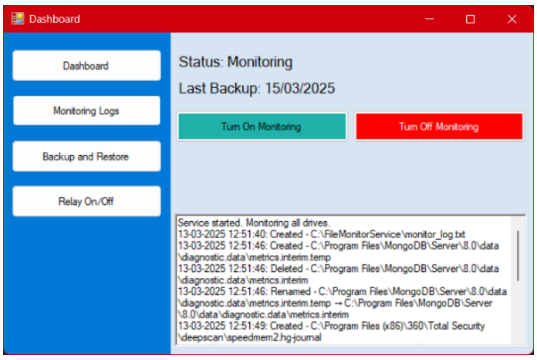

Fig. 2: Dashboard Page

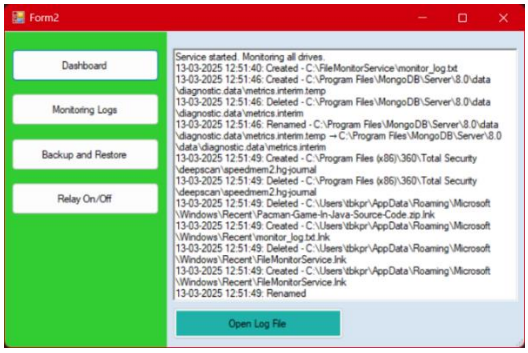

Fig. 3: Monitoring Logs Page

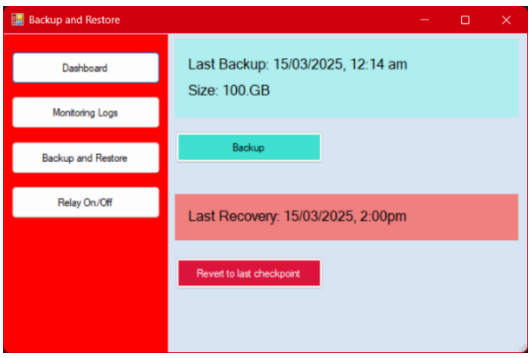

Fig. 4: Backup and Restore Page

10. Top 5 Security Measures for Ransomware Prevention in Modern Systems

Safe guarding the data against the ransomware requires multiple layers or measures for real time monitoring, proactive network isolation mechanism, automated backup and restore mechanism. In this section we will take a look the various

measure of ransomware presentation. This measure ensures that proper protection of files and folders.

1) *File Monitoring System:* This is one of the most important aspects in the application since the files has to monitored in real time for any type changes or modifications done to the files and folders. This is done by a Python script with advances custom library for file monitoring. Since this script is very light weight it does not affect the system performance while monitoring the whole system even for large file system. It provides a robust advantage for file monitoring using python. The script also triggers the IoT modules and disables the network drivers to prevent the spread of the ransomware attack.

2) *Network Isolation Mechanism:* This module is done by the ESP8226 IoT controller since it is the safest IoT device in the industry because of the protocols used in ESP8226 Controller is very secure and it cannot be easily cracked. This mechanism ensures that the network isolation is done perfectly and pro-actively. By cutting of the system from the network we ensure that the spread of the attack prevented by stopping the encryption of the files and stopped

3) *Image-Based Threat Detection System:* Some ransomware likes to flex, plastering your screen with ransom notes or creepy lock screens. Here's where Python's OpenCV flexes back: it keeps snapping screenshots from your desktop, scanning for those ransom demands. If it spots one, it jumps into action maybe shuts down a nasty process, pings you with a warning, the works. It's like having a digital bouncer watching the club doors all night long.

4) *Automated Backup and Recovery System:* Let's face it if you don't have backups, you're basically taping your wallet to your front door and inviting thieves inside. This system keeps your files safely zipped up, away from prying ransomware hands. Something gets hit this module just rolls you back like nothing happened. No panic. No paying ransoms. No embarrassing I-told-you-so's from your IT buddy.

5) *Multi-Layered Security and Encryption System:* Stacking on all the good stuff multi-factor authentication, hardcore encryption, tight-as-heck access controls. Random hackers are not even getting near your files. Everything's locked up, and if something fishy goes down, you get real-time alerts. It's not just defense; it's a fortress. Look, there's no "magic bullet" for ransomware, but throw these five into your arsenal and you'll make the bad guys' lives a whole lot harder.

11. Opportunities Related to Cybersecurity

Cyber threats just keep getting sneakier every year. That means, honestly, there's a gold rush for anybody cooking up new ways to slam the brakes on ransomware. Take this whole "Ransomware Prevention System" built with Python and IoT gadgets that's not just some techie fantasy, it's the sort of solution that's starting to feel less like a luxury and more like a lifeline.

Huge corporations have entire teams propping up their firewalls, washing their hands every time someone sneezes on the internet. But the corner bakery or the local accounting firm are using the same password everywhere and hoping for the best. Yikes. They're just sitting ducks, really. If you've got a tool that can sniff out file hijinks and shut down infected machines before everything melts down – and doesn't cost a fortune – that's a game-changer for the little guys. Gives them a fighting chance, instead of just crossing their fingers and praying nothing explodes.

Governments are always rolling out new rules, waving the stick about data protection. Feels like every month there's a new acronym or compliance checklist to deal with. CERT-In, GDPR, you name it. Well, a system that plugs right into those requirements, automates a bunch of the headaches, and actually keeps up with threat detection as it happens. Yeah, companies are lining up for that. It's like someone finally brought snacks to a three-hour meeting.

Almost everyone is working remotely on at least some days, half of our lives are floating in the cloud, and people want stuff that isn't a pain in the neck to set up. If the Ransomware Prevention System can keep an eye on your files, lock down the network if something sketchy pops up, and maybe even uses OpenCV to visually spot trouble... that's pretty slick. It's like having a guard dog that doesn't sleep and doesn't chew your shoes.

Long story short: this isn't just a niche geek thing. Real-time defense, government compliance, keeping costs down for small businesses – all of that's a massive opportunity. With the way ransomware is exploding, I'd bet my coffee budget demand for this kind of automated protection is heading straight up. If you've ever worried about your stuff getting held hostage, now's the time to jump on this bandwagon.

12. Conclusion

Cyber threats just won't chill. Ransomware is everywhere these days encrypting files, holding people hostage for cash. It's like, if you blink, your inbox might start demanding bitcoin. So yeah, having something that actually keeps an eye out for weird stuff and shuts it down instantly. Total game changer.

This Ransomware Prevention System cooked up with Python, OpenCV, and some IoT wizardry it's not just another security buzzword salad, it's actually doing work. It's always watching your files, clocking anything that smells fishy, and slamming the door on ransomware before it eats your

homework, or your boss's quarterly sales spreadsheet. And with everyone going hybrid or cloud, nobody wants to wake up to "Oops, all your files are gone."

Still, the bad guys aren't just gonna roll over they keep leveling up, dodging the old-school antivirus like they're playing tag. That's why you need something nimble nothing bulky that slows everything down, just smart, sneaky protection that kicks in right when you need it. That's kinda why this system hits different: it spots shady changes, pulls the plug on infected machines, and doesn't get in your way while you're working.

Regulations are getting stricter, people are finally talking more about security, and the big dogs are throwing cash at anything that promises not to let their data get hijacked. Makes sense. At the end of the day, if you've got a simple, user-friendly tool wired with AI and IoT smarts, and it's helping the good guys stay one step ahead. That's the future right there. So, bottom line: this Python + IoT setup isn't just another fancy science project. Real-time monitoring, instant lock-down, clever as heck. Honestly, it just gives people one less thing to freak out about which, considering how wild ransomware's gotten, is worth its weight in gold.

References

1] Skulkin, O. (2022). Incident Response Techniques for Ransomware Attacks: Understand modern ransomware attacks and build an incident response strategy to work through them. Packt Publishing.
2] Khaliq, K., Ab Rahim, N. Z., Hamid, K., Ibrar, M., Ahmad, U., & Ullah, M. U. (2024). Ransomware Attacks: Tools and Techniques for Detection. 2024 2nd International Conference on Cyber Resilience (ICCR). IEEE.
3] Grimes, R. A. (2022). Detecting Ransomware. In Ransomware Protection Playbook (pp. 45–67). Wiley.
4] Grimes, R. A. (2022). Future of Ransomware. In Ransomware Protection Playbook (pp. 210–225). Wiley.
5] Cheon, S. B., Choi, G. Y., & Kim, D. (2023). A Cheating Attack on a Whitelist-based Anti-Ransomware Solution and its Countermeasure. 2023 IEEE International Conference on Consumer Electronics (ICCE). IEEE.
6] Kumar, A., & Sharma, I. (2023). Understanding the Behaviour of Android Ransomware Attacks with Real Smartphones Dataset. 2023 International Conference for Advancement in Technology (ICONAT). IEEE.
7] Singh, R., Singh, S., & Singh, A. (2024). REvil Ransomware. 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET). IEEE.
8] Alvee, S. R. B., Ahn, B., Kim, T., Su, Y., Youn, Y. W., & Ryu, M. H. (2021). Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations. 2021 6th IEEE Workshop on the Electronic Grid (eGRID). IEEE.
9] Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive Survey on Petya Ransomware Attack. 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS). IEEE.
10] Malik, N. A., Delshadi, A. M., Ibrar, M., Hamid, K., Aamir, M., Ahmed, F., & Ahmad, G. (2024). Behavior and Characteristics of Ransomware - A Survey. 2024 2nd International Conference on Cyber Resilience (ICCR). IEEE.
11] FileSystemWatcher Class (System.IO) - Microsoft Learn - https://learn.microsoft.com/en-us/dotnet/api/system.io.filesystemwatcher?view=net-9.0&utm_source=chatgpt.com
12] File System Monitoring Using Windows Service https://srikanthtechnologies.com/articles/dotnet/file_system_monitoring.html?utm_source=chatgpt.com
13] Using FileSystemWatcher in VisualBasic.NET - https://www.youtube.com/watch?v=j2R4lGPjE-Q&utm_source=chatgpt.com
14] Basic Security With ESP8266 - IoT : 8 Steps – https://www.instructables.com/Basic-Security-with-ESP8266/?utm_source=chatgpt.com
15] ESP8266 for IoT: A Complete Guide - https://www.nabto.com/esp8266-for-iot-complete-guide/?utm_source=chatgpt.com
16] Python Watchdog Documentation https://pypi.org/project/watchdog/?utm_source=chatgpt.com
17] Automate Backup with Python Script https://www.geeksforgeeks.org/automate-backup-with-python-script/?utm_source=chatgpt.com
18] Automating Database Backups with Python - https://devops.supportsages.com/automating-database-backups-with-python-a-practical-guide-87a308c9b365
19] Python Backup Script – https://gist.github.com/tompaton/1208368/575dff7831dcb2a03799ceea5c1768ab047e3c72
20] Performing System Restore in Window - https://www.dell.com/support/contents/en-au/videos/videoplayer/how-to-perform-a-system-restore-in-windows-10/6079814806001?utm_source=chatgpt.com