Team Stack Smashers Idea Submission for SIH2021

Need

In today’s time where cybersecurity is a major concern, almost all organizations need secure software on their machines so that their data and network is not compromised. All organizations have authorized software preinstalled on their PC’s/Workstations during system build. If by any chance these softwares get deleted by a staff or infected by some virus, they might have to install freely available ones over the internet. This may pave the way to virus/ spyware/ spamware which may potentially paralyze the network.

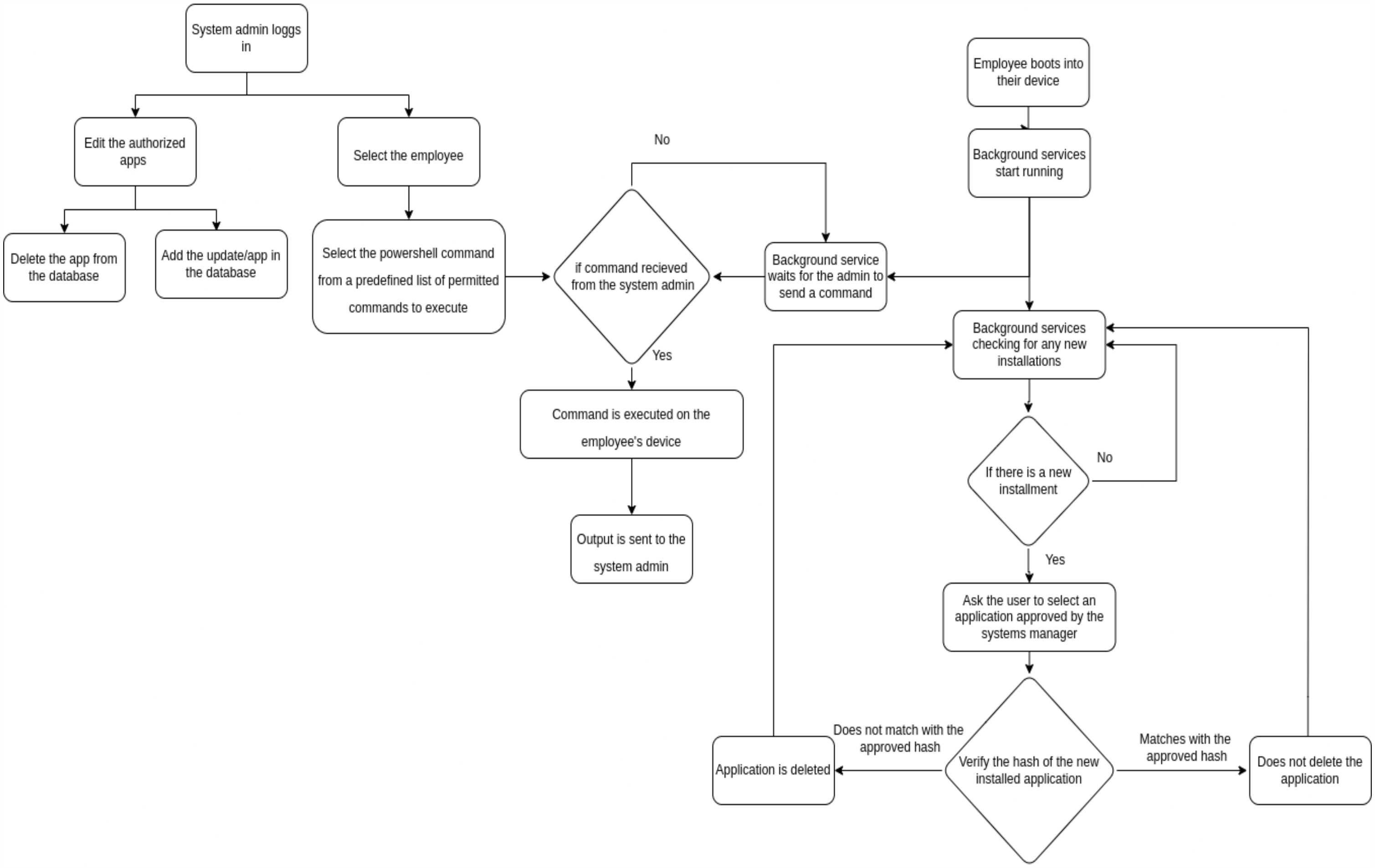
As a result, we must create software (scheduler-based) to track the list of all software installed on PC/Workstations connected to the network and generate a report based on IP addresses. This report can assist administrators in deciding whether to keep or uninstall applications from a specific user's PC.

We need a Remote Monitoring and Management (RMM) tool for managing a computer or a network from a remote location. This tool gives the administrator control over the network which involves installing/deleting software and managing all activities on the systems/network, workstations, servers or endpoints of a client. This tool is needed for a systematic management of clients’ IT requirements since it can help detect issues before they cause critical system failure.

Objectives

- To track the list of all softwares installed in the PC’s attached to the network of an organization, reduce security and compliance headaches, and gain the transparency that is needed across complex and hybrid environments of organizations.
- To have the latest information regarding the inventory of computer CIs (configuration items) of client area, networks, software applications, vulnerabilities reports and georeferences.
- To check the integrity of the software being installed to avoid the installation of malicious software and take immediate action in case of discrepancy.
- To provide a user-friendly web interface capable of visualizing the inventory.
- To facilitate easy and fast-track incident management initiatives in situations where quick action is required.
- Employee privacy and security is given the highest priority in our solution.

Lifecycle Diagram


System admin loggs in
Edit the authorized apps
Select the employee
Delete the app from the database
Add the update/app in the database
Select the powershell command from a predefined list of permitted commands to execute
No
if command recieved from the system admin
Yes
Command is executed on the employee's device
Output is sent to the system admin
Background service waits for the admin to send a command
Employee boots into their device
Background services start running
Background services checking for any new installations
If there is a new installment
No
Yes
Ask the user to select an application approved by the systems manager
Verify the hash of the new installed application
Does not match with the approved hash
Application is deleted
Matches with the approved hash
Does not delete the application

Business Value:

- Around 74% of organizations experienced malware activity that spread from one employee to another, thus increasing the need to protect the devices.[1]
- According to a global survey, 86% of individuals believe that remote monitoring would become more prevalent in the near future. As a result, there is significant business potential[2].
- Unlike other softwares in the market our solution allows the system administrator to only run predefined commands on the employees pc, only used for the security purposes of that device.
- It also verifies the software's integrity, which is done automatically without the administrator's oversight, and if the software appears to be compromised, it is automatically removed. As a result it ensures that employees have a fair share of security.
- Our solution can be used in a variety of settings, ranging from large tech firms to internet cafes.
- The SaaS model allows for revenue to be created by monetizing our software.

[1] https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-report-2021.pdf
[2] https://www.cipd.co.uk/knowledge/work/technology/workplace-technology-employee