Automated critical infrastructures have been a lucrative target for cyber attacks. These systems should be updated and patched as vulnerabilities are found. Also before backing up and restoration, integrity of the backup should be checked. We are developing a blockchain based framework for patch management to enforce security policy and to help in integrity verification of backup before restoration.

**CHALLENGES**
- Tracking Latest update throughout the facility
- Tamper resistance logs
- Minimize downtime

**STAKEHOLDERS**
- Latest patch notification to concerned persons

**IMPLEMENTATION STEPS**
- Patch notification
- Patch Acquisition
- Patch verification
- Patch Testing
- Patch Deployment
- Securing infrastructures
- Time stamped hash verification
- System Restore
- Backing Up
- Compute hash

**PROPOSED ARCHITECTURE**

**ABSTRACT**

The text is about developing a blockchain-based framework for patch management in critical infrastructures to ensure security policy enforcement and integrity verification before restoration.