**SECURING IOT USING BLOCKCHAIN**

|  |  |  |  |
| --- | --- | --- | --- |
| **GUIDE** |  | **STUDENTS NAME** | |
| Ms.P.Abirami | | Aishwarya R | (19DC01) |
|  | | Ragavi N V | (19DC18) |
|  | | Shriehari A C | (19DC23) |

The existing Blockchain-based IoT security solutions do not address the challenges- latency, applicability and resource-constraint. In direct wiretapping attacks, the attacker passively listens to network communications to gain access to private information, such as node identification numbers, routing updates, or application sensitive data. In sensor tampering attack manipulate the sensors to acquire data readings and sensor feed modification to modify the sensor feed and firmware during communications process.

In IoT devices ultrasonic sensor calculates the distance and collects the data, which can be manipulated. Which has a risk of privacy leakage and causes malicious traffic. The authentication system is based on single server architecture in which limitations are in terms of privacy, anonymity and integrity in direct wiretapping attack and DDoS attack.

Our proposed approach works in application and network layer using Hyperledger fabric Blockchain and add on hardware modules which offers a higher level of assurance, low level of assurance comparatively. A Blockchain-based status monitoring system is created for defending against unauthorized software updating in IoT devices. It can be solved using Blockchain based sensor data protection system (SDPS) and privacy aware data sharing using Blockchain VPN. It is filtered by SDN switch on the edge network which ensures synergy with the Blockchain environment and access from the Blockchain information about trustworthy resources and computers. A computer called validator is implemented which checks the IoT device validity using protocol of authentication.

