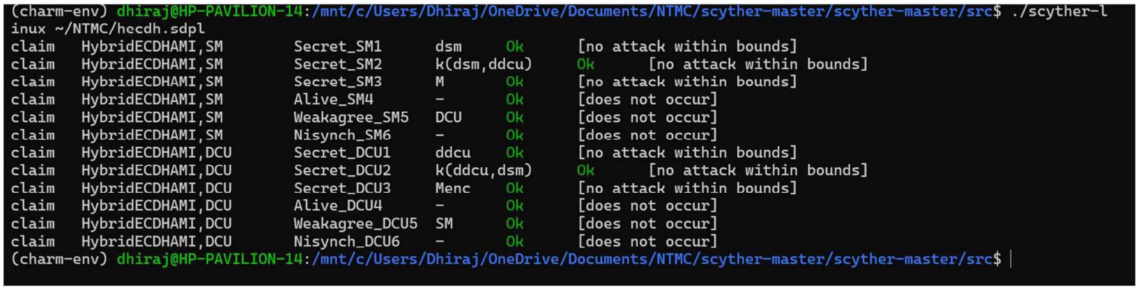
**SCYTHER O/P AND INSTALLATION SCREENSHOTS:**



```
(charm-env) dhiraj@HP-PAVILION-14:/mnt/c/Users/Dhiraj/OneDrive/Documents/NTMC/scyther-master/scyther-master/src$ ./scyther-l
inux ~/NTMC/hecdh.sdpl
claim   HybridECDHAMI,SM        Secret_SM1      dsm     Ok      [no attack within bounds]
claim   HybridECDHAMI,SM        Secret_SM2      k(dsm,ddcu)     Ok      [no attack within bounds]
claim   HybridECDHAMI,SM        Secret_SM3      M       Ok      [no attack within bounds]
claim   HybridECDHAMI,SM        Alive_SM4       -       Ok      [does not occur]
claim   HybridECDHAMI,SM        Weakagree_SM5   DCU     Ok      [does not occur]
claim   HybridECDHAMI,SM        Nisynch_SM6     -       Ok      [does not occur]
claim   HybridECDHAMI,DCU       Secret_DCU1     ddcu    Ok      [no attack within bounds]
claim   HybridECDHAMI,DCU       Secret_DCU2     k(ddcu,dsm)     Ok      [no attack within bounds]
claim   HybridECDHAMI,DCU       Secret_DCU3     Menc    Ok      [no attack within bounds]
claim   HybridECDHAMI,DCU       Alive_DCU4      -       Ok      [does not occur]
claim   HybridECDHAMI,DCU       Weakagree_DCU5  SM      Ok      [does not occur]
claim   HybridECDHAMI,DCU       Nisynch_DCU6    -       Ok      [does not occur]
(charm-env) dhiraj@HP-PAVILION-14:/mnt/c/Users/Dhiraj/OneDrive/Documents/NTMC/scyther-master/scyther-master/src$
```

## Gaps, Drawbacks, and Proposed Solutions

Although the proposed framework demonstrates strong resistance against a wide range of attacks, certain limitations persist. One major drawback lies in the reliance on a centralized Certificate Authority (CA), which introduces a single point of failure within the Advanced Metering Infrastructure (AMI). This issue becomes particularly critical when the system scales to millions of Smart Meters (SMs), as any compromise or downtime of the CA could disrupt the entire network's trust chain. Furthermore, the absence of a time-based validation parameter (Δt) increases the system's vulnerability to Denial-of-Service (DoS) and replay attacks. Another limitation is the lack of adaptability of the protocol to heterogeneous AMI components — since AMI encompasses various devices such as smart meters, data concentrator units (DCUs), home area network (HAN) devices, and other lightweight IoT nodes, deploying a computationally heavy protocol uniformly across all devices may not be feasible.

To address these issues, we propose the following enhancements inspired by the hybrid cryptographic approach discussed in the reference paper:

Decentralization via Identity-Based Encryption (IBE):

Implementing an IBE-based key management scheme for SMs, DCUs, and other entities can effectively eliminate the single point of failure introduced by the centralized CA. In IBE, public keys are derived directly from unique identities (such as device IDs or MAC addresses), which reduces the dependency on certificate issuance and management. This approach simplifies trust establishment while maintaining strong cryptographic assurance. For example, each smart meter could generate its public key from its unique identifier, with the Private Key Generator (PKG) distributed across multiple nodes to avoid centralization.

Enhanced Scalability and Lightweight Registration:

The introduction of IBE also improves scalability since it minimizes the registration overhead compared to traditional PKI systems. Only an initial identity verification and limited private key extraction are required, making the system more efficient for large-scale AMI deployments. For instance, new devices can be seamlessly added to the network with minimal communication overhead, thereby supporting dynamic grid expansion.

Lightweight Protocol Design for Constrained Devices:

Given that not all AMI components possess the same computational capabilities, we propose developing a lightweight variant of the protocol for resource-constrained devices (e.g., HAN sensors or smart plugs), while retaining the existing hybrid protocol for more capable units like SMs and DCUs. This layered approach ensures both security and efficiency across the network. Techniques such as hash-based message authentication or elliptic curve cryptography (ECC) with smaller key sizes can be employed to maintain adequate protection without imposing excessive computational burden.