**Module implementation**

1. **Mobile Device layer:**

This layer is composed of hierarchical SDVs mobile devices (MDs) connected to the blockchain. Each MD has a blockchain account that can access the network and offload tasks to the cloud server. –

1. **Edge computing layer:** It consist of wireless access point (AP) or base station (BS) for wireless communication with mobile devices. Main controller (MC) are used to perform tasks, while lightweight edge servers are used to handle instant data. This layer be able to supply low-latency computing services at network edge. But, for complicated computing resource, the edge server forwards them to the resource-rich cloud server over a wired line to prevent overloading tasks on the edge side. Furthermore, edge servers are also considered to be blockchain entities, which ensure security by establishing trusted communications with cloud nodes and MDs on the blockchain network. All transactions and offloading actions in the offloading system are recorded by the blockchain and then broadcast to the edge server to reach a common agreement.
2. **Cloud control layer:** This layer includes powerful computing and storage functions that can solve the complex computing tasks of local vehicle network equipment. In the ECCO system, the cloud also includes a blockchain entity network manager that controls access to all vehicles, which is used for smart contract admins and miners for mining transactions.
3. **Dynamic Update of the Cipher text**

The dynamic update procedure to the ciphertext can be regarded as a rerun of step (c) based on a new binary encoding matrix. It is particularly designed to realize dynamic security protection. The flexibility to choose the new binary encoding matrix endows a tradeoff between efficiency and security, which enhances the adaptability to different application scenarios. It is worthwhile to note that using invertible matrices in step (a) and (c) for encryption is essentially a type of K-block cipher. The novel idea in this paper is that we can find an efficient way to get the feasible and dynamically updatable encryption matrix based on NC.