ABSTRACT :

Cloud security, also mentioned as cloud computing security, is that the practice of protecting cloud-based data, applications, and infrastructure from cyber attacks and cyber threats. Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and the way it's used. Cloud database systems are subject to several equivalent threats that affect cloud technology. Block chain technology may be a distributed ledger with records of knowledge containing all details of the transactions administered and distributed among the nodes present within the network. All the transactions carried out in the system are confirmed by consensus mechanisms, and the data once stored cannot be altered. This paper first analyses the security threats in the cloud, privacy protection issues associated with cloud computing across all stages of the data life cycle, then briefly introduces the block chain technology, summarizes the classification of the current block chain technology to solve the cloud data security problems, and defects existed. Finally, a new cloud forensic storage architecture model based on block chain technology is proposed to protect the cloud data, which lays a foundation for our future research.

KEYWORDS : Cloud computing Block chain , Data security , Data management Integration of Cloud and Block chain