Chapter 7
IoT Application-enabled Deep Learning Model With Secure ECC-Based Cloud Data Storage Optimization Strategy for Data Deduplication

Manjunath Singh H.
https://orcid.org/0009-0007-6891-3614
UVCE, India

R. Tanuja
UVCE, India

ABSTRACT

Due to the development of the "Internet of Things (IoT)," a huge quantity of data is transferred to the cloud architecture. As a consequence, expenses and storage charges are associated with cloud servers. Storage capacity can be enhanced by implementing a deduplication technique to spot duplicate information. Both cryptography and deduplication are carried out using the full hash values of the information chunks. The deduplication systems are vulnerable to file threats. So, we developed an effective optimal key-based deduplication model. The proposed model uses attributes including filename, size, block name, size, type of file, and data pattern for deduplication. The "Long Short-Term Memory (LSTM)" model is introduced for effective deduplication performance. The LSTM model separates the attributes and deduplicated attributes once the data file is not duplicated. Once it is

DOI: 10.4018/979-8-3373-4672-4.ch007

proved that the data are deduplicated, the edge node (client) enciphers the data by utilizing the Optimal Key-Based Elliptical Curve Cryptography (OK-ECC). Further, it passes the data to the cloud system.

INTRODUCTION

Commercial efficiency and security can be increased by implementing data-driven approaches through the IoT (Patra et al., 2021). The automation of factories was previously centralized, but using the IoT, it is currently independently managed. For a more productive and secure generation, the industrial data is processed using a semi-trusted cloud server (Shukla et al., 2023). Nearly all the time, the duplicates in the outsourced IoT data raise storage costs. The outsourced information must be deduplicated before being stored on a cloud server to lower this overhead (Kumar and Shantala, 2020). During de-duplication, private information should not be transferred to cloud architecture. Consequently, to satisfy the security and data management needs of the IoT (Licaj et al., 2024), a successful de-duplication solution is used that can maintain access control and privacy and safeguard the data being transmitted from other cyber-attacks (Periasamy and Latha, 2021).

The majority of prior research has used deduplication algorithms directly at third parties. Consequently, for redundancy verification, all of the created data is immediately transferred to cloud storage (Muthunagai and Anitha, 2022). The blocks of information will be discarded when they repeatedly appear. It causes substantial communication expenses when sending all the information to cloud storage for redundancy evaluations. Convergent key encryption produces a private key for encryption using one-way hashing, which vast deduplication algorithms use (Vignesh and Preethi, 2022). The secret keys generated from the hash values encrypt the data blocks. The encryption texts and convergence keys are produced since the hash values are consistent for identical information blocks. These encrypted texts are subsequently used to detect duplication and are denied access to cloud storage (Sharma and Saini, 2020). The most fundamental de-duplication method compares the newly received file from the corresponding person with the actual file to safeguard a connection between the source file and the file holder on the cloud server (Raja et al., 2024). The main drawback is that the competitors might easily extrapolate the contents of the data that has been outsourced (Li et al., 2017). Convergent cryptography is used on cloud servers to safeguard and maintain data uniqueness. The uploaded file is encrypted with the convergent method of encryption using the file's hash sequence (Yeh and lin, 2018). Every single digest is reviewed against the owner's digests. Developing equivalent digests during cross-data repetition causes vulnerability to brute force attacks and tag mismatches (fu et al., 2018). To overcome the challenges,