

18. The device of claim 16, wherein the step C comprises:

extracting the verification ciphertext from the version control file and decrypting the extracted verification ciphertext using a public key generated in advance by a key generator, to obtain the corresponding plaintext encrypted value of the verification ciphertext, where the public key is matched with a private key in a key pair to which the public key belongs, and the public key is prestored in a corresponding preset type file of the application.

19. The device of claim 18, wherein the processing unit is further configured for executing the system for preventing accessed data from being tampered with to cause the device to perform the following operations:

building accessed data of the application, and encrypting the configuration file of the accessed data according to the preset encryption method, to obtain the corresponding plaintext encrypted value of the configuration file;

encrypting the obtained plaintext encrypted value using the private key generated in advance by the key generator, to obtain the corresponding verification ciphertext of the plaintext encrypted value; and

putting the verification ciphertext in the version control file of the accessed data, and distributing the accessed data, the version control file carrying the verification ciphertext, as well as the configuration file to the data server.

20. The device of claim 16, wherein the preset encryption method comprises a message digest algorithm.