**A] Techniques for cryptographic key generation using biometric data of a user**

In this model techniques are described for cryptographic key generation based on biometric data associated with a user. Biometric data, such as fingerprint(s) and/or heartbeat data, may be collected using one or more sensors in proximity to the user which could be analysed to generate a cryptographic key. In some implementations, the key may be employed by the user to access data, access certain feature(s) of an application, authenticate the user, digitally sign document(s), and/or for other purpose(s).

**B] POOFster: a secure mobile text message and object sharing application, system, and method.**

The invention described here is directed to a secure text messaging and object sharing mobile application that provides encryption, digital rights management (DRM) of the text and of the attachments, the capability of sending SMS, RCS, MMS, IM or blockchain communications, the capability of attaching documents, photos and so forth, the capability of interfacing with a user's contacts application, and that operates in both Android and iOS environments.

**C] Authentication test for testing simulation data on driverless vehicle**

The method realizes authentication to the driverless vehicle simulation testing data, which may ensure reliability of the authentication result while reducing the time and cost consumed for the authentication. This data authentication method, comprises of response to receiving a request submitted to authentication nodes in a system for authenticating that a vehicle passes self-driving scene testing, verifying the authentication request, the authentication request containing simulation data regarding self-driving testing of the vehicle in a simulated driving scene.

**D] Methods and apparatus to manage timing of an operational node in a block chain network**

In a method for operating a node in a blockchain network, a node in the network automatically determines whether a new block has been committed to a blockchain in the network. It is a data processing system with technology to enable the data processing system to operate as a node in a blockchain network automatically determining whether a new block has been committed to a blockchain in a blockchain network for which the data processing system is a node.

**E]** **Parallel assurance of blockchain signatures to verify authenticity of signed elements**

A parallel assurance of blockchain signatures ("PABS") record includes a cryptographic message, comprising the block identifier and the hash, and is signed using a second digital signature algorithm, which is different from the first digital signature algorithm. Integrity and origin authenticity of the signed block content are verified by verifying the digital signature of the first cryptographic message.