

CLAIMS:

1. A system for controlling access to vehicular data comprising:

a vehicle device (200) configured to:

collect vehicular data of a vehicle, wherein each vehicular data is tagged to an identity, wherein each identity is represented as a node on a nodular tree structure, whereby the nodular tree structure includes a root node associated with the vehicle;

encrypt each collected vehicular data using a corresponding child key, wherein each corresponding child key is generated based on a node tagged to each vehicular data and a root key corresponding to the root node;

transmit the encrypted vehicular data and their tagged nodes to a cloud server (105);

the cloud server (105) configured to:

receive and store the encrypted vehicular data and their tagged nodes;

a service device (200) configured to:

send a request to the cloud server (105), wherein the request includes a time period such that upon receiving the request, the cloud server (105) retrieves encrypted vehicular data having tagged nodes that correspond to the time period;

receive the retrieved encrypted vehicular data from the cloud server (105) together with their tagged nodes, wherein each node represents a node on the nodular tree structure;

determine a group of sub-nodes that is common to the tagged nodes of the received encrypted vehicular data;

request for an aggregated key for the group of common sub-nodes; and

generate a child key for each received encrypted vehicular data based on the requested aggregated key and the node tagged to each received encrypted vehicular data, wherein each generated child key is used to decrypt a corresponding encrypted vehicular data.

2. The system according to claim 1 wherein the nodular tree structure further comprises a first sub-node associated with a class element, a second sub-node associated with a large time unit and a third sub-node associated with a small time unit;

wherein a hierarchical relationship of the first, second and third sub-nodes is defined by:

the first sub-node being connected to the root node, the second sub-node being connected to

the first sub-node, the third sub-node being connected to the second sub-node;

whereby each identity is represented as a node on the nodular tree structure by:

determining a class element of the collected vehicular data;

acquiring a current time comprising a large time unit and a small time unit;

identifying a node in the nodular tree structure corresponding to the identity based on the determined class element and the acquired current time.

3. The system according to claim 2, wherein the generating of each corresponding child key based on the node tagged to each vehicular data comprises:

ascertaining a first sub-node, a second sub-node, and a third sub-node of a node tagged with each collected vehicular data, whereby for each node:

generating a first sub-node key using the root key, the first sub-node and the root node;

generating a second sub-node key using the first sub-node key, the second sub-node, the first sub-node and the root node; and

generating a child key using the third sub-node, the second sub-node, the first sub-node, the root node and the second sub-node key.

4. The system according to any one of the claims 1 to 3, further comprising a mobile device (200);

the mobile device (200) configured to:

retrieve a shared password, whereby the shared password is known to the vehicle device (200); and

encrypt the shared password and communicate the encrypted shared password to the vehicle device (200) to negotiate a shared cryptographic key for establishing secure communications between the mobile device (200) and the vehicle device (200); and the vehicle device (200) is configured to:

encrypt the root key using the shared cryptographic key; and

communicate the encrypted root key to the mobile device (200).

5. The system according to claim 4 wherein the mobile device (200) is configured to:

in response to receiving a request for the aggregated key for the group of common sub-nodes, generate the aggregated key for the group of common sub-nodes based on the root key and the hierarchical relationship of sub-nodes in the group of common sub-nodes; and

communicate the generated aggregated key to the service device (200).

6. The system according to claim 1 wherein the vehicle device (200) is configured to:

in response to receiving a request for the aggregated key for the group of common sub-nodes, generate the aggregated key for the group of common sub-nodes based on the root key and a hierarchical relationship of sub-nodes in the group of common sub-nodes; and

communicate the generated aggregated key to the service device (200).

7. The system according to any one of claims 2 to 5 wherein the large time unit comprises a unit of time that is larger than a unit of time of the small time unit.

8. A vehicle device (200) provided in a vehicle for generating encrypted vehicular data, the vehicle device (200) comprising:

a processor (205); and

a non-transitory media (225) readable by the processor (205), the non-transitory media (225) storing instructions that when executed by the processor (205), cause the processor (205) to:

collect vehicular data of the vehicle, wherein each vehicular data is tagged to an identity, wherein each identity is represented as a node on a nodular tree structure, whereby the nodular tree structure includes a root node associated with the vehicle;

encrypt each collected vehicular data using a corresponding child key, wherein each corresponding child key is generated based on a node tagged to each vehicular data and a root key corresponding to the root node; and

transmit the encrypted vehicular data and their tagged nodes to a cloud server (105).

9. The vehicle device (200) according to claim 8 wherein the nodular tree structure further comprises a first sub-node associated with a class element, a second sub-node associated with a large time unit and a third sub-node associated with a small time unit;

wherein a hierarchical relationship of the first, second and third sub-nodes is defined by:

the first sub-node being connected to the root node, the second sub-node being connected to

the first sub-node, the third sub-node being connected to the second sub-node;

whereby instructions for directing the processor (205) to represent each identity as a node on the nodular tree structure further comprises: for each identity, instructions for directing the processor (205) to:

determine a class element of the collected vehicular data;

acquire a current time comprising a large time unit and a small time unit;

identify a node in the nodular tree structure corresponding to the identity based on the determined class element and the acquired current time.

10. The vehicle device (200) according to claim 8, wherein the instructions for directing the processor (205) to generate each corresponding child key based on the node tagged to each vehicular data comprises:

instructions for directing the processor (205) to:

whereby for each tagged node, ascertain a first sub-node of the tagged node, a second sub-node of the tagged node, and a third sub-node of the tagged node,

generate a first sub-node key using the root key, the first sub-node and the root node;

generate a second sub-node key using the first sub-node key, the second sub-node, the first sub-node and the root node; and

generate a child key using the third sub-node, the second sub-node, the first sub-node, the root node and the second sub-node key.

11. The vehicle device (200) according to any one of claims 8 to 10, further comprising: instructions for directing the processor (205) to:

in response to receiving a request for the aggregated key for the group of common sub-nodes, generate the aggregated key for the group of common sub-nodes based on the root key and a hierarchical relationship of sub-nodes in the group of common sub-nodes; and

communicate the generated aggregated key to the service device (200).

12. A service device (200) for controlling access to vehicular data of a vehicle, whereby each vehicular data is collected and tagged to a node in a nodular tree structure, and the

collected vehicular data is encrypted by a vehicle device (200) provided in a vehicle and stored in a cloud server (105), the service device (200) comprising:

a processor (205); and

a non-transitory media (225) readable by the processor (205), the non-transitory media (225) storing instructions that when executed by the processor (205), cause the processor (205) to:

send a request to the cloud server (105), wherein the request includes a time period such that upon receiving the request, the cloud server (105) retrieves encrypted vehicular data having tagged nodes that correspond to the time period;

receive the retrieved encrypted vehicular data from the cloud server (105) together with their tagged nodes, wherein each node represents a node on the nodular tree structure;

determine a group of sub-nodes that is common to the tagged nodes of the received encrypted vehicular data;

request for an aggregated key for the group of common sub-nodes; and

generate a child key for each received encrypted vehicular data based on the requested aggregated key and the node tagged to each received encrypted vehicular data, wherein each generated child key is used to decrypt a corresponding encrypted vehicular data.

13. The service device (200) according to claim 12 wherein the nodular tree structure further comprises:

a first sub-node associated with a class element, a second sub-node associated with a large time unit and a third sub-node associated with a small time unit,

wherein a hierarchical relationship of the first, second and third sub-nodes is defined by:

the first sub-node being connected to the root node, the second sub-node being connected to

the first sub-node, the third sub-node being connected to the second sub-node;

whereby instructions for directing the processor (205) to tag each collected vehicular data to a node further comprises:

for each node, instructions for directing the processor (205) to:

determine a class element of the collected vehicular data;

acquire a current time comprising a large time unit and a small time unit;

identify a node in the nodular tree structure corresponding to the identity based on the determined class element and the acquired current time.

14. The service device (200) according to any one of claims 12 or 13, wherein the instructions for directing the processor (205) to generate a child key for each received encrypted vehicular data based on the requested aggregated key and the node tagged to each received encrypted vehicular data comprises:
 - for each tagged node, instructions for directing the processor (205) to:
 - generate a first sub-node key for a first sub-node of the tagged node based on the aggregated key, the root node and the first sub-node;
 - generate a second sub-node key for a second sub-node of the tagged node based on the first sub-node key, the root node, the first sub-node and the second sub-node; and
 - generate the child key for the tagged node based on the second sub-node key, the root node, the first sub-node, the second sub-node and a third sub-node of the tagged node.
15. The service device (200) according to any one of claims 12 or 13, wherein the instructions for directing the processor (205) to generate a child key for each received encrypted vehicular data based on the requested aggregated key and the node tagged to each received encrypted vehicular data comprises:
 - for each tagged node, instructions for directing the processor (205) to:
 - generate a second sub-node key for a second sub-node of the tagged node based on the aggregated key, the root node, a first sub-node of the tagged node and the second sub-node; and
 - generate the child key for the tagged node based on the second sub-node key, the root node, the first sub-node, the second sub-node and a third sub-node of the tagged node.
16. The service device (200) according to any one of claims 12 or 13, wherein the instructions for directing the processor (205) to generate a child key for each received encrypted vehicular data based on the requested aggregated key and the node tagged to each received encrypted vehicular data comprises:
 - for each tagged node, instructions for directing the processor (205) to:
 - generate the child key for the tagged node based on the aggregated key, the root node, a first sub-node of the tagged node, a second sub-node of the tagged node and a third sub-node of the tagged node.
17. The service device (200) according to any one of the claims 12 to 16, further comprising:
 - instructions for directing the processor (205) to:

retrieve a shared password from the vehicle device (200), whereby the shared password is known to the vehicle device (200); and

encrypt the shared password and communicate the encrypted shared password to the vehicle device (200) to negotiate a shared cryptographic key for establishing secure communications between the service device (200) and the vehicle device (200).

18. The service device (200) according to claim 17 further comprising: instructions for directing the processor (205) to:

in response to the request for the aggregated key for the group of common sub-nodes, generate the aggregated key for the group of common sub-nodes based on the root key and the hierarchical relationship of sub-nodes in the group of common sub-nodes.