WE CLAIM:

1. A method of securing a computing device, wherein the computing device is configured to store an access key in a storage location in order for the computing device to operate in an operational mode and the computing device is configured to prevent operation in the operational mode without the access key, the method comprising:

the computing device retrieving the access key from an external computing device in response to provision of identification data by a user and storing the access key in the storage location;

the computing device operating in said operational mode in response to receipt and storage of the access key;

the computing device removing the access key from the storage location in response to an event indicative of the end of the operational mode,

wherein removing the access keyfrom the storage location comprises deleting the access key, and

wherein removing the access key comprises storing the access key on a further computing device in data communication with the first computing device.

2. A method as claimed in claim 1, wherein the external computing device is a remote server in data communication with the computing device.

3. A method as claimed in claim 1, wherein the external computing device is a local computing device in local data communication with the computing device.

4. A method as claimed in claim 3, wherein the local computing device is a mobile phone.

5. A method as claimed in claim 1, wherein removing the access key from the storage location comprises overwriting the access key with alternative data.

6. A method as claimed in claim 1, wherein the further computing device is in local data communication with the first computing device.

7. A method as claimed in claim 1, wherein the further computing device is a remote computing device in data communication with the first computing device.

8. A method as claimed in claim 7, wherein the computing device is connected to at least a first remote computing device and a second remote computing device via a network and the method comprises storing a first part of the access key on the first remote computing device and a second part of the access key on the second remote computing device.

9. A method as claimed in claim 8, wherein the computing device is connected to a third remote computing device and the method comprises storing one of the first part or the second part of the access key on the third remote computing device.

10. A method as claimed in claim 8, wherein the network is a peer-to-peer network.

11. A method as claimed in claim 1, wherein the computing device comprises volatile memory and the method comprises storing the access key only in the volatile memory during the operational mode, whereby the access key is cleared from the volatile memory when the power supply to the computing device is interrupted.

12. A method as claimed in claim 1, wherein the step of removing the access key is automatic in response to said event and is effected without user intervention.

13. A method as claimed in claim 1, wherein the event comprises receipt of a command from a further computing device in data communication with the first computing device.

14. A method as claimed in claim 1, wherein the event comprises a change of location of the computing device.

15. A method as claimed in claim 1, wherein the event comprises closing an application running on the computing device.

16. A computing device configured to operate in accordance with the method of claim 1.

Dated this 13th day of June 2014.

Abhishek Sen
IN/PA Reg No: 980
Of S. MAJUMDAR & CO.
(Applicant's Agent)

~~CLAIMS~~**WE CLAIM:**

1. A method of securing a computing device, wherein the computing device is configured to store an access key in a storage location in order for the computing device to operate in an operational mode and the computing device is configured to prevent operation in the operational mode without the access key, the method comprising:

the computing device retrieving the access key from an external computing device in response to provision of identification data by a user and storing the access key in the storage location;

the computing device operating in said operational mode in response to receipt and storage of the access key;

the computing device removing the access key from the storage location in response to an event indicative of the end of the operational mode,

wherein removing the access keyfrom the storage location comprises deleting the access key, and

wherein removing the access key comprises storing the access key on a further computing device in data communication with the first computing device.

2. A method as claimed in claim 1, wherein the external computing device is a remote server in data communication with the computing device.

3. A method as claimed in claim 1, wherein the external computing device is a local computing device in local data communication with the computing device.

4. A method as claimed in claim 3, wherein the local computing device is a mobile phone.

~~5. A method as claimed in any preceding claim, wherein removing the access keyfrom the storage location comprises deleting the access key.~~

~~6.~~5. A method as claimed in ~~any preceding~~ claim 1, wherein removing the access key from the storage location comprises overwriting the access key with alternative data.

~~7. A method as claimed in any preceding claim, wherein removing the access key from the storage location comprises storing the access key in a different, secure storage location on the computing device.~~

~~8.~~6. A method as claimed in ~~any preceding~~ claim 1, wherein ~~removing the access key comprises storing the access key on a~~the further computing device is in local data communication with the first computing device.

~~9.~~7. A method as claimed in ~~any preceding~~ claim 1, wherein ~~removing the access key comprises storing the access key on~~ the further computing device is a remote computing device in data communication with the first computing device.

~~10.~~8. A method as claimed in claim ~~9~~7, wherein the computing device is connected to at least a first remote computing device and a second remote computing device via a network and the method comprises storing a first part of the access key on the first remote computing device and a second part of the access key on the second remote computing device.

~~11.~~9. A method as claimed in claim ~~10~~8, wherein the computing device is connected to a third remote computing device and the method comprises storing one of the first part or the second part of the access key on the third remote computing device.

~~12.~~10. A method as claimed in claim ~~8 10 or 11~~, wherein the network is a peer-to-peer network.

~~13.~~11. A method as claimed in ~~any preceding~~ claim 1, wherein the computing device comprises volatile memory and the method comprises storing the access key only in the volatile memory during the operational mode, whereby the access key is cleared from the volatile memory when the power supply to the computing device is interrupted.

~~14.~~12. A method as claimed in ~~any preceding~~ claim 1, wherein the step of removing the access key is automatic in response to said event and is effected without user intervention.

~~15.~~13. A method as claimed in ~~any preceding~~ claim 1, wherein the event comprises receipt of a command from a further computing device in data communication with the first computing device.

~~16.~~14. A method as claimed in ~~any preceding~~ claim 1, wherein the event comprises a change of location of the computing device.

~~17.~~15. A method as claimed in ~~any preceding~~ claim 1, wherein the event comprises closing an application running on the computing device.

~~18.~~16. A computing device configured to operate in accordance with the method of ~~any preceding~~ claim 1.

~~19. Computer software which configures a computing device to operate in accordance with the method any of claims 1 to 14.~~

Dated this 13th day of June 2014.

Abhishek Sen
IN/PA Reg No: 980
Of S. MAJUMDAR & CO.
(Applicant's Agent)