

Claims

1. An access management system for controlling access to a plurality of entry points each secured by an electronic lock, comprising
 - a user management module configured to provision access rights to an authorized user associated with the electronic lock, wherein a first factor authentication data is configured to be associated with the authorized user;
 - at least one server arranged in wireless communication with the access management system and each electronic lock associated with the each of the plurality of entry points;
 - wherein the at least one server is configured to:
 - receive, by the server, an input first factor authentication data from the authorized user;
 - determine if the input first factor authentication data corresponds with the first factor authentication data associated with the authorized user of the electronic lock;
 - generate, by the server, a second factor authentication data configured for transmission to a user device of the authorized user, in response to the input first factor authentication data matching the first factor authentication data associated with the authorized user;
 - receive, by the server, an input second factor authentication data from the authorized user;
 - perform a second factor authentication of the user, wherein the second factor authentication includes determining that the input second factor authentication data corresponds with the second factor authentication data;
 - release, by the electronic lock, a locking mechanism into an open position for granting entry to the authorized user of the entry point, in response to the input second factor authentication data matching the second factor authentication data generated by the server.
2. The access management system according to claim 1, further comprising a grant

access module configured to assign an authorized time period to the authorized user, wherein the authorized time period defines a first time period when the authorized user is authorized to unlock the electronic lock and a second time period when the authorized user is not authorized to unlock the electronic lock.

3. The access management system according to claim 1, further comprising a role management module configured to assign a predetermined role to the authorized user, wherein the predetermined role is associated with a predetermined authorized time period when the authorized user is authorized to unlock the electronic lock.

4. The access management system according to claim 1, further comprising a lock management module configured to create a predetermined virtual perimeter around an intended destination, wherein the electronic lock is activated to receive a first factor authentication data when the electronic lock is within the predetermined virtual perimeter around the intended destination, and deactivated to receive the first factor authentication data when the electronic lock is outside the predetermined virtual perimeter around the intended destination.

5. The access management system according to claim 1, wherein the first factor authentication data includes any one of the following: a unique passcode, a biometric signature or a secret key.

6. The access management system according to claim 1, wherein the input first factor authentication data is received by a gateway device in wireless communication with the electronic lock, wherein the gateway device is configured for transmitting the input first factor authentication data to the application server.

7. The access management system according to claim 1, wherein the one or more electronic lock each includes a memory and a wireless transceiver in data communication with the memory, wherein the memory is configured to synchronize

the plurality of first factor authentication data with the application server at a predetermined time interval.

8. A method for controlling access to a plurality of entry points each secured by an electronic lock controlled by a lock controller having a memory, the method comprising the steps of:

storing a plurality of first factor authentication data, wherein each of the plurality of first factor authentication data is configured to be associated with an authorized user of one or more of the electronic locks;

receiving, by an application server configured for wireless communication with the electronic lock and a user device of the authorized user, an input first factor authentication data from the authorized user;

determining if the input first factor authentication data corresponds with the first factor authentication data associated with the authorized user of one or more of the electronic locks;

generating, by the application server, a second factor authentication data configured for transmission to the user device of the authorized user, in response to the input first factor authentication data matching the first factor authentication data associated with the authorized user of the one or more electronic locks;

receiving, by the application server, an input second factor authentication data from the authorized user;

performing a second factor authentication of the authorized user, wherein the second factor authentication includes determining that the input second factor authentication data corresponds with the second factor authentication data;

releasing, by the electronic lock, a locking mechanism into an open position for granting entry to the authorized user, in response to the input second factor authentication data entered by the authorized user matching the second factor authentication data.

9. The method according to claim 8, wherein the first factor authentication data

includes any one of the following: a unique passcode, a biometric signature or a secret key.

10. The method according to claim 9, wherein the biometric signature includes any one of the following: a fingerprint information or a facial profile information.

11. The method according to claim 8, wherein the plurality of first factor authentication data are stored in a lock user database of the application server.

12. The method according to claim 8, wherein the input first factor authentication data is received by a gateway device in wireless communication with the electronic lock, wherein the gateway device is configured for transmitting the input first factor authentication data to an application server.

13. The method according to claim 8, wherein the input first factor authentication data is received by an application server configured for wireless communication with the electronic lock, wherein the wireless communication further includes any one of the following: Sigfox, Lora, or Narrow-Band IoT technologies.

14. The method according to claim 8, wherein the electronic lock further includes a wireless transceiver in data communication with the memory, wherein the memory is configured to synchronize the plurality of first factor authentication data stored on the application server at a predetermined time interval.

15. The method according to claim 8, wherein the input first factor authentication data is received by the user device of the authorized user and transmitted wirelessly to the electronic lock through short-range wireless communication technology.

16. The method according to claim 8, wherein the user device includes any one of the following: a mobile device, an electronic token or a software token.

17. The method according to claim 8, wherein the input second factor authentication data includes any one of the following: a one-time passcode, a time-based one-time passcode, a biometric signature or a secret key.

18. The method according to claim 8, wherein the input second factor authentication data is received by the user device of the authorized user and transmitted wirelessly to the electronic lock through short-range wireless communication technology.

19. The method according to claim 8, wherein the input second factor authentication data is configured for transmission to the user device via any one of the following communication channels: Short-Messaging System, Email, or Whatsapp.

20. The method according to claim 8, further comprising the steps of:

logging an event in the lock controller, wherein the event corresponds to a date and time stamp of an instance when the input first factor authentication data does not match the first factor authentication data associated with the authorized user of the one or more electronic locks; and

sending an alarm notification to the authorized user of the one or more electronic locks.