CLAIMS

1. A system for transferring data between a plurality of nodes through a bridging module (8), wherein the system comprising:

at least a first node (11) for receiving and transmitting data;

at least a second node (12) for receiving and transmitting data; and

the bridging module (8) establishes communication between said at least a first node (11) and said at least a second node (12) and regulates data transmitted to and received from said at least a first node (11) and said at least a second node (12);

wherein the bridging module (8) receives data from said at least a first node (11) in a format type incongruent with a required format in said at least a second node (12), maps the data into the required format such that the mapped data is readable by said at least a second node (12), and transmits the mapped data to that of said at least a second node (12);

wherein the data transmission is executed in a transient data transmission process.

2. A system according to claim 1, wherein said at least a first node (11) comprises any one or in a combination of an extraction module (101) for extracting data therefrom, an encryption module (102) for encrypting data, a decryption module (103) for decrypting data, a transmitter (104) for transmitting data, a receiver (105) for receiving data

3. A system according to claim 1, wherein said at least a second node (12) comprises any one or in a combination of an extraction module (201) for extracting data therefrom, an encryption module (202) for encrypting data, a decryption module (203) for decrypting data, a transmitter (204) for transmitting data, a receiver (205) for receiving data.

4. A system according to claim 1 or 2, wherein the bridging module (8) comprises a processor (21) for regulating the data transmission on per session basis.

5. A system according to claim 1, wherein the bridging module (8) regulates the data transmitted for maintaining consistency of the data transmission from said at least a first node (11) and said at least a second node (12).

6. A system according to claim 1, wherein the bridging module (8) comprises an encryption module (301) for encrypting data, a decryption module (302) for decrypting data, a transmitter (303) for transmitting data, a receiver (304) for receiving data, or in any combination thereof.

7. A system according to claim 1, wherein the data is protected during transmission.

8. A system according to claim 1, wherein the data is protected during data mapping.

9. A system according to claim 1, wherein data security is applied during transmission.

10. A system according to claim 1, wherein data security is applied during data mapping.

11. A system according to claim 1, wherein said at least a first node (11) transmits data by the steps of:

extracting data for transmission;

encrypting the extracted data; and

transmitting the encrypted data.

12. A system according to claim 1, wherein the bridging module (8) transmits data by the steps of:

receiving encrypted data;

decrypting the data;

mapping the decrypted data to a corresponding data;

encrypting the mapped data; and

transmitting the encrypted data.

13. A system according to claim 1, wherein said at least a second node (12) receives and processes data by the steps of:

receiving encrypted data;

decrypting the received data;

validating the decrypted data; and

processing the decrypted data.

14. A system according to claim 13, wherein said at least a second node (12) transmits an acknowledgement message to said at least a first node (11).

15. A system according to claim 13, wherein said at least a second node (12) transmits a status update message to said at least a first node (11).

16. A system according to claim 1, wherein the bridging module (8) comprises a risk management module to protect the data from attacks.

17. A system according to claim 1, wherein the data transmitted from said at least a first node (11) is encrypted through cryptographic key pairs.

18. A system according to claim 17, wherein the cryptographic key pairs authenticates users.

19. A system according to claim 1, wherein the system uses a corresponding key to decrypt the data.

20. A system according to claim 1, wherein the system comprises integrity means for delivering data.

21. A system according to claim 1, wherein the system is configured to prevent data breach.

22. A system according to claim 1, wherein the system operates in a virtual machine environment.