CLAIMS:

1. A system for securing a series of data files, the system comprising:

a transformation module comprising sets of reduced row echelon form (RREF) matrices that have been transformed from the series of data files, whereby the series of data files have been mapped to the sets of RREF matrices, the transformation module being configured to:

retrieve an altered data file from the system and transform the altered data file into an altered set of RREF matrices;

map the altered data file to the altered set of RREF matrices, and provide the altered set of RREF matrices to a trained artificial neural network (ANN) module;

the trained ANN module configured to:

determine if the altered set of RREF matrices comprise malicious activity, whereby when it is determined that the altered set of RREF matrices comprise malicious activity, the altered set of RREF matrices and the altered data file are moved to a virtual secure area in a memory of the system;

a clustering module configured to:

retrieve, using a backpropagation module, variations of the altered set of RREF matrices from the sets of RREF matrices;

cluster the retrieved variations of the altered set of RREF matrices and the altered set of RREF matrices to identify sets of RREF matrices that contain malicious activity;

provide the identified sets of RREF matrices that contain malicious activity to the trained ANN module, whereby the trained ANN module is configured to identify a type of malicious activity associated with the identified sets of RREF matrices; and

secure data files mapped to the identified sets of RREF matrices that contain malicious activity according to the type of malicious activity associated with the data files as identified by the trained ANN module.

2. The system according to claim 1, wherein the transformation of the altered data file into the altered set of RREF matrices by the transformation module comprises the transformation module being configured to:

convert the altered data file into an intermediate data frame, wherein the intermediate data frame comprises a multimedia data frame or a character-based data frame;

transform the intermediate data frame into a set of matrices using a first linear function; and

transform the set of matrices into the altered set of RREF matrices.

3. The system according to claim 1 whereby the clustering module is further configured to provide sets of RREF matrices that do not contain malicious activity to the transformation module, whereby the transformation module is further configured to convert the provided sets of RREF matrices into data files, and map the data files to the provided sets of RREF matrices.

4. The system according to claim 1 whereby the variations of the altered set of RREF matrices comprise related sets of RREF matrices that have differing timestamps.

5. The system according to claim 1, whereby the mapping of the series of data files to the sets of RREF matrices, and the mapping of the altered data file to the altered set of RREF matrices is done for each data file or each altered data file by applying a hashing function to an address of the data file and to a contextual metadata layer of the data file, and using a result of this hashing function to link each data file to each sets of RREF matrices.

6. The system according to claim 1 whereby the trained ANN module is further configured to further train the neural network in the ANN module based on the identified sets of RREF matrices that contain malicious activity.

7. The system according to claim 1, wherein the transformation of the series of data files into the sets of RREF matrices by the transformation module comprises the transformation module being configured to:

convert each of the data files into an intermediate data frame, wherein the intermediate data frame comprises a multimedia data frame or a character-based data frame;

transform the intermediate data frame into a set of matrices using a first linear function; and

transform the set of matrices into a set of RREF matrices.

8. A method for securing a series of data files using a system comprising a transformation module that comprises sets of reduced row echelon form (RREF) matrices that have been transformed from the series of data files, whereby the series of data files have been mapped to the sets of RREF matrices, the method comprising the steps of:

retrieving, using the transformation module, an altered data file from the system and transforming the altered data file into an altered set of RREF matrices;

mapping, using the transformation module, the altered data file to the altered set of RREF matrices, and providing the altered set of RREF matrices to a trained artificial neural network (ANN) module;

determining, using the trained ANN module, if the altered set of RREF matrices comprise malicious activity, whereby when it is determined that the altered set of RREF matrices comprise malicious activity, the altered set of RREF matrices and the altered data file are moved to a virtual secure area in a memory of the system;

retrieving, using a backpropagation module, variations of the altered set of RREF matrices from the sets of RREF matrices;

clustering, using a clustering module, the retrieved variations of the altered set of RREF matrices and the altered set of RREF matrices to identify sets of RREF matrices that contain malicious activity;

providing, using the clustering module, the identified sets of RREF matrices that contain malicious activity to the trained ANN module, whereby the trained ANN module is configured to identify a type of malicious activity associated with the identified sets of RREF matrices; and

securing, using the clustering module, data files mapped to the identified sets of RREF matrices that contain malicious activity according to the type of malicious activity associated with the data files as identified by the trained ANN module.

9. The method according to claim 8, wherein the transforming of the altered data file into the altered set of RREF matrices comprises:

converting, using the transformation module, the altered data file into an intermediate data frame, wherein the intermediate data frame comprises a multimedia data frame or a character-based data frame;

transforming, using the transformation module, the intermediate data frame into a set of matrices using a first linear function; and

transforming, using the transformation module, the set of matrices into the altered set of RREF matrices.

10. The method according to claim 8 whereby the method further comprises the step of:

providing, using the clustering module, sets of RREF matrices that do not contain malicious activity to the transformation module, whereby the transformation module is further configured to convert the provided sets of RREF matrices into data files, and map the data files to the provided sets of RREF matrices.

11. The method according to claim 8 whereby the variations of the altered set of RREF matrices comprise related sets of RREF matrices that have differing timestamps.

12. The method according to claim 8, whereby the mapping of the series of data files to the sets of RREF matrices, and the mapping of the altered data file to the altered set of RREF matrices is done for each data file or each altered data file by applying a hashing function to an address of the data file and to a contextual metadata layer of the data file, and using a result of this hashing function to link each data file to each sets of RREF matrices.

13. The method according to claim 8 whereby the method further comprises the step of training the neural network in the ANN module based on the identified sets of RREF matrices that contain malicious activity.

14. The method according to claim 8, wherein the transforming of the series of data files into the sets of RREF matrices by the transformation module comprises the steps of:

converting, using the transformation module, each of the data files into an intermediate data frame, wherein the intermediate data frame comprises a multimedia data frame or a character-based data frame;

transforming, using the transformation module, the intermediate data frame into a set of matrices using a first linear function; and

transforming, using the transformation module, the set of matrices into a set of RREF matrices.