Semiconductor Optoelectronics
ISSN: 1001-5868

TO SECURE THE ASSOCIATION RULES WITH THE HELP OF PLAYFAIR CIPHER ENCRYPTION USING TRANSPOSITION MAPPING AND DES ALGORITHM

M. Malathi
Research Scholar, PG and Research Department of Computer Science, Government Arts College (Autonomous), Nandanam, Chennai-600035.
Email- malathimano918@gmail.com

M. Rameshkumar
Associate Professor & Head, PG and Research Department of Computer Science, Government Arts College (Autonomous) , Nandanam, Chennai-600035.
Email-proframeshkumar@gmail.com

ABSTRACT:
Nowadays, Data mining plays a crucial role in our day to day life. It helps to mine informative information to gain knowledge from the data‟s. It‟s simple known as „Knowledge Discovery‟. In this paper, encrypt the Association Rules with the help of Play fair encryption algorithm with Ceasor cipher encryption algorithm. Using double columnar Transposition mapping to convert our plaintext into more powerful cipher text with help multiple times of processing. Finally the DES Symmetric Encryption Algorithm is used to improve the security of the data. In this paper we will discuss about that how our plaintext is securely convert into cipher text with the help of mentioned algorithms. We can Analyse the accuracy and efficient of security level using this Algorithm.
Key Points: Data Mining, DES Algorithm, Association rule, Multiple Transposition, Play fair Algorithm, Ceasor cipher.

INTRODUCTION

Data Mining is used to sort large data sets, which can help to find the relationships of the data to solve a business problems. It is with the help of data analysis. In other words, data mining is the process of discovering knowledge from data. Predicting future decisions is made easier with it[1]. Identifying valuable information from large data sets is accomplished through a number of steps, starting with data collection and ending with visualization. Analysing a target data set using data mining techniques can result in descriptions and predictions. Classification and regression methods are also used to classify and cluster data, and to identify outliers for a variety of purposes, like spam detection.

Play fair cipher was the first digraph substitution cipher encryption algorithm. It is also called Play fair square or wheatstone algorithm. It is used to encode a message. In this encryption process the Brute force attack does not affect it. All alphabetic characters are supported by this

algorithm[2]. Ceasor cipher is one of the easiest and simplest encryption process so we use this algorithm to process our cipher text again. Only one short key is used for processing this encryption process.

The use of association rule mining enables the discovery of interesting associations and relationships between large datasets of data. The frequency in which a transaction occurs for a given item set can be determined by this rule. An important technique used by large companies to show associations between items is Market Based Analysis. Retailers are then able to identify consumer patterns between items they frequently purchase together. The occurrence of one item in a transaction can be predicted by the occurrence of others in the transaction based on the occurrence of other items[3]. Transposition technique, one of the main cryptographic technique. It converts our plaintext into cipher text for each round. By rearranging plaintext units according to a regular system, transposition ciphers produce ciphers texts that are permutations of plaintext. The multiple rounds of columnar transposition technique, process the data in more than once.

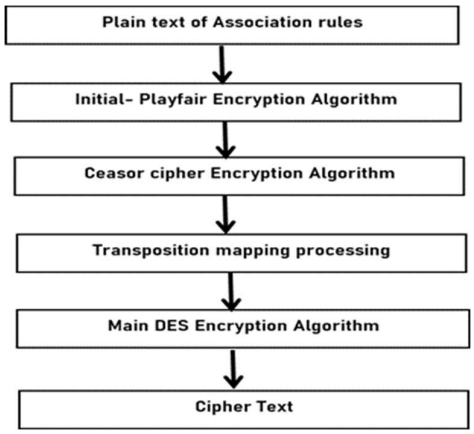
A symmetric key block cipher algorithm, the Data Encryption Standard (DES), uses symmetric key encryption. An algorithm using 56 bits of key size is called the DES algorithm. With help of this key, the DES processes a block of 64-bit plain text and generates a block of 64-bit cipher text. By using the same key, it can process encryption and decryption of data[4]. All
U.S. government financial transactions involving electronic funds transfers must use the DES algorithm. The DES process has a several number of steps to encrypt. There is a variation in the number of rounds based on the size of the key used.

EXISTING RESEARCH

In Data Mining, security of data is one of the major problems. There are many algorithms and techniques are followed to secure the association rule without entering into a data leakage. These Algorithms are used to encrypt the data and performed some activities to prevent the association rule data mining. In our Existing system[[5], the association rules are encrypt with initial stream cipher encryption with dynamic mapping to improve security and follow modified AES algorithm to improve the efficiency and performance of the data. DES Algorithm is also used to encrypt the association rules with adding fake patterns. But it also have some disadvantages, in our proposed system we will add some additional processing methods to make our association rules more powerful. So we use one of the important cryptographic encryption algorithm to improve the efficiency much faster than that of the Existing[6].

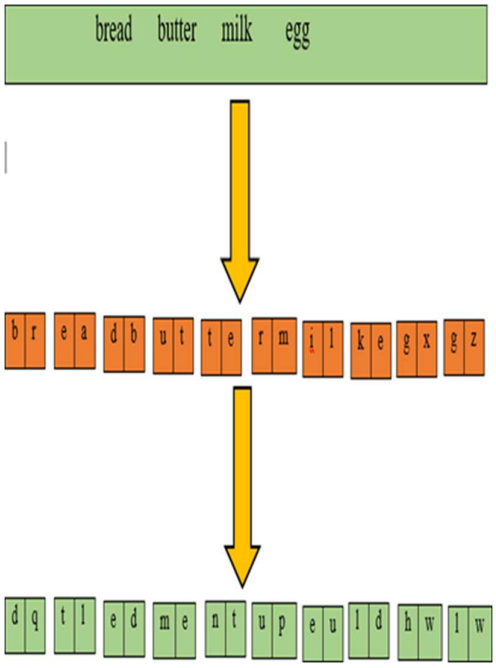
PROPOSED RESEARCH

In this proposed system, we can analyze and predict the security of data using the Play fair cipher Encryption with the help of ceasor cipher, following Transposition mapping to increase the security of the pattern[7]. Additionally DES symmetric Algorithm is used to improve the efficiency and processing time of the association rule. First we perform the initial encryption to convert our plain text into cipher text and perform transposition mapping. Atlas we apply DES algorithm to improve our association rules becomes more secure.



INITIAL PLAY FAIR ENCRYPTION PROCESS

In the initial stage of this paper discuss about the Play fair cipher Encryption Algorithm. In the starting stage, Play fair cipher is used to encrypt our data. It is a manual symmetric encryption. It is a digraph substitution cipher. Security of data is one of the important factors in the today‟s world. In Play fair cipher encryption process, it gives more security of our data and substitution are very easy to perform. The process of decoding cipher without knowing key[8]. It generate 5*5 key square, to encrypt a plaintext. The matrix contains alphabets that acts as the key for encryption of the plaintext. Pair of Alphabets can be encrypted by Play fair Algorithm. The pairs cannot be made with same letter, break that particular letter into single and add Bogus(x) letter. If our plaintext is odd, Z is added to the last one. Below diagram illustrate how Play fair algorithm works on single association rules.

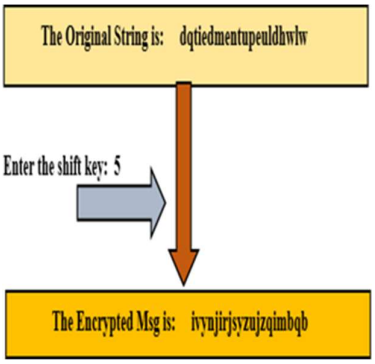


CEASOR CIPHER ENCRYPTION ALGORITHM

Ceasor cipher is also known as shift cipher encryption algorithm. At the next level of adding

security of our data, this paper handling ceasor cipher algorithm to encrypt the cipher text came from the previous stage. This particular process substitutes a fixed number of alphabet letters for every letter in the text. For encrypting the plaintext, this algorithm proposed the equation of En(x)=(x+n)mod

26. Our data is encrypted below using the ceasor cipher.



TRANSPOSITION CIPHERING

Next stage of our encryption process is Transposition ciphering. It is very efficient and useful for data transposition. In this stage our cipher text is encrypted by multiple roundsAn algorithm that consists of rows of plain text messages organized into grids of rectangles with a predefined size is used in this algorithm. The plaintext is read by column manner. The obtained results of round 1 is repeated as many times as desire. The execution of the algorithm is perform more than once. This process keeps on going until the specified condition fails[9]. The final message that we obtain after the last round is the cipher text that is sent to the receiver. Below figure demonstrate how the columnar transposition with multiple rounds works.

For Example, Let"s take 5 column and assign 1,3,5,2,4 is an order of our process.

b	r	e	a	d
b	u	t	t	e
r	m	i	l	k
e	g	g		

Cipher text → **bbreetigdekrumgati**

b	b	r	e	e
t	i	g	d	e
k	r	u	m	g
a	t	i		

Cipher text → btkabirtrguiedmeeg

→ ..... n times

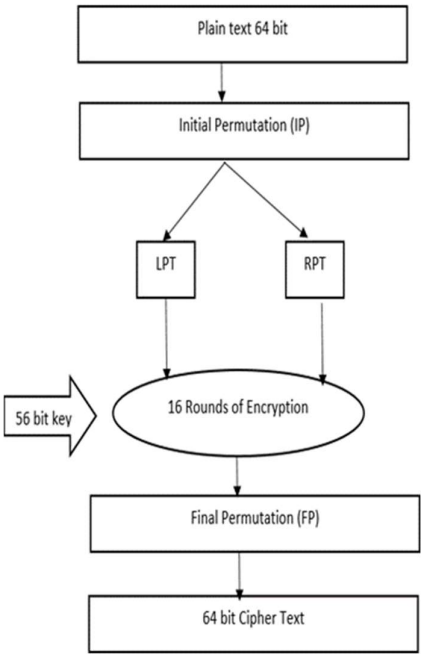
It will process more than once until the specified condition fails. In our encrypted data is shown

below:

```
Please enter the message you wish to encrypt/decrypt below:
 >> ivynjirjsyzujzqimbqb

Double Columnar Transposition
Please enter the key:
 >> 5,6
Encrypted Message: jziyqsbvzbriiqjmnjyu_
```

THE MAIN DES ENCRYPTION ALGORITHM

The next step will involve applying the DES Algorithm after the first three steps are completed. This improves the level of security and time. With the help of a key, plaintext is converted into cipher text. This increases the security of our encryption process. It is based on the Feistel block cipher.



The 64 bit plaintext block is processed under Initial Permutation (IP). For example, the Initial Permutation replaces the first bit of our plain text block with 48th bit and second bit is replaced with 28th position and so on. Next, the initial permutation block is split into two types: Left Plain Text (LPT) and Right Plain Text (RPT).

There are 16 rounds of encryption process are performed on each LPT and RPT. During 16 rounds of encryption, it perform five stages. These are: Key transformation, Expansion Permutation, S-Box Permutation, P-Box Permutation, XOR and Swap. Finally the left plaintext and right plaintext are combined and handed over to Final Permutation (FP). The result

will produce the desired 64 bit cipher text. So the gotten results show their good improvement and security level. Our data is encrypted below using the DES Algorithm.

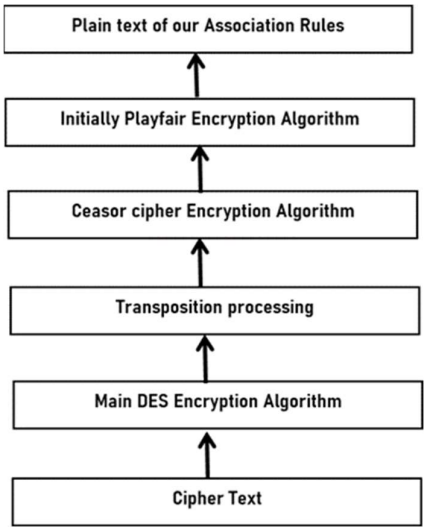
```
Enter the message to be encrypted : jxiyysbvrzbxiiqjmxjyu
Enter a key of 8 length (64-bits) (characters or numbers only) : af1324bc

Encrypted Ciphertext is : '\x9a\x1f2A\x045¶'ÌX§\x9b^ôIÿ3Ò\x1a0\x98æ\x0cÓ\x7f'
Decrypted plaintext is  : jxiyysbvrzbxiiqjmxjyu
```

When executing cipher text decryption, the above four steps of encryption process will be work in reverse manner.

RESULT ANALYSIS:

The proposed approach is implemented in python programming language. It performed on a sample combinations of items. In the first stage of encryption process, our proposed gives minimum time to implement than existing. Below figures shows how our implementation of proposed system works.

Existing:



Proposed:

```
print('The CPU usage is: ', psutil.cpu_percent(4))

print('RAM memory % used:', psutil.virtual_memory()[2])
print('RAM Used (GB):', psutil.virtual_memory()[3]/1000000000)
time.sleep(1)

# program body ends

# end time
end = time.time()

# total time taken
print(f"Runtime of the program is {end - start}")

if __name__ == '__main__':
    main()
```

```
Input your message: breadbuttermilkegg
Input a key: association
Encrypt or decrypt a message?(1,0): 1
/q+{D_3gRR][z[b~pg
Press enter to exit.
The CPU usage is:  9.3
RAM memory % used: 82.5
RAM Used (GB): 3.341164544
Runtime of the program is 15.885865926742554
```

```
# program body ends

# end time
end = time.time()

# total time taken
print(f"Runtime of the program is {end - start}")
```

```
Key text: association
Plain Text: breadbuttermilkegg
CipherText: dqtiedmentupeuldhwlw
enter the textdqtiedmentupeuldhwlw
enter the shift key2
the original string is : dqtiedmentupeuldhwlw
the encripted msg is: fsvkgfogpvwrgwntjyny
The CPU usage is:  7.6
RAM memory % used: 85.4
RAM Used (GB): 3.46017792
Runtime of the program is 12.761083602905273
```

Existing:

```
print('RAM memory % used:', psutil.virtual_memory()[2])
print('RAM Used (GB):', psutil.virtual_memory()[3]/1000000000)
time.sleep(1)

# program body ends
end = time.time()

# total time taken
print(f"Runtime of the program is {end - start}")

if __name__ == '__main__':
    main()
```

```
Input your message: cola, milk
Input a key: abc
Encrypt or decrypt a message?(1,0): 1
n}z.%Ep(tN
Press enter to exit.
The CPU usage is:  4.6
RAM memory % used: 84.9
RAM Used (GB): 3.4407424
Runtime of the program is 14.773526191711426
```

Proposed:

```
time.sleep(1)

# program body ends

# end time
end = time.time()

# total time taken
print(f"Runtime of the program is {end - start}")
```

```
Key text: abc
Plain Text: colamilk
CipherText: dnqfogpf
enter the textdnqfogpf
enter the shift key4
the original string is : dnqfogpf
the encripted msg is: hrujsktj
The CPU usage is:  8.0
RAM memory % used: 83.0
RAM Used (GB): 3.361411072
Runtime of the program is 11.804523944854736
```

CONCLUSION

Encryption techniques are used to secure our data from unknown attackers. One of the most important aspects of data mining is preserving the privacy of association rule mining. A rule mining algorithm is used to generate the results of this paper. Four encryption techniques are used to generate the results. These dynamic techniques gives a good security improvement of our data. The DES Algorithm is used to adding additional security of our data from association rules. When using this method, the efficiency of run time is increased at the starting stage when compared to existing.

REFERENCES:

[1] M. Hussein, A. El-Sisi and Nabil Ismail " Fast Cryptographic PrivacyPreserving Association Rules Mining on Distributed Homogenous Data Base, Knowledge-Based Intelligent Information and Engineering Systems, Lecture Notes in Computer Science, Volume 5178/2008, pp. 607-616 2008.

[2] R.. S. Mohammed, E.. M. Hussein and Jinan. R. Mutter, "A novel technique of privacy-preserving association rule mining", Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) – IRAQ (9-10) May 2016.

[3] S. B. Sadkhan ; F. H. Abdulraheem, "A proposed ANFIS evaluator for RSA cryptosystem used in cloud networking", 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT).

[4] Enaas M, Hussein ; Russeen M, Hussain, "Encryption of Association Rules Using Modified Dynamic Mapping and Modified (AES) Algorithm", 2019 International Conference of Computer and Applied Sciences (1st CAS2019) Mustansiriyah University, Education College, Computer Science Department, Baghdad, Iraq.

[5] W. K. Wong, D. W. Cheung, E. Hung,
B. Kao, and N. Mamoulis, "Security in outsourcing of association rule mining," in Proc. Int. Conf. Very Large Data Bases, 2007, pp. 111-122.

[6] M. Kantarcioglu and C. Clifton, "Privacy-preserving distributed mining of association rules on horizontally partitioned data," IEEE Trans. Knowledge Data Eng., vol. 16, no. 9, pp. 1026-1037, Sep. 2004.

[7] S. J. Rizvi and J. R. Haritsa, "Maintaining data privacy in association rule mining", in Proc. Int. Conf. Very Large Data Bases, 2002.

[8] A. Evfimievski, R. Srikant, R. Agrawal, J. Gehrke, "Privacy Preserving Mining of Association Rules", Information System, 2004.

[9] Ms. Rani Yashwant Mankar, 2 Prof. Anup Gade 3 Prof.Rajesh Babu, "Association Rules Generation of Outsourced Transaction Data with Privacy-Preserving using Paillier Encryption", Proceedings of the International Conference on Smart Electronics and Communication (ICOSEC 2020) IEEE Xplore ISBN: 978-1-7281-
5461-9

[10] Hyeong-jin kim, Jae-Hwan Shin, Young-ho song, Jae-woo chang" Privacy – Preserving Association rule mining Algorithm for Encrypted Data in Cloud Computing" 2019 IEEE 12th International Conference on Cloud Computing (CLOUD)