Optimal Test Mirroring (OTM)

Dr.N.Rajkumar[1], Dr.S.N.Sivanandam[2], J. Stanly Thomas[3]

[1]Professor and Head, Department of CSE, New Horizon College of Engineering, Bangalore, Karnataka, India
[2]Professor and Head, Department of CSE, PSG College of Technology, Coimbatore, Tamilnadu, India
[3]Research Scholar, Dept of Computer Applications, Periyar University, Salem, Tamilnadu, India

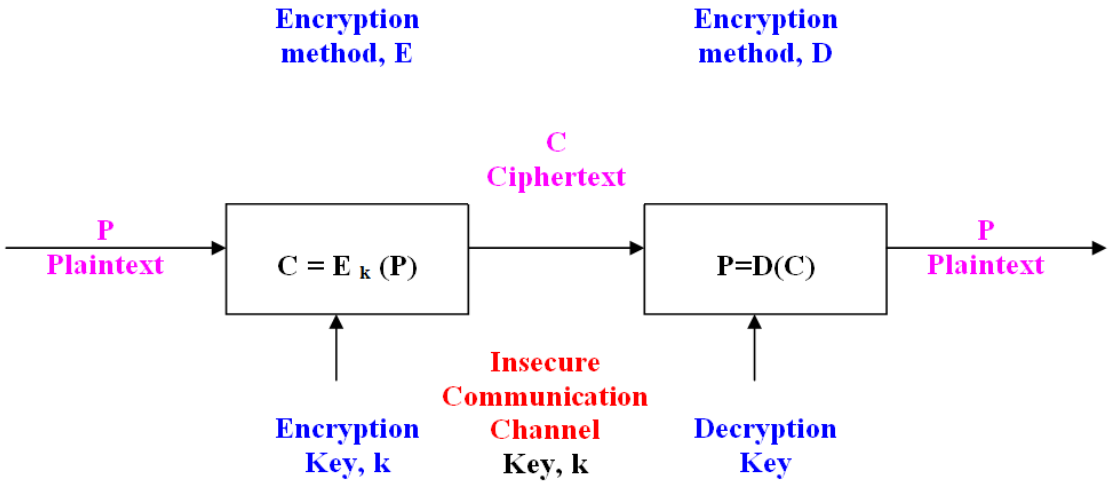
Abstract
One way of strengthen security system in radar system is to encrypt sensitive records and messages in transit and in storage [1]. Many algorithms roaming for cryptography in secured world. However, administrator may suffer because of delay in data deciphering. While closely watches this delay we found security path and poor database mining are the two primary reasons for the delay. Therefore, we proposed the new algorithm that dealt with highly protective and healthy data sharing. For this, we used Data mining Association Rule with distributive procedure to normalize a data and database[3]. This algorithm plays with three vital rolls such as instant data capturing, data mirroring to maintain security levels and storing of data logs in different location for process in next cycle. This algorithm tests with 1, 00,000 data that completes an entire process with 1.27 Milliseconds. This approach entirely overcomes the delay in Data Detect Algorithm (DDA).

Key words:
Data Mining, Association Rules, optimal test mirroring, cryptography

1. Introduction

The association Rule is a classical problem in the Data mining, artificial intelligence and theoretical literature and is used to find the similar groups of rewards in very large datasets. The association Rule is used for similarity search, customer segmentation, pattern recognition, trend analysis, classification, and cryptography. The method has been studied inconsiderable detail by both statistics and database communities for different domains of data [1], [2], [3], [4], [5], [6].The basic model of a cryptography system in illustrated in the following figure. The unenciphered text is called the “Plaintext” or the clear text. It can be encrypted using some encryption method parameterized by a key. The result is called “cipher text”. The cipher text may be stored or transmitted via the communication medium, such as wires and radio links, or – more – traditionally – by a messenger. Plaintext can be obtained by decrypting the enciphered message using the decryption key. A cryptographic system that uses the same key for both encryptionand decryption is said to be “symmetric”. In “asymmetric” schemes, different keys are used at the two ends.

The increased confidence in the integrity of systems that use encryption is based on the notion that cipher text should be very difficult to decipher without knowledge of the key.



Manuscript received August 5, 2008
Manuscript revised August 20, 2008

2. General Cryptography

1) **Limit$_0$ Receive $_0$ = time(input)**
2) **Repeat for all n:(1..capacity)**
   Limit $_n$=Receive n -1
   Receive $_n$ =Limit n –1
3) **Output=t-1 (Limit $_{capacity}$ Receive $_{capacity}$)**

2.1 Algorithm (Proposed)

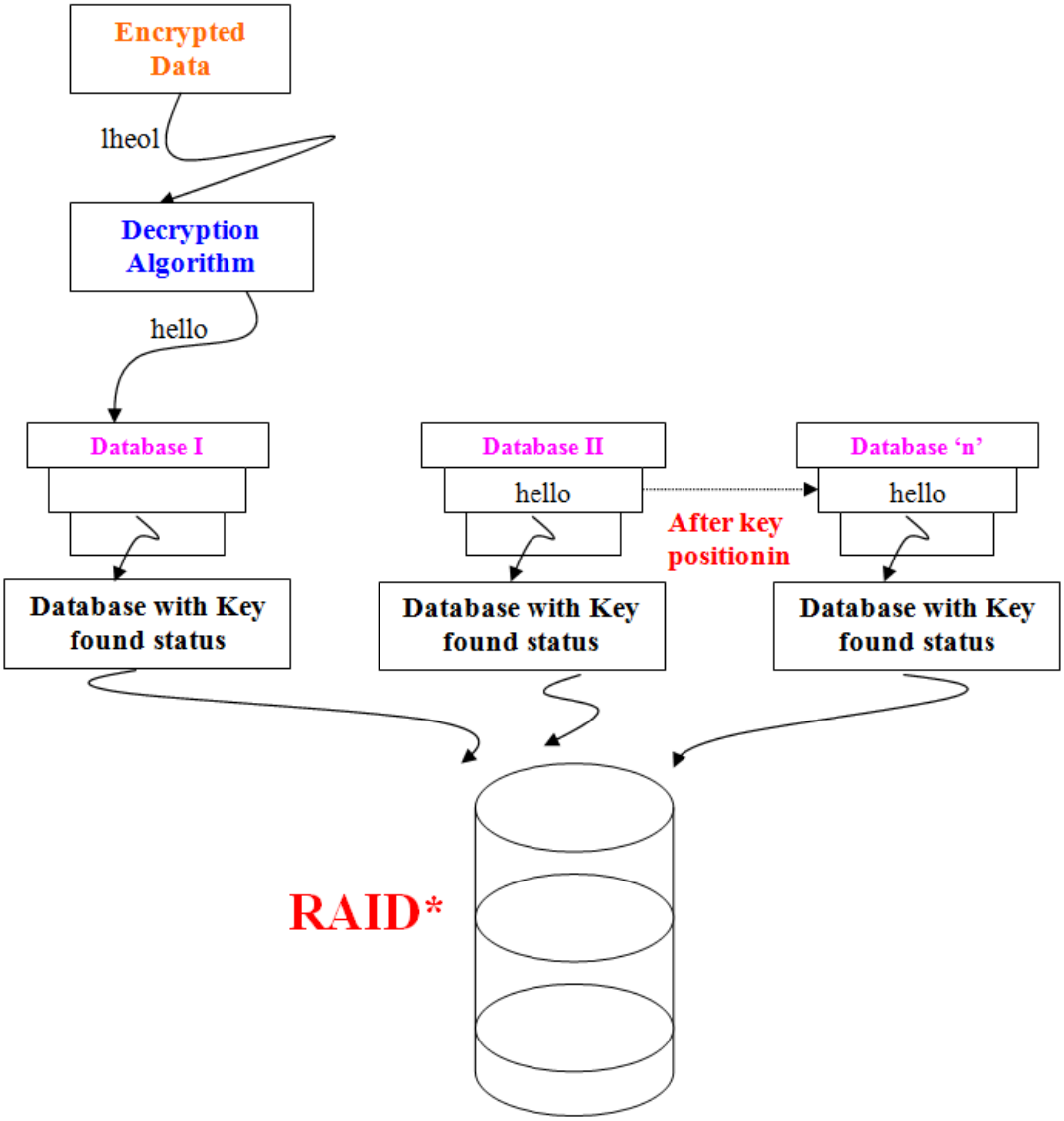
```
module key_analysis

        Key:variable ;
        begin
                buffer,dump : array

[1..capacity][1..capacity] of data;
                        r_input,c_input,  row,col  :
(1..capacity);

        in: user_input;
        flag: test(capacity)
        procedure k_search (pdata:data);
                        begin
                                if  r_input=capacity
then search col;
                                {search  from  first
col}{mirroring}

        dump[r_input][c_input]=buffer[r_input][c_input];
                                        if  in=
buffer[r_input][c_input]

        flag:=1;

        r_input:=r_input –1;

c_input=c_input +1;
                                else  if
c_input=capacity then search row;
                                {search  from  first
row}{mirroring}

        dump[r_input][c_input]=buffer[r_input][c_input];
                                        if  in=
buffer[r_input][c_input]

        flag:=1;

        r_input:=r_input +1;

        c_input=c_input -1;

                        end; {k_search}

                        Procedure b_disp (var cdata:
data);
                        begin
                                forall row,col
                                        disp
dump[r_input][c_input];
                        end; {b_disp}

                        procedure  k_store  (var
cdata:data);
                        begin
                                {Random storing}

if flag=1 then process

        r_input:=(r_input mod capacity);

        c_input:=(c_input mod capacity);
                                        temp:=in;

        in:=buffer[r_input];

        buffer[r_input][c_input]=temp;
                        end; {k_store}

                        {Initialization}

                        r_input:=capacity;
                        c_input:=1;

                end key;

        end; {key_analysis}
```

2.2 Algorithm

1) Get input as a Deciphered Entity (DE).
2) Make data and variable ready for circular search, mirroring and swapping
3) Enter into procedure termed key analysis with adequate data.
4) Search all rows and columns systematically with DE.
5) Handle row and column element in continual fashion.
6) Mirror it parallely with search process
7) If DE found in a database, then set a flag to success and trace the position for next cycle (swapping)
8) Enter into a procedure named as **b_disp** with buffer value
9) Append latest copy in a RAID disk

10) Enter the procedure **k_store** with this latest copy and find a key value in it.
11) Shift this key value into different position to maintain a data security for next cycle.
12) Halt the data and variable with ground value

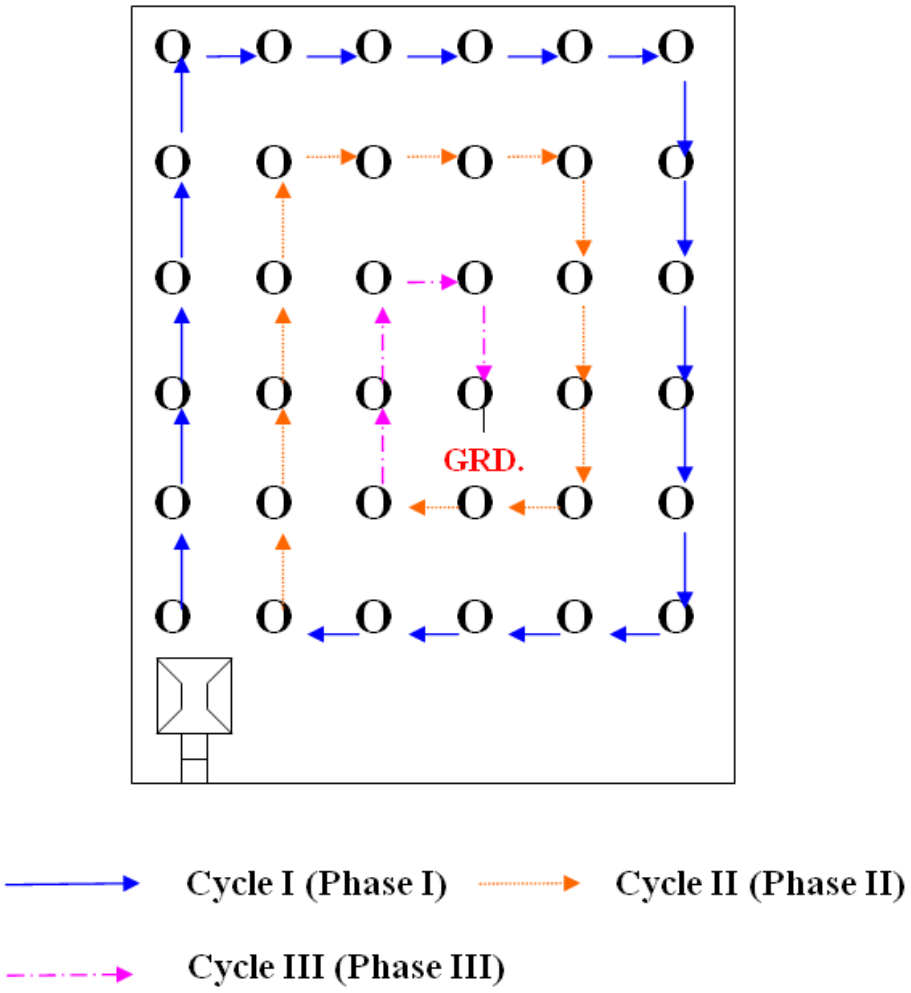
2.3 Testimonial of OTM



2.4 RAID* Redundant Array of Independent Disks

- Initially, Encrypted format is converted into plaintext using general cryptography algorithm.
- After getting deciphered format algorithm goes for matching the key value from any of the local or remote databases.
- If it is found, and then regularize the user entry and every status logs are mirrored and stored into a RAID for process monitoring and backup purpose.
- Position of the key in a database may go for repositioning for protection purpose in next cycle.

2.5 Traversal Pattern of OTM



The cited above Data Flow Control diagram divided into three phases to complete the entire processes such as Data Capture, Mirroring and Shift Keying. It is the algorithm merges all the above activities in a single unit. This algorithm mainly focuses on cons of DDA and time study primarily compared with this algorithm.

2.6 An Overview of Referral Input

Referral Input (RI) refers a database for standard input. For instance, CRYPT (2), here CRYPT is a database and 2 is the field index. If the input is L , CRYPT(2),O then it substitute 2nd field's row simultaneously or sequentially (Depends on algorithm). The operator "," separates a standard input with referral input. The following are the different input related with L, CRYPT (2), and O. In this input L and O are two standard inputs and CRYPT (2) is the single referral input.

User_Id	Code	Encrypted Text
Jakson	HEL	LHELO
Ravi	S	LSO
Rajesh	KQ	LKQO
Rakesh	LE	LLEO

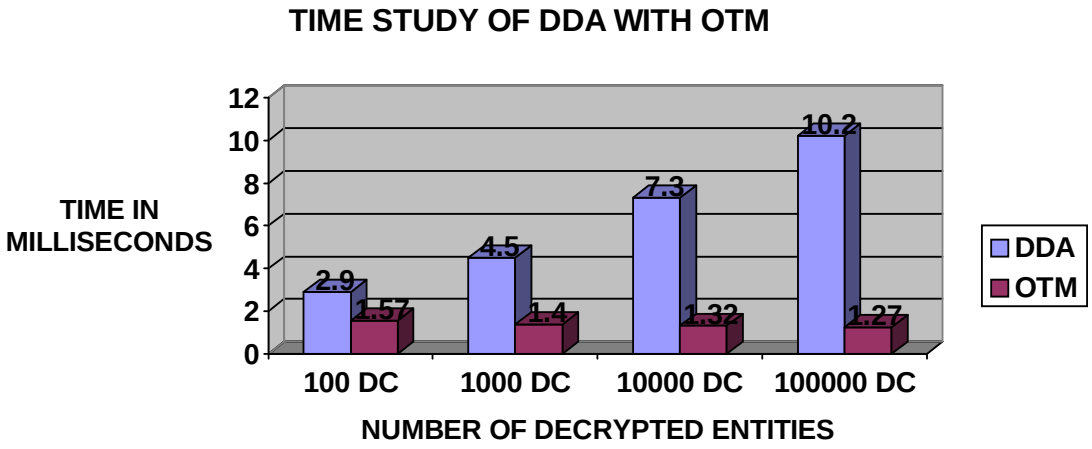
2.7 Cons of Data Detection Algorithm

The following are the major demerits we found in DDA. The newly proposed OTM chalk out these demerits.

- No standard fashion designed for data capturing. Owing to this time delay may increase in case of huge database.
- In case, first cycle skip a database with six elements then the next searching process starts from seventh element and it goes until 'n'th element but if result physically exists in <=6 th element means it displays "data does not exist" message to an user. But data physically present but searching algorithm absent in rare situations like this.
- No proper shut down of database in every cycle. It is only dealt with data control systems. It depends on separate algorithm to handle mirroring and shift keying.

2.8 Comparison between DDA and OTM

Data Detection Algorithm (DDA)	Optimal Test Mirroring (OTM)
Intakes Standard Deciphered Format	Intakes Referral as well as standard Deciphered Format
Searches Key in a database	Searches Key in a database and mirror this activity
No standard fashion for data traversal	Swing method used for quick data traversal
Standard Key Position	Shift Keying used in every cycle to maintain data integrity
No Proper shutdown of database	Proper shutdown of database in every phase
Collectively it only dealt with data capturing.	Dealt with data capturing, mirroring and shift keying
Perfect algorithm for small database with standard deciphered format.	Flexible algorithm for cryptologist to maintain data integrity with rigid security. (Referral Input Pattern)



Algorithm	100 DC	1000 DC	10000 DC	100000 DC
DDA	2.9 ms	4.5 ms	7.3 ms	10.2 ms
OTM	1.57 ms	1.4 ms	1.32 ms	1.27 ms
Note: Time for OTM refers an entire transaction. DDA refers only Data Capturing.				

3. Conclusion

In this paper, we discussed the concept of optimal test mirroring with Association Rule, instant data capturing, data mirroring to maintain security levels and storing of data logs in different location. This algorithm entirely overcomes the relay in data detect algorithm.

References

[1] Lampson, B.W. 1993, Protection. Proceedings of the Fifth Princeton Symposium on information sciences and systems. Princeton University: 437- 443.

[2] Kohler, W.H. 1991, A survey of Techniques for synchronization and Recovery in Decentralized Computer Systems. Computing Surveys, Vol. 13, no. 2 (June): 149-183.

[3] Lamport.L, R.Shostak and M. Pease, 1997. Time, Clocks, and the Ordering of events in a distributed system. Communications of the ACM, vol.21, no. 7(July):558-565

[4] Sholom M. Weiss and Loannis Kauleas, Rotgers Univ, 1999. An empricial comparison of pattern recognition, neural nets and machine learning classification methods, ACM vol.20.

[5] Choulam .K. Shamir,McGenGill, 2001, Hit count pattern simulator using Data mining and Neural Networks, IEEE chapter, Canada

[6] Noboru Murata, Shuji Yoshizawa, Shun-ichi-amari,1994,Network Information Criterion – Determining the number of hidden units for an ANN model, IEEE Transactions and Neural Networks Vol 5 and 6.

Dr.N Rajkumar obtained his Bachelor's degree in Computer Science and Engineering from Madurai Kamaraj University in 1991 and His Masters in Engg .the same stream in the 1995 from Jadavpur University. Kolkata. He has completed his Masters in Business Administration from IGNOU in the year 2003. His doctorate is in the field of Data Mining, which he completed in 2005 from PSG College of Technology, Coimbatore. He is currently the Head of the Department of Computer Science and Engineering at New Horizon College of Engineeering, Bangalore, Karnataka. He has served in the field of education for over 17 years at various Technical Institutions. He has been instrumental in the conduct of 30 Short- Term Courses and has also attended 20 courses conducted by other Institutions and Organizations. He has authored 2 books for the benefit of the Student Community in Networking and Computer Servicing. He has published as many as 30 papers, 3 in International Journals, 17 International Conferences and others at the National level in his area of expertise namely Data Mining, Networking and Parallel Computing respectively. He has guided 100-Project scholar's to-date.