International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Secured Event Data Recorder (EDR) System for Analysis of Data

Love Sharma[1], Pankaj Chandankhede[2], Dr. Milind Khanapurkar[3]

[1]Student, M.Tech (Communication Engineering) Electronics and Telecommunication Engineering, G. H. Raisoni College of Engineering Nagpur, India

[2]Research Scholar Electronics and Telecommunication Engineering, G. H. Raisoni College of Engineering Nagpur, India

[3]Professor & Head of Department, Electronics and Telecommunication Engineering, G.H. Raisoni College of Engineering Nagpur, India

Abstract: ***In today's world there is an immense need of data which is recorded in real time, such as the data of vehicle crash, system monitoring, and many more related domains. This data can be further used to make the analysis of the system such as finding a loophole or for checking any kind of fraud. In this paper, we are going to review different EDR techniques, Encryption algorithm, Backup algorithms and Data extraction algorithms. Here we will review multiple techniques for each of the modules and will conclude the best method according to the analysis made***

Keywords: - EDR, Encryption, Backup, Data Extraction

1. Introduction

Event Data Recorder is one of the important parts nowadays in the vehicles which are also termed as the black box or flight data recorder in aircraft. The main aim of this system is to gathers the information from different parameters like a crash, time, speed and much more. If the EDR is attached inside the vehicle it traces everything whatever activity happens i.e. before, after and also when any anomaly takes place. This recorded data is very useful for car accident investigation.

Primarily, an EDR is an onboard device or technique that has requisite qualities such as monitoring, recording, displaying, storing and transmitting data with respect to the event it was stored. All this information can be reused, for example, if we take the same situation i.e. of the Vehicle Monitoring, the driver's data can be put to use while training the driver in case of emergencies or can be applied while an investigation or the performance. Due to this reason all the cars in the USA were equipped with EDR.

In this paper, we are going to study about an EDR whose data is used for data analysis. The system contains multiple modules, first is the hardware part on which the actual EDR is present. In this paper, we will study about such system. Once the hardware module is over, we will directly jump to the software module in which the first part is the encryption of the data. The encryption is required to save the data from any intruder which may or may not be present. If the system in not encrypted then any intruder can change the data resulting in varying results.

After the data is encrypted the data is to be fetched to gain knowledge from the data collected by the system, for this Top K rules can be used which are reviewed in the following section. Lastly, the data needs a backup for which various data backup algorithms are studied. The paper is organized, the following section explains the different EDR system following with the Encryption, Data extraction, and Backup algorithms review. Finally, the paper is concluded with a conclusion

2. Event Data Recorder

2.1 EDR based on ARM7 and CAN:

The EDR systems are generally equipped with the number of best of the sensing components which are triggered as soon as there is a possibility of the problem. The block diagram of the system is shown below:

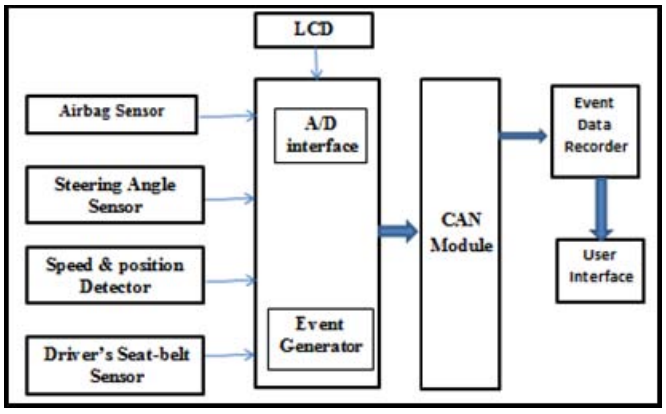

Figure 1: Block Diagram of Vehicular system

This system contains multiple sensors like IR, Temperature, Vibration, Accelerometer and Alcohol sensors installed and connected with a CAN bus with the Controller Area Network (CAN) module. This module is then connected to the ARM processor handling the EDR and the GUI.

The system starts with initializing the sensor and system. The data from the sensor are collected using the CAN bus. The data processed using the ARM7 processor and if the sensor

limit exceeds the data is stored into the flash memory. Then the data is sent to the user for analysis.

2.2 EDR using ARM

Nitin P. Sirsikar and Pankaj H. Chandankhede has proposed an EDR with the ARM-based processor. The system contains different sensors like Alcohol, Accelerometer, Speed, Position, Temperature and Proximity Sensor. The setup is splitted into three modules. The first part is the Data collection module where the data is collected using the sensors on different moving useful info and conditional information. The second module is the information Processing module, it receives data from the data collection module and then processing of the data is done with the help of ARM and the coding is done using embedded C. The HCI is the third module which displays the data information on the screen.

Security

For true communication between sender and receiver the method which comes into existence is cryptography. It is the process of protecting the information i.e safety of data. The set of points which are covered under data security like covertness of true content, integration, priority, non redundancy or no refusal of information.

The technique of manufacturing the most important piece of information for attackers indecipherable & only provided to true receivers. That is no fear of leaking of data and transmitting it successfully.

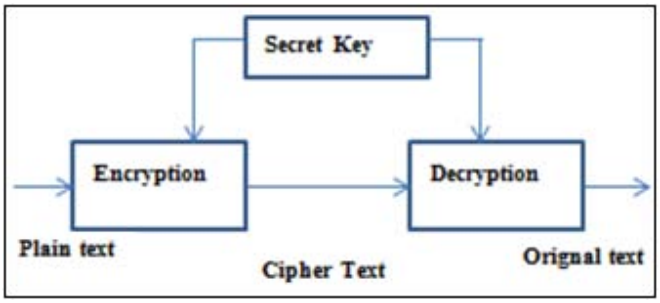

Figure 1: Symmetric key Encryption

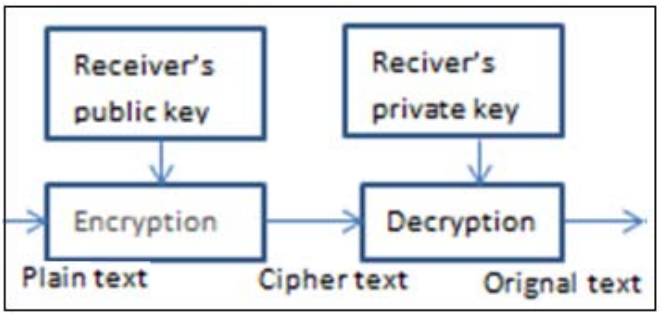

Figure 2: Asymmetric Key Encryption

The most known cryptographic techniques are as follows:

1) Symmetric key encryption: Similar keys utilized at transmission & reception. Using same keys for encoding and decoding. The types are Blowfish, RC5, RC4, CAST, IDEA.
2) The process including 2 keys which differ by each other for encrypting as well as decrypting messages known as key assyemtric encoding. For encryption the transmitter section utilize public key and while decryption utilize personal key. This methods are Hellman Diffie, Gamal El, elliptic curve, RSA.
3) Mixed Encoding: The combination of above 2 methods termed as hybrid encryption. Utilizing two keys called as session key & key bulk.SSL is one of the best technique known for it.

3. Data Extraction

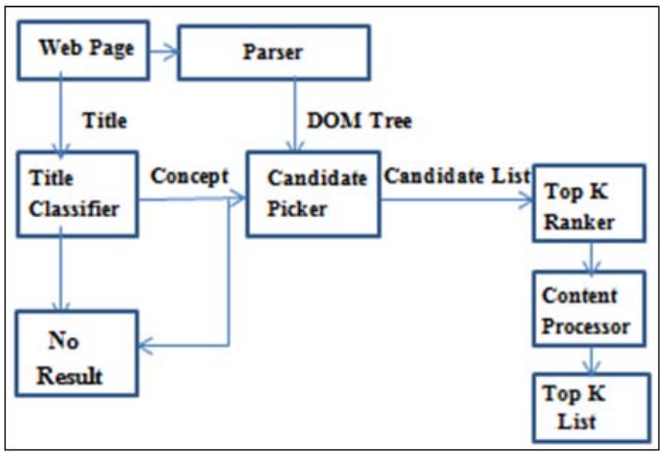

Figure 1: Top k system overview

Process of Searching Top grade values of data set which is standard are as follows

1: Initiate
2: i/p
2.1 Transaction Database
2.2 n
2.3 Miniconf
3: take minimum support value=0
4: follow 5 to 6
5: best rule is selected if support = minsup & minimconfidence =minconfvalue;then included in list of rules.
Support arrange the sequence of n first grade rules.
6: putting support value as the lowest order.
7: End

Different top k techniques:

A. AIS algorithmic rule.

The AIS algorithmic mining association rule. It specializes in the level of the databases together with the functionality required to support queries method calls. At a time,while applying this rule formation of only 1 item sequent association rules take place, for example, we have inclinated alonely to form rules same as P∩ R -> T .Morover not those rules as P -> R ∩ T. The databases were examined sequentially many times to insert the frequent item sets in AIS.

The major limitation of the AIS, is that the several sets of candidate elements finally are being small plating generated and you require additional space and abundant waste to be

inadequate. At fixed time this algorithmic rule also requires several passes for full information.

B. Apriori Algorithm

Apriori is a remarkable improvement in the historical context of membership mining principle. The AIS is just a simple methodology that needs several outlets for the database, generating various sets of promising elements and store counters each applicant while the majority of them banned not be continuous.

Apriori is more effective in the mid of the process and it was optimistic because of the two reasons, apriori participates in focusing on the era of the distinctive applicant and is another method of pruning. It also mitigates calculation.

Apriori has the disadvantage of examining the whole database reiteratively. His prior principle maintained new calculations were seen with some changes or change. As a rule, it has been 2 approaches:

- One is to reduce the quantity of disregard the complete information with exclusive piece of it so as to upheld this succeeding itemset,
- Another approach is to examine fully different kindsof rectifying methods, framing the quantity of competitor itemsets. Apriori-TID and Apriori-Hybrid, DHP, SON or modifications of the Apriori principle.

In any case, the algorithm is having two challenges: One is the intricate competitor strategy that is used more often, region and memory. And another bottleneck is the different sweep of the database data. .

C. RARM

It stands for rapid association rule mining. RARM is one of the fastest methods to get the FP-Tree algorithmic program, it was proved in the base papers using various experiments and results. When the SOTrieIT structure is exploited it will generate 1 and 2 item sets data quickly without scanning the rest of the information again and again and also generates candidates.

D. Multiple Level ARM

When an application is implemented there is a need to seek robust association rule which acts as a glue between the Knowledge at the most basic level of the three-dimensional data. Whereas robust association rules generated at the next thought level could also be wisdom to some users, however, it can also be novel to alternative users. To mine the robust and most effective rule mining for the system multiple level rule mining is done that is the rules are made more generalized. For example from a shoppers dataset it has been observed that Bread and Milk are bought by the customer each time together then in multi-layer mining it would generalize it as there is a relation between the milk and bakery products which will conclude that both f then are often bought together which will negate the effect of adding an item data into the database.

3. Data Security

When there is a data its security is one of the important problems, in this paper we are proposing a few techniques to secure the data from the intruders. Here algorithms like RC6, RSA, AES and much more which are explained as follows:

Encoding algorithm

Before application of RC6,selection and storing the file in a cloud is necessary.

Reading the file selected and converting the file info into array of bytes

a. Key Expansion

1) key is generated according to system time in millisecond.
2) Accumulate that key in the database along with the name of file,then enter that key in key expansion function.
3) Key expansion function generates key in fixed byte format in a byte array.

b. Encryption function

1) Enter the original data and key in terms of byte array in the obscuring data function.
2) The outcome of encryption function results out encrypted information in bytes of array.
3) Write encrypted data in the file and store them in the cloud.

Decryption Algorithm:

File is selected in the cloud then following step will be performed.

1) Access key from the database according to file in the cloud.
2) After passing key in key expansion function,fixed byte array formation takes place.Reading information from selected file and conversion of encrypted data in byte array takes place.
3) Pass data and key (byte array) in decryption function.
4) By utilization of decryption function we get the decrypted data in terms of byte array & then in temporary file data is to be writed.
5) User can see that information from a temporary file.

Table 1: Decoding & encoding time for different size of files by utilizing RC6 law

File Size (KB)	Time of Encryption(Milliseconds)	Time of Decryption(Milliseconds)
100	13	8
200	19	17
300	26	24
400	36	34

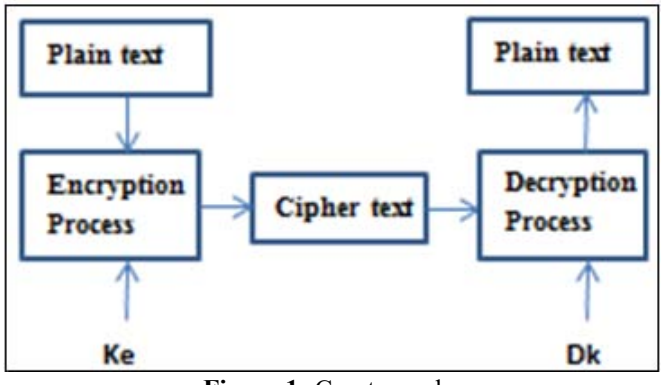

Figure 1: Cryptography

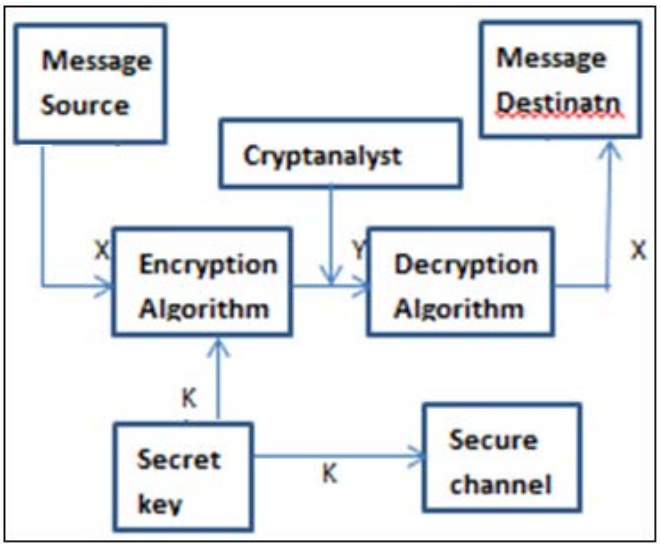

Figure 2: Model of symmetric system for data security

A.DES (Data Encryption Standard)

In 1970 a security protocol which was using Feistel structure was developed, which was named Data Encryption Standard. DES is an algorithm in which similar keys are used for encrypting and decrypting, hence for transmitter and reciver private keys are similar. The key can be as long as 64bits with 8 bits reserved for parity check. To perform the encryption of the message a 16 step long permutation is performed. The steps are a lot similar in encryption and decryption only they are reversed.

The DES protocol is vulnerable to brute force attack which is amongst the most common attacks. There are a few fast and advanced attacks done on DES, which are

a) The differential cryptanalysis
b) The linear cryptanalysis
c) Davies Attack

Since these attacks can breach the security easily DES is considered to be less secure and not widely used.

B. TDES (Triple DES)

With the advancements, the DES also advances and TDES (Triple DES) came into picture overcoming the design flaws or the attacks which DES didn't meet. In this protocol, the DES is permuted thrice making the old 16 step permutation to 48 and extending the key length to 168 bits. The encryption is done by applying such a large key. The TDES also provides us with three encoding options. In the first option the keys namely K1, K2, K3 all of them are independent whereas in type two K1 and K2 are identical and K3 is identical and lastly, all the three keys that are the K1, K2, K3 are identical to each other.

C.AES (Advanced Standard Encryption)

Another method evolved to overcome the problems made by the DES was AES or the Advanced Standard Encryption. It is also symmetric and blocks cipher as DES. The block size in AES is 128bits with key sizes of 128 bit which is around 10 laps or 12 rounds. The permutation is reduced to 4 here which includes substitution of bytes, changing rows, mixing columns and lastly adding a round key. All three stages are explained as follows:

Stage 1 substitution of bytes takes place & inversion and replacement of matrix takes place by original matrix for regaining the original data.
Sage 2 includes shifting of rows, the rows are shifted keeping in mind the constraints specified.
Stage 3. Comprises the function of integrating coloumns then every coloumn is multiplied with constant polynomial & instant result values are assigned as output.

Lastly, stage 4 adds a round key. From main a subkey is generated which is the round key. This key is then XORed with the matrix to get the final encrypted matrix.

D. RSA

A public key encryption was generated by Ron Rivest, Adi Shamir and lastly Leonard Adleman which was later named RSA based on the name of the researchers who developed it. The algorithm has a two call public and private keys of length 1024 bits. To generate the Public and Private Key RSA randomly takes two prime numbers. The known attacks to breach RSA are as follows:

The exponent small number can be easily broken.

- If more receivers are each message encrypted with the same exponential they can be deciphered.
- Also, the chosen ciphertext is possible.

Data Backup

After security one of the important aspects that arises is the backup of the data or the server as if by any case the data is lost, got corrupted or intruded we need a free and fresh copy of all the data so that the loss is minimum in this section of the paper we will learn about various Data backup system. Data Backup can be done in many forms it can be local or on a cloud if the backup is at a distance then it is called as the Distant information Restore server. Similarly multiple notations like a central repository, remote repository are explained with the techniques in the following paragraphs. TO boot or to accumulate large amount of information we need given below terms to be satisfied:

1) Integration of information
2) Privacy.
3) Rearrangement of servers to the cloud.
4) cryptography of the data
5) coverting data
6) Factor of trust
7) factor of cost effectiveness
8) Appropriate Timing

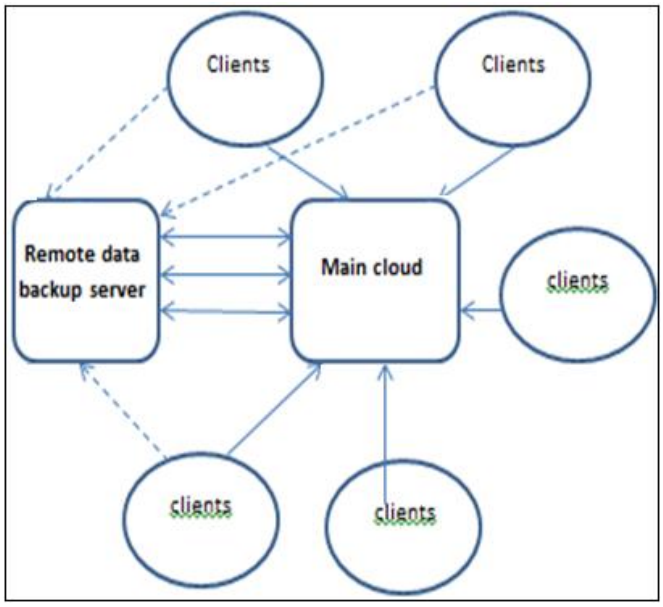

Figure 1: Distant infomation restore server & its structure

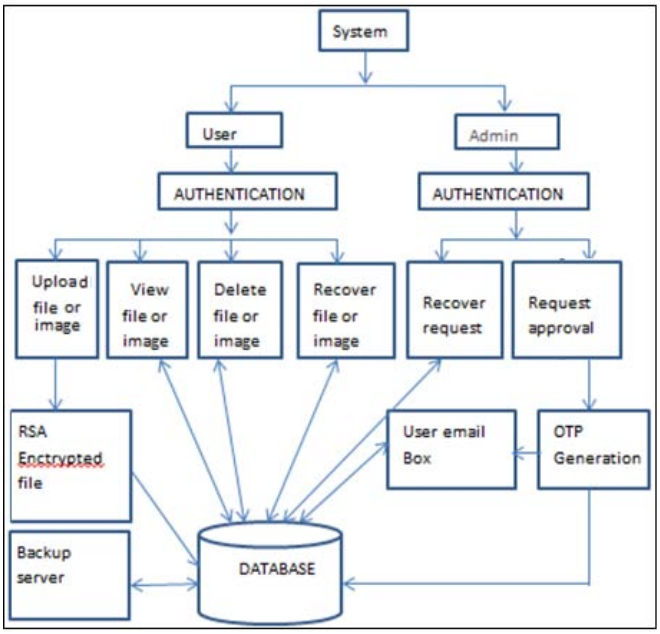

Diagram no.2.Proposed seed block law structure

Seed Block Algorithm (SBA) Architecture

Backup and restoring is one of the tedious jobs which is simplified by the Seed Block algorithm using a simple XOR method. Let us consider that we have two sets of data M to be the main Q to be a constant data and P is the final output. In seed P = M XOR Q for example M = 1 and Q = 1 then P = 0. Now for some reasons the main data M gets deleted but we can still regenerate this by using the rule M = P XOR Q i.e. M = 0 XOR 1 which is M = 1 which is true according to the condition taken.

The figure two above illustrates the architecture of SEED Block Algorithm which constitutes of the Main Cloud, Remote Cloud, and the users/ Client. To get it working first a client is register to the SEED server where a unique ID of the client is generated then a random number is generated which is XORed with the data of the client the XORed value of the client is stored with its client ID. Similar steps are done for all the clients connected to the system. The advantage of using seed is that the recovery is of same size data, therefore, there is no data loss. The second advantage is the privacy and lastly, the SEED is implemented at low cost.

HSDRT (High-Speed Data Rate Transfer)

Since the clients today are not bound to a location we need a system which will help to take backups of mobile devices such as cellphones, laptops, tablets and more. The technique used to overcome this problem is HSDRT. It utilizes an high level vast information delivering operation and maximum accuracy obscuring process. The drawback faced by it is that it will not decrypt accurate data for backup & for recovery process. Also it fails to save out or record the data at distant distance servers.

PCS

Parity cloud service supports parity restoring service. It is simple & easy to carry out operation, with maximum probability it regains data. As a backup it forms virtual disk, forms groups over it, utilizes Exor operation for making parity data. limitation faced by it was of large amount of complexity.

ERGOT

Efficient rounding grounded on taxanomy is a system which is based on semantic analysis but it also fails to focus on the time complexity as well as it is hard to implement. Information backup is produced in efficient way and it is the process which assist service discovery.

Table 1: Existing cloud backup techniques

Sr.no	Method	Advantages	Disadvantages
1.	HSDRT	-used for mobile clients like laptops, tablets & cellphones	-Expensive -Data -Redundancy
2.	PCS	-Reliable -Security -Less Expensive	-Difficult to implement due to implementation complexity
3.	ERGOT	-Perform perfect retrieval of data -Low cost for implementing	-Time complex Implementation Complexity

As observed from the table above all the techniques listed have one or the other drawbacks which make remote backup unstable. Therefore we dicussed SBA that rectify drawbacks of newly formed backup methods.

References

[1] Mr. Amit V.Lute, Asst. Prof. P. H. Chandankhede, Dr. M. M. Khanapurkar,"ARM7 Processor based Event Data Recorder using CAN For Vehicular Systems", International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 02; February–2016.

[2] Nitin P. Sirsikar, Prof. Pankaj H. Chandankhede,"Design of ARM based Enhanced Event Data Recorder & Evidence Collecting System",IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 5, Ver. V (Sep - Oct. 2014.

[3] Shital V Vaidya, Prof. Pankaj H. Chandankhede,"Designing of Event Data Recorder for Vehicle Monitoring based on ARM processor",Image Processing andNetworking Volume:8 Special Issue IV Feb 2014 ISSN No:0973-2993.
[4] By Dr. Prerna Mahajan & Abhishek Sachdeva,"A Study of Encryption Algorithms AES, DES and RSA for Security",Global Journal of Computer Science and Technology Network, Web &Security Volume 13 Issue 15 Version 1.0 Year 2013.
[5] Rajdeep Bhanot and Rahul Hans,"A Review and Comparative Analysis of Various Encryption Algorithms",International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306.
[6] Sunil Yadav, Kanishk Bahadur Singh,"Evaluation and Review of Security Algorithm on Cloud Computing Environment",International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2015.
[7] Jaspreet Singh, Sugandha Sharma,"Review on Cloud Computing Security Issues and Encryption Techniques",IJEDR | Volume 3, Issue 2,2015.
[8] Lovedeep Singh, Er.MandeepKaur,"REVIEW PAPER ON -NOVEL TECHNIQUE OF CRYPTOGRAPHY ALGORITHM FOR IMPROVING DATA SECURITY",Global Journal of Advanced Engineering Technologies, Volume3 Issue4.
[9] Harsh Kumar Verma and Ravindra Kumar Singh,"Enhancement of RC6 Block Cipher Algorithm and Comparison with RC5 & RC6",20133rd IEEE InternationalAdvanceComputingConference (IACC)
[10] Abdul Hamid M. Ragab, Nabil A. Ismail,"Enhancements and Implementation of RC6 Block Cipher for Data Security",IEEE Catalogue No. 01 CH37239 0-7803-7101-1.
[11] Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho,"An improved RC6 algorithm with the same structure of encryption and decryption",ISBN 978-89-5519-139-4 -1211- Feb. 15-18, 2009 ICACT 2009
[12] Zhixian Zhang, Zheng Wang, Haixun Wang, Kenny Q. Zhu, "Automatic Extraction of Top-k Lists from the Web",Shanghai Jiao Tong University Shanghai, China.
[13] Amardeep Kumar, Arvind Upadhyay,"AN EFFICIENT AND ENHANCE TOP K ASSOCIATION RULES MINING", International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 1 (January-February, 2016), PP. 17-21
[14] Somesh P. Badhel, Prof. Vikrant Chole,"A Review on Data Back-up Techniques for Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.12, December- 2014, pg. 538-542.

Author Profile

Love Sharma received the B.E degree in Electronics and Telecommunication Engineering from G.H Raisoni College of Engineering, Nagpur. Presently doing M.Tech from G.H Raisoni College of Engineering, Nagpur.