RESEARCH ARTICLE OPEN ACCESS

Design of Secured Ground Vehicle Event Data Recorder for Data Analysis

Mr. Love Sharma, Pankaj Chandankhede and Dr. Milind Khanapurkar
** M. Tech. Student, Department of Electronics and Telecommunication Engineering, G. H. Raisoni College of Engineering, Nagpur, India*
*** Assistant Professor, Department of Electronics and Telecommunication Engineering,G. H. Raisoni College of Engineering, Nagpur, India*
**** Professor & Head, Department of Electronics and Telecommunication Engineering,G. H. Raisoni College of Engineering, Nagpur, India*

ABSTRACT
The Event Data Recorder (EDR) is now one of the important components installed in the vehicles by the automakers since it is helping in calculating an independent measurement of crash severity which is far better than the traditional systems used. There is limited research is done on the domain. In this paper we are going to propose an EDR which is based on ARM controller and will sense the alcohol, brake pressed, Speed, Location, Humidity, and Temperature. The data collected from the sensors is aggregated using a threshold-based technique, then the data is encrypted using RC6 and finally, the data is mined for knowledge using top k rules.
Keywords **-** Event Data recorder (EDR), RC6, Top K Rules

I. INTRODUCTION

All the automakers are now using event data recorders as a standard device in vehicles, which are particularly designed to record data elements before and during the collision which are used for crash reconstruction. Every manufacturer has given a different name for the device. The NHTSA refers to all of them as Event Data Recorder (EDR). One of the important aspect to detect a crash is the velocity of the car which is also termed as delta-V. It is also a widely accepted measure to calculate crash severity. There are different methods to calculate velocity which is calculated upon correlations with post-crash vehicle deformation management which is always successful. The direct measure of the velocity of the vehicle which is provided by EDR can independently measure the crash severity, this measure can help in avoiding the difficulties of crash reconstruction technique.

EDR, vehicle framework information, and crash data are consistently put away in an unpredictable information buffer amid ordinary operation. Contingent upon the module and the sort of occasion, the unpredictable information might be flashed to an EEPROM. In the case of an airbag organization in a General Motors vehicle, this information is for all time written to the EEPROM (and the module must be supplanted). Notwithstanding, if the airbag is not sent, EEPROM information is cleared after the SDM is turned on 250 circumstances. These qualities fluctuate for modules from different producers; intrigued per users are alluded for extra data about SDMs utilized as a part of General Motors autos. Driven by the need to guarantee the precision, dependability, and protection of vehicle occasion information, the Society of Automotive Engineers (SAE) and the Institute of Electrical and Electronics Engineers (IEEE) joined with NHSTA to shape working gatherings to address approach issues and institutionalization. Intrigued per users are alluded to the NHTSA site for data about these working gatherings and their exercises.

Generally, the primary concern has been the unwavering quality of car occasion information in accordance with supporting physical confirmation in crash examinations. Therefore, the dominant part of studies identified with EDRs has concentrated on utilizing information after it has been recouped and decoded. In any case, it is similarly as essential to guarantee that occasion information utilized as a part of legitimate procedures precisely reflects the information caught by the EDR. In this paper we have proposed a novel idea for EDR, the following section briefly describes the proposed technique following with the implementation. The 4th section of the paper illustrates the result of the proposed technique and the conclusion concludes the paper.

II. PROPOSED SYSTEM

In this section of the paper, we are going to study the proposed technique. The figure below shows the block diagram of the proposed system:

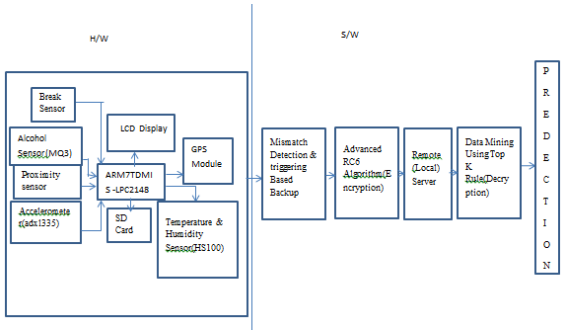

Figure 1: Block diagram of proposed system

The above figure shows that the proposed EDR model is having a lot of modules, majorly the system is divided into two parts i.e. the Hardware and the software. As observed from the diagram the hardware consists of the kit, sensors and display modules which are explained as follows:

A. HARDWARE UNIT

Arm 7 kit: this is the base of the hardware part on which all the sensors are mounted. The Arm Controller Kit used is LPC2148. The controller used is a high performance 64 pin with a flash program memory of 512KB. Since we are in need of multiple I/O devices as we have to mount the sensors the kit provides 45 I/O pins with two 32bit timers and a real time clock with independent power. Temperature Sensor: temperate is one of the aspects of our technique as it affects the driving condition of the driver. To sense the temperature LM35 temperature sensor is used. The LM series sensor is used because it provides the results directly in Celsius. The range of the sensor starts from -55° C up to 150° C. Also, the sensor is useful for remote applications as it can operate from 4 V to 30 V and the cost is also low due to water level trimming.

Humidity Sensor: humidity is also an aspect that affects the behavior of the driver, therefore to detect the humidity we have used HS100 sensor. The sensor designed by NetBotz can be used for monitoring the humidity of a remote location. Also, the humidity values can be set once the sensor is mounted.

Location: the location of the vehicle can be easily found using the GPS module. The GPS module will find the latitude and the longitude of the vehicle location.

Accelerometer: a standout amongst the most well-known inertial sensors is the accelerometer, a dynamic sensor fit for a boundless scope of detecting. Accelerometers are so accessible that it can quantify increasing acceleration in one, two, or three orthogonal tomahawks i.e. axes. The sensor used is AX100.

Alcohol: One of the reasons for the crash is the lack of stable state of mind, this uncertain state can be because of alcohol consumption. A strong smell is emitted from the mouth of the alcohol consumer to detect that smell sensor is used. The sensor used here is MQ3. It is used because the energy required to run the sensor is 5V. It is also easy to use with good sensitivity to alcohol gas providing both digital and analog outputs.

Distance: long distance travel can create fatigue and can lead to crash, therefore, the distance traveled by the driver is an important aspect therefore to calculate the distance we will take help of the GPS module. It will calculate the distance using the start and end position.

Speed: another important aspect of crashing is the speed of the driver. To calculate the speed of the driver we apply the following formula:

Speed = Distance / Time

Brake: while traveling braking also possesses importance as it depends on the driver if the brake is pressed late by a couple of seconds there could be chances of collision. Since there is no sensor for brakes we are using the key of the kit as a brake.

The above hardware module helps in detecting multiple events while the driver is driving the car but if a car is crashing there are usually more than one reason to it. Therefore we have to aggregate the data so that we can make analysis efficiently for that in this system we are using threshold based Data Aggregation.

B. THRESHOLD BASED DATA AGGREGATION:

Since the data is produced from various sources we are in need of a technique which can aggregate the important data and send it to the user for processing. When the system sends the input there is not necessary that all the accidents are caused due to a mixture of features and also there might be a case where there is no accident but still the sensors are sensing and sending the data. Therefore to overcome this problem we are going to use a threshold based system for data aggregation as shown in the following figure:

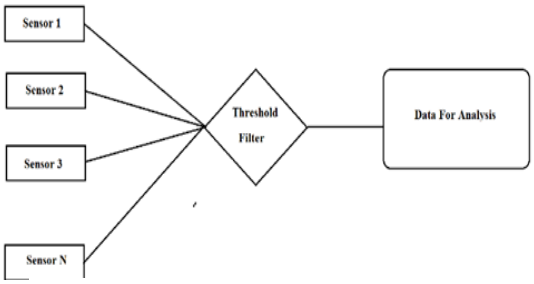

Figure 2: Block diagram of Data Aggregation

As we can observe in the above figure, the system records the data using the sensors which are then send to check for their fitness. In the filter block, a threshold is already initialized let us assume that the threshold is 1. Now when the input of sensors has received the values of sensor 1 and sensor 2 is subtracted to find the difference. The difference calculated if then checked with the threshold if the difference is greater than the threshold then only the data is sent else the data is not sent. The algorithm for the technique is as follows:

Algorithm:
Initialize threshold t
Step 1: Sense the input using the sensors,
Step 2: for all the sensor (s1, s2, s3 … sn) values:
Subtract the value of sensor 1 with other sensors,
Repeat until all the differences are found.
Step 3: for all the difference value (d1, d2, d3 … dn):
If di > t
Send the sensor value
Else
Reject sensor value
Step 4: Send all the selected sensor values for analysis
Step 5: end

Once the data is filtered it is then encrypted so that it can be uploaded to servers and then the analyst can access it from anywhere and make the analysis.

C. RC6 ENCRYPTION:

Since the data will be sent to an online server we need some encryption to save the data from intruders. Therefore RC6 algorithm is used. It is one of the important members of the block cipher family. RC is a family of the fully parameterized encryption algorithm. It is also denoted as RC6-w/r/b, where 'w' represent the word size available, 'r' is the number of rounds and lastly to denote the length of encryption key we use b. One of the important shorthand version of RC6 is where the dimensions of RC6 are w = 32 and r =20. Therefore when 'r' and 'w' with AES it makes w = 16, r = 10 and b = 32 bytes. There are six basic operators used by RC6 which are denoted as follows:

a+b integer addition module 2^w
a-b integer subtraction module 2^w
a $\oplus$ b integer XOR module 2^w
a X b integer multiplication module 2^w
a<<<b integer rotation left module 2^w
a>>>b integer rotation right module 2^w

We can observe that the round is similar to that of DES half of the part is updated with the other half. The key schedule can be derived from user provided a key which is given during encryption and decryption. The key is in the range of 0 to 255. The encryption algorithm is as follows:

i. Encryption Algorithm:

Input: Plain text, the number of rounds r.
Output: cipher text
Procedure:
B = B + S[0]
D = D + S[1]
for i =1 to r do
{
t =(B X (2B + 1))<<<lg w
u =(D X (2D + 1))<<<lg w
A = ((A X t)<<<u)+S[2i]
C = ((C X u)<<<t)+S[2i + 1] (A;B;C;D)=(B;C;D;A)
}
A = A + S[2r + 2]
C = C + S[2r + 3]

ii. Decryption Algorithm:

Input: Cipher text and w-bit round keys
Output: Plain Text
Procedure:
C = C - S[2r + 3]
A = A - S[2r + 2]
for i = r down to 1 do
{
(A;B;C;D)=(D;A;B;C)
u =(D X (2D + 1))<<<lg w
t =(B X (2B + 1))<<<lg w
C = ((C - S[2i + 1])>>>t) $\oplus$ u
A = ((A S[2i])>>>u) $\oplus$ t
}
D = D - S[1]
B = B - S[0]

Once the encryption and decryption of the data is done it is optimized using the gold code which is explained in following paragraphs.

D. GOLD CODE OPTIMIZATION:

Gold Codes are one of the important binary sequence used in telecommunications and navigations. It is also denoted as Gold Sequence and is named after Robert Gold. Gold codes are useful only when the transmission is over the same frequency range from its start to end for that they have bounded some small cross-correlations to them. There are $2^n - 1$ sequence with a period difference of $2^n - 1$ in the gold code. We have to follow the following steps to generate gold code. Initially, pick two maximum length sequence of the same length, but make sure that the absolute cross-correlation is less than or equal to $2^{(n+2)/2}$. Here n is the size of linear feedback shift register since the LFSR is used to generate maximum length sequence. The set of $2^n - 1$ XOR's of the two sequences in their various phases is also a set of gold code. There is also a highest level absolute cross-correlation present for the codes denoted by $2^{(n+2)/2} + 1$ when the length of the code is even and $2^{(n+1)/2} + 1$ when the length of the code is odd. In this case, the encrypted data is sent through Gold Code for increasing the efficiency of the system.

E. TOP K RULES:

Once the data is received by the system it is then sent for testing, the testers or the data analyst performs mining on the data to get the desired knowledge in this system we are going to use Top K Rules as the technique. Top k rules are one of the important technique where the algorithm is initialized using an input database, a set of rules to be found denoted by k and threshold that is minconf. Initially, minsup is set to 0, then the searching of the rule starts. A list L is maintained where all the searched rules are stored. One the L list is full with k rules, the minsup is set to the lowest support value of L.This threshold value is raised because the search space when searching for more rule if a new rule is found it is then added to the list L. the process is continued till all the rules are found. The classical two-step approach is not an efficient method to find the rules. Therefore instead of a two-step approach, it generates rules containing a single item of the antecedent and one of the consequent. When the rules are found an item is added to both antecedent as well as consequent. To select the items to add to make the rule list grow, the technique scans the transactions which contain the rule is expanded in both rights and left direction. We name the two procedures for growing principles in TopKRules left extension and right extension. These procedures are connected recursively to investigate the pursuit space of affiliation principles. Another thought fused in TopKRules is to attempt to produce the most encouraging guidelines first. This is on account of if standards with high support are discovered before, TopKRules can raise its interior minsup variable quicker to prune the pursuit space. To play out this, TopKRules utilizes an inward factor R to store every one of the principles that can be extended to have a shot of discovering more substantial tenets. TopKRules utilizes this set to decide the principles that are the well on the way to deliver substantial standards with a high support to raise minsup all the more rapidly and prune a bigger piece of the inquiry space. The figure below shows the TopKRules algorithm:

```
TOPKRULES(T, k, minconf) R := Ø. L := Ø. minsup := 0.
1.  Scan the database T once to record the tidset of each item.
2.  FOR each pairs of items i, j such that |tids(i)| ×|T| ≥ minsup and |tids(j)| ×|T| ≥ minsup
3.      sup({i}→{j}) := |tids(i) ∩ tids(j)| / |T |.
4.      sup({j}→{i}) := |tids(i) ∩ tids(j)| / |T|.
5.      conf({i}→{j}) := |tids(i) ∩ tids(j)| / |tids(i)|.
6.      conf({j}→{i}) := |tids(i) ∩ tids(j)| / |tids(j)|.
7.      IF sup({i}→{j}) ≥ minsup THEN
8.          IF conf({i}→{j}) ≥ minconf THEN SAVE({i}→{j}, L, k, minsup).
9.          IF conf({j}→{i}) ≥ minconf THEN SAVE({j}→{i}, L, k, minsup).
10.         Set flag expandLR of {i}→{j}to true.
11.         Set flag expandLR of {j}→{i}to true.
12.         R := R∪{{i}→{j}, {j}→{i}}.
13.     END IF
14. END FOR
15. WHILE ∃r ∈ R AND sup(r) ≥ minsup DO
16.     Select the rule rule having the highest support in R
17.     IF rule.expandLR = true THEN
18.         EXPAND-L(rule, L, R, k, minsup, minconf).
19.         EXPAND-R(rule, L, R, k, minsup, minconf).
20.     ELSE EXPAND-R(rule, L, R, k, minsup, minconf).
21.     REMOVE rule from R.
22.     REMOVE from R all rules r ∈ R | sup(r) <minsup.
23. END WHILE
```

Figure 3: Top K Rules Algorithm

Here we completed the proposed technique section where the hardware components and the technique used in making the proposed EDR. The next section helps in briefly explaining the simulation of the technique

III. SIMULATION

In this section of the paper, we are going to briefly describe the implementation of the proposed EDR technique. The figure below shows the data flow of the proposed system.

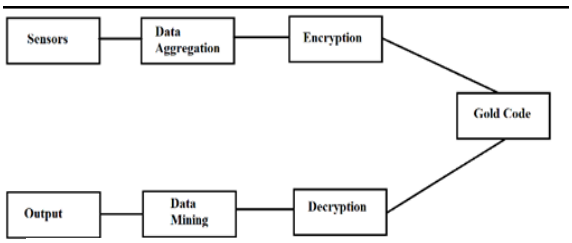

Figure 3: Flow Diagram of the proposed system

As we can observe from the above illustration, first of all, we have to sense the data for which all the sensors explained above like the temperature, alcohol, GPS are fixed on the ARM processor kit. We have to give the input to the sensors. For example, the GPS sensor will detect the current location of the system and will store it, similarly, all the sensors will detect the input and will store it to send it for analysis. Once the input is ready the system sends a request to the data aggregation module. This module will then checks the input of the sensor as explained by the algorithm in the paragraphs above and if the input values passed the threshold test then they are sent for further processing. For example let us assume we have a threshold of 1 and the inputs are 25, 26, 27, 28. Then the difference is checked and values 25, 27, 28 are sent for analysis.Since the data is sensitive and needs to be safe we have applied an encryption algorithm to do safeguard the data against intruders. To encrypt the data RC6 encryption is applied. To optimize the performance of the algorithm the system uses gold code. Once the data is sent and received at the storage point it is then decrypted using the information available and is stored in the databases in the same format sent. This data now can be used by analysts to scrape knowledge. To extract the knowledge we have used TopKRules algorithm which will find patterns/rules which can satisfy the demand. Once the rules are found they can be easily studied for analysis. This is the simulation of the proposed system, now in the next section, the results which we observed while testing the system are present.

IV. RESULT

This section of the paper illustrates the observed results while testing the proposed system

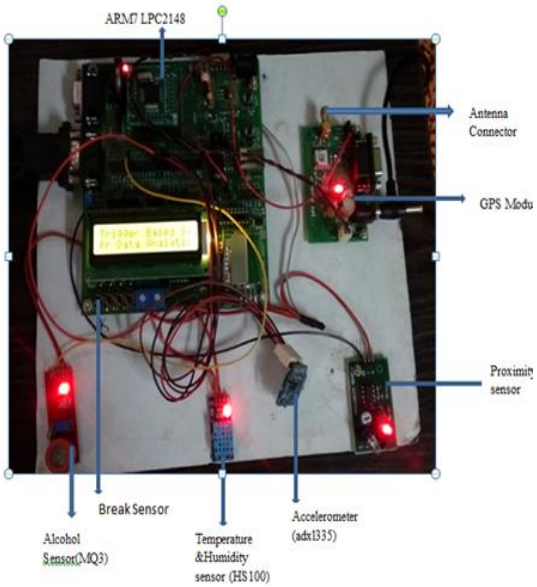

Figure 4: Hardware shot of the proposed system

The above figure illustrates the arrangement of the hardware present in our proposed system. It contains all the components explained in the proposed system section of the paper.

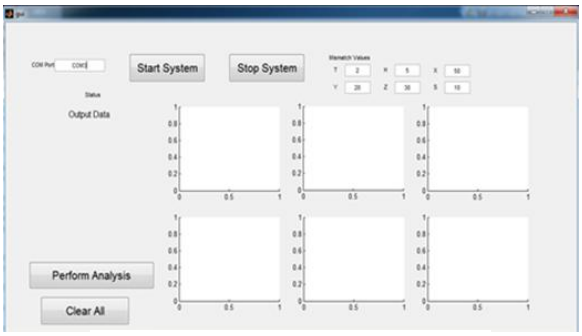

Figure 5: GUI of the analysis system

As observed the above figure is the screenshot of the analysis software created. It can start and stop the sensing system i.e. hardware part. Also, it displays the output values of the sensors and graphs of the analysis.

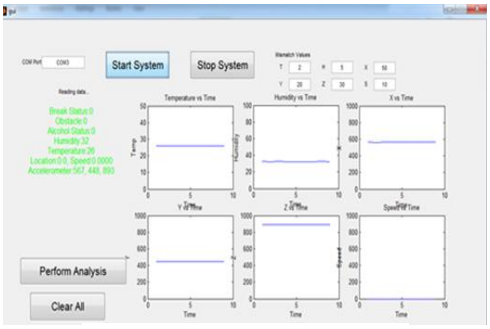

Figure 6: Sensing of the Input

The above figure depicts the start system button when the button is pressed the sensors are refreshed and are ready to sense the input the green color shows that the sensors are waiting to sense the surrounding input.

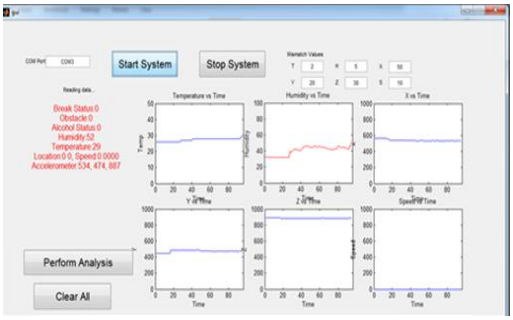

Figure 7.1: Analysis of humidity values

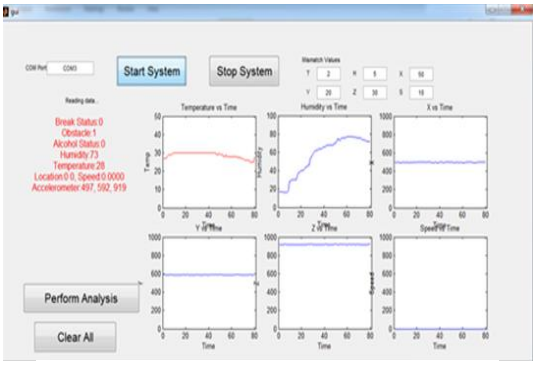

Figure 7.2: Analysis of temperature values

The above figures shows the humidity in(%)and temperature values in (^{o}C)which are inputted and the graphs showing temperature VS Time and humidity VS time plots. Similarly, all the values from the sensors are tested.

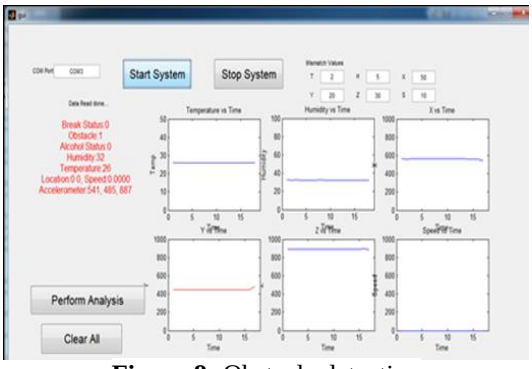

Figure 8: Obstacle detection

The above figure shows obstacle detection.As front obstacle gets detected by PIR sensor status of obstacle displays its value as 1 in red colour otherwise it is 0 at a time of no obstacle detection.

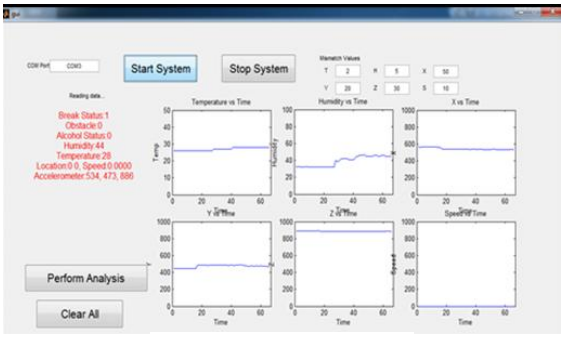

Figure 9: Break Pressed

The above figure shows Break status. As Vehicle is in motion and driver applies break at a certain instant then our status of Break displays its value as 1 in red colour otherwise it is 0 at a time of no Break Applied.

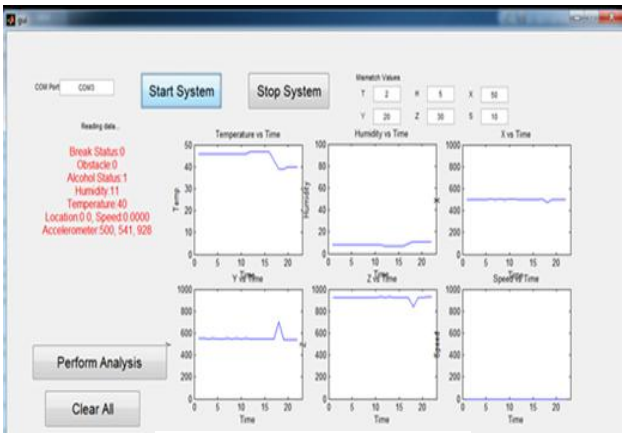

Figure 10: Alcohol detection

The above figure shows Alcohol status, Likewise applied for Alcohol detection if driver is drunk then GUI Analysis software display Alcohol status as 1 and we can say driver consumed alcohol about 300mg/liter otherwise 0.

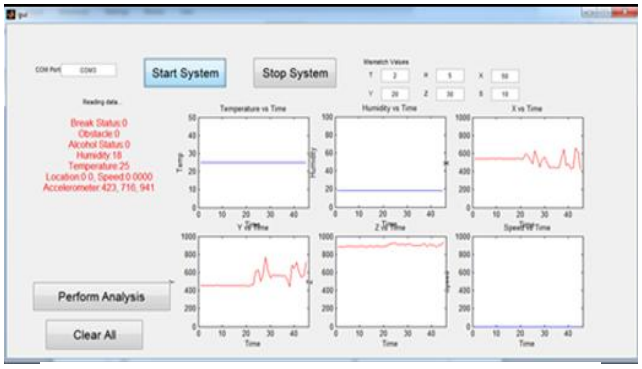

Figure 11: Analysis of Accelerometer(x,y,z)Values

The above figure shows the Accelerometer[x,y,z] values voltage outputs which are inputted and the graphs showing [x,y,z] VS Time plots. Similarly, all the values from the sensors are tested with signal conditioned voltage outputs.

Figure 12: Getting latitude and longitude values (Location) & getting speed

The above figure shows latitude and longitude values i.e we can know the location of vehicle and also the speed in (m/s) with which the vehicle was moving from source to destination at each instant of time with help of GPS module.

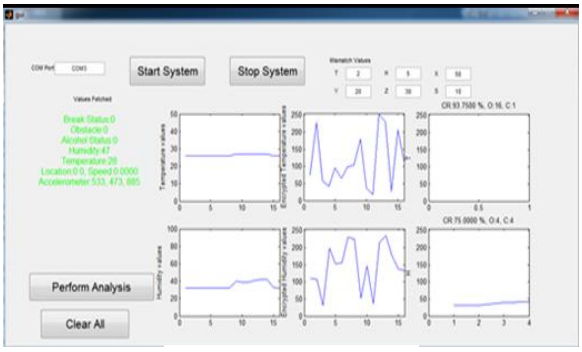

Figure 13: Stop system

When the system is stopped the values are stored and the data is then encrypted, it also shows the status of the encryption i.e. how many bytes of data is encrypted.

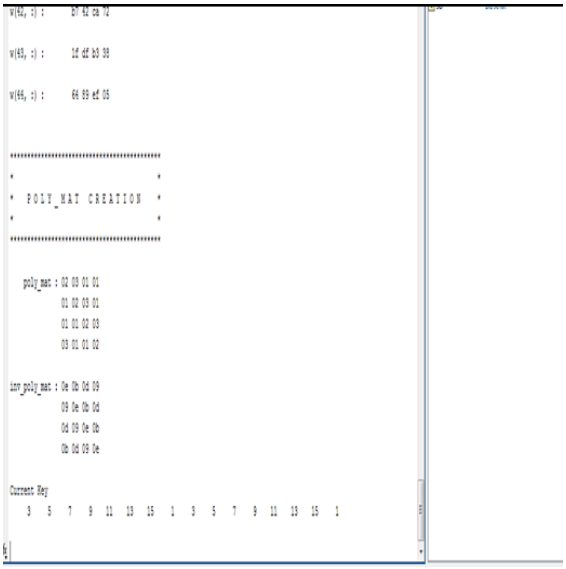

Figure 14.1: Modifying keys at run time while Performing Analysis (Gold code Optimization)

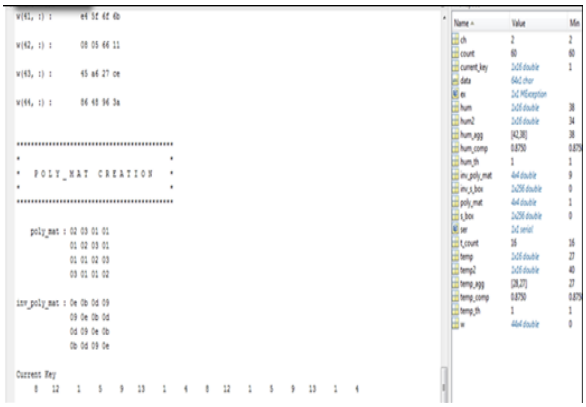

Figure 14.2: Changing keys at run time while performing Analysis (Gold Code Optimization)

The gold code function optimized the key by modifying it changing its value at run time, getting random key at each instant until analysis is done.

	A	B	C	D	E	F	G	H	I	J	K
1	Temp(+C)	Hum(%)	X(cm)	Y(cm)	Z(cm)	Speed(m/s)	Obstacle	Break	Alcohol	Time	
2	27	34	456	537	931	17	0	0	0	22.02.17 08.52.03	
3	27	34	455	533	927	15	0	0	0	22.02.17 08.52.05	
4	29	34	455	533	925	20	0	0	0	22.02.17 08.52.10	
5	30	40	456	533	924	26	0	0	0	22.02.17 08.52.13	
6	31	41	456	536	926	29	0	0	0	22.02.17 08.52.15	
7	32	43	458	537	928	30	0	0	0	22.02.17 08.52.17	
8	32	47	455	532	929	36	0	0	1	22.02.17 08.52.19	
9	32	48	460	535	924	37	0	0	1	22.02.17 08.52.21	
10	32	47	453	535	927	40	0	0	1	22.02.17 08.52.23	
11	30	47	455	535	928	31	0	0	0	22.02.17 08.52.25	
12	30	49	455	533	925	29	0	0	0	22.02.17 08.52.27	
13	30	49	457	535	927	25	0	0	0	22.02.17 08.52.29	
14	28	50	454	533	926	21	0	0	0	22.02.17 08.52.31	
15	28	50	457	536	929	20	0	0	0	22.02.17 08.52.33	
16	28	52	458	535	929	17	0	0	0	22.02.17 08.52.35	
17	28	52	457	537	928	15	0	0	0	22.02.17 08.52.37	
18	28	52	455	533	925	12	1	0	0	22.02.17 08.52.42	
19	28	54	457	535	927	10	1	0	0	22.02.17 08.52.45	
20	28	54	457	535	931	0	1	1	0	22.02.17 08.52.47	
21	28	53	460	535	926	0	1	1	0	22.02.17 08.52.49	
22	28	54	460	535	926	0	1	1	0	22.02.17 08.52.51	
23	28	57	457	539	928	0	1	1	0	22.02.17 08.52.53	
24	28	58	454	533	926	16	0	0	0	22.02.17 08.52.56	
25	27	60	461	535	929	21	0	0	0	22.02.17 08.52.58	
26	27	60	455	532	927	23	0	0	0	22.02.17 08.53.00	
27	27	61	453	533	925	26	0	0	0	22.02.17 08.53.03	
28	27	59	456	532	924	37	0	0	0	22.02.17 08.53.06	
29	27	59	455	535	929	40	0	0	0	22.02.17 08.53.09	

Figure 15: Analysis of data The values are stored in excel sheets to perform analysis on then by the analyst.

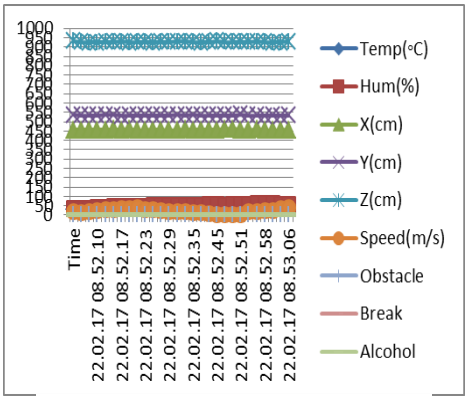

Figure16: Combined Graph vs Time

The above figure is the graph plot for the various readings of each sensor, humidity, temperature, Accelerometer(x, y ,z) values, speed, obstacle ,break, alcohol vs time instant.

	A	B	C	D	E	F	G
1	ΔT(°C)	ΔH(%)	ΔX(cm)	ΔY(cm)	ΔZ(cm)	ΔSPEED(m/s)	Time
2	0	0	1	4	4	2	22.02.17 08.52.03
3	-2	0	0	0	2	-5	22.02.17 08.52.05
4	-1	-6	-1	0	1	-6	22.02.17 08.52.10
5	-1	-1	0	-3	-2	-3	22.02.17 08.52.13
6	-1	-2	-2	-1	-2	-1	22.02.17 08.52.15
7	0	-4	3	5	-1	-6	22.02.17 08.52.17
8	0	-1	-5	-3	5	-1	22.02.17 08.52.19
9	0	1	7	0	-3	-3	22.02.17 08.52.21
10	2	0	-2	0	-1	9	22.02.17 08.52.23
11	0	-2	0	2	3	2	22.02.17 08.52.25
12	0	0	-2	-2	-2	4	22.02.17 08.52.27
13	2	-1	3	2	1	4	22.02.17 08.52.29
14	0	0	-3	-3	-3	1	22.02.17 08.52.31
15	0	-2	-1	1	0	3	22.02.17 08.52.33
16	0	0	1	-2	1	2	22.02.17 08.52.35
17	0	0	2	4	3	3	22.02.17 08.52.37
18	0	-2	-2	-2	-2	2	22.02.17 08.52.42
19	0	0	0	0	-4	10	22.02.17 08.52.45
20	0	1	-3	0	5	0	22.02.17 08.52.47
21	0	-1	0	0	0	0	22.02.17 08.52.49
22	0	-3	3	-4	-2	0	22.02.17 08.52.51
23	0	-1	3	6	2	-16	22.02.17 08.52.53
24	1	-2	7	-2	-3	-5	22.02.17 08.52.56
25	0	0	6	3	2	2	22.02.17 08.52.58
26	0	-1	2	-1	2	-3	22.02.17 08.53.00
27	0	2	-3	1	1	-11	22.02.17 08.53.03
28	0	0	1	-3	-5	-3	22.02.17 08.53.06

Figure17: Delta values (ΔT,ΔH,ΔX,ΔY,ΔZ,ΔSpeed)

The above figure shows the delta values of each sensor i.e the difference taken place(Mismatch difference) for readings of each sensor.the difference is between current and previous reading.

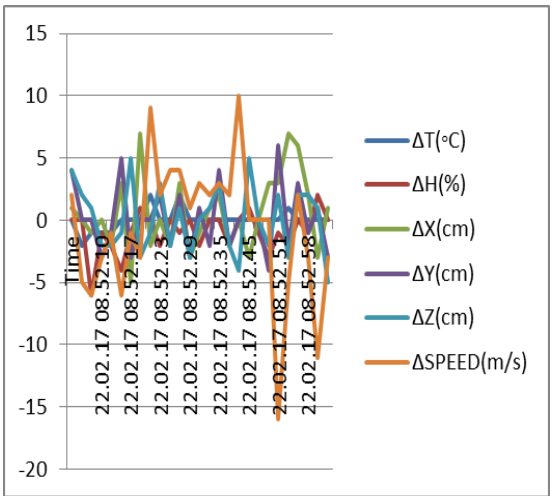

Figure 18: (Delta Values) Combined Graph vs Time The above figure is combined graph for the delta values of each sensor.

V. CONCLUSION

This paper deals with Secured EDR System for analysis of data recorded. Securing The sensed data by implementing security algorithmRC6 by modifying keys at run time using gold code function to provide safety to data by intruders and hackers .At the same time we are using top k rule for mining the data. Also we can get to know real cause with fault safety. Various sensors sense and record data by means of triggering based backup. Also the sensed information is displayed on GUI .The system provides information of vehicle parameters like location ,speed through GPS module ,Break status through break sensor, Sudden change in motion (x.y.z) direction values by Accelerometer sensor, Alcohol status by alcohol sensor, Front obstacle detection by proximity sensor, Humidity &temperature values by means of humidity & temperature sensor. Graphical comparison of different parameters wrt Time is also done.Time wise Analysis for each sensor is easier with aid of these results.This results are helpful in case of training program of driver, police investigation, insurance cases.

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 International Advance ComputingConference (IACC)

[10]. Zhixian Zhang, Zheng Wang, Haixun Wang, Kenny Q. Zhu,"Automatic Extraction of Top-k Lists from the Web",Shanghai Jiao Tong University Shanghai, China.

[11]. 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

[12]. 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.

[13]. Peter Niehoff, Hampton C. Gabler, "EVALUATION OF EVENT DATA RECORDERS IN FULL SYSTEMS CRASH TESTS", National Highway Traffic Safety Administration United States Paper No: 05-0271.

[14]. Amardeep Kumar, Arvind Upadhyay, "An Efficient Algorithm to Mine Non Redundant Top K Association Rules", IJETST- Vol.||03||Issue||01||Pages 3491-3500||January||ISSN 2348-9480.

[15]. Shahansha Quadri and Garimella Rama Murthy, "ETSHRA: Energy Efficient Threshold Sensitive Hierarchical Routing

Algorithm for Cognitive Wireless Sensor Networks", International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.

[16]. Maneesha V. Ramesh P. V. Ushakumari, "Threshold Based Data Aggregation Algorithm to Detect Rainfall Induced Landslides", Amrita University.

[17]. Mr David Connolly, "Event Data Recorder as A Forensic Tool", 4-5th September, University of Limerick, Proceedings of the ITRN2014.

[18]. Vikas Tyagi, Shrinivas Singh, "ENHANCEMENT OF RC6 (RC6_EN) BLOCK CIPHER ALGORITHM AND COMPARISON WITH RC5 & RC6", Journal of Global Research in Computer Science, Volume 3, No. 4, April 2012.

[19]. Jayshri Banpurkar, Amreen Khan, "Mining Frequent Sequential Patterns and Top Rules from Large Uncertain Database", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 05 | May-2016.

[20]. Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, "The RC6 Block Cipher", v1.1 - August 20, 1998.

[21]. Philippe Fournier-Viger, Cheng-Wei Wu and Vincent S. Tseng, "Mining Top-K Association Rules".