Analytic Hierarchy Process (AHP) to Find Most Probable Web Attack on an E-Commerce Site

P. S. Lokhande
AIKTC, Mumbai University
Navi Mumbai
MS, India
0091-9224174473
pslokhande@gmail.com

B. B. Meshram
ACM Member
VJTI, Matunga, Mumbai
MS, India
0091-9969381962
bbmeshram@vjti.org.in

ABSTRACT
Attackers are using various techniques to attack on an E-Commerce site; they do have various options to initiate attack. On other hand web administrators finding it difficult to prioritize the defense mechanism against each web attack. The Analytic Hierarchy Process (AHP) is an effective method in dealing with the situations where we need to select one among available alternatives or prioritize them according to their severity. Here we try to focus on some major type of attacks which are most offensively happening on the web-services; like Cross-Site Scripting Attack, DoS Attack, SQL Injection Attack and Man-in-Middle Attack. These top online web attack methods were chosen to decide the most probable happening attack on a website. The prposed methods shows step by step approach to find the most probable alternative that hackers could first use to do the attack.On the basis of this model the administrator can take care of it at first place.

Keywords
AHP, Web Attack, DoS, DDoS, CSS, Man-in-Middle Attack, SQL Injection Attack, E-commerce.

1. INTRODUCTION
As per OWASP the top 10 threats of year 2013 to web application security are given as follows. The OWASP listed Top 10 threats for 2013 is based on 8 datasets from 7 firms that specialize in web application security, including 4 consulting companies and 3 tools/SaaS vendors (1 Static, 1 Dynamic, and 1 with both). This dataset covers over five hundred thousand vulnerabilities across hundreds of web organizations and thousands of applications [6]. The Top 10 items are selected and prioritized according to this universal data, in combination with equated estimates of exploitability, detectability, and impact estimates. The top 10 threats are listed as follows:

1) SQL Injection Attack (SQLi)
2) Broken Authentication and Session Management Flaws.
3) Cross Site Scripting (XSS) Attack
4) Insecure Direct Object Reference Issue.
5) Security Misconfiguration Flaw.
6) Sensitive Data Exposure.
7) Missing Function Level Access Control.
8) Cross Site Request Forgery (CSRF) Attack or One Click attack.
9) Using components with known vulnerabilities in programming.
10) Unvalidated redirects and forwards to un-trusted sites.

2. LITERATURE SURVEY
Dr. Thomas L. Satty has developed Analytic Hierarchy Process (AHP) in 1970, is often referred as the Satty method. AHP helps decision-makers select the best solution from several available options and selection criteria. [1] [3] [4] [5]

ICTCS '16, March 04-05, 2016, Udaipur, India

DOI: http://dx.doi.org/10.1145/2905055.2905120

2.2 How to Know the Attackers Mind with AHP?
Attackers do have several choices to initiate attacks on target; our aim was to think the way attacker thinks before initiating the attack. For finalizing the most happening web attack and prioritizing them, we took a survey of web security experts, ethical hacker also the various crime records were referred to know the top 4 web threats. To validate the received information through survey and cyber crime record, we used AHP (Analytic Hierarchy Process) by Thomas L. Satty to rank and prioritize the four web threats based on their probability to happen on an e-commerce site. Finally the outcome of the AHP and referred data is matched to know the most probable attack.

Table-1: Scale to define the importance of criteria and alternatives (Satty's Scale) [2].

Intensity of importance	Definition	Explanation
1	Equal or same importance	Two activities share equally to the objective
3	Moderate or average importance	Expert experience and judgment slightly favour one activity over another.
5	Strong or high importance	Experience and judgment of expert strongly favor one activity over another.
7	Very strong or demonstrated importance	An activity is favored very strongly over another; its dominance proved in practice.
9	Extreme importance	The evidence favoring one activity over another having highest possible order of attestation.
2,4,6,8	Intermediate values	When compromise is needed between two activities.

3. PROPSED PRIORITIZE DEFENCE MECHANISM
Attackers are using various methods to attack e-commerce sites, web administrators are struggling to defend the it implementing various security measures for their e-commerce website and

implementing number of security patches may overload the system and downgrading the performance of application. Here we are trying to predict the next move of web attacker by using Analytic Hierarchy Process (AHP). There are many types of threats to e-commerce application but top most threat vectors for an e-commerce site that will severely hamper the creditability, privacy and performance are Data Access, Data Modification, Data Transfer and service unavailability. Based on an extensive survey of Cyber Crime cases registered at Navi Mumbai Police stations , input from various cyber security experts from industry and OWASP following threats are identified i) SQL Injection, ii) CSS iii) MiM iv) DoS and DDoS.

Analytic Hierarchy Process (AHP): Thomas L. Satty proved that AHP is the best method to choose the alternative among the available choices [3]. In the AHP method, given problem is divided into the hierarchy of criteria and alternatives [4] as shown in following Fig. 2.1

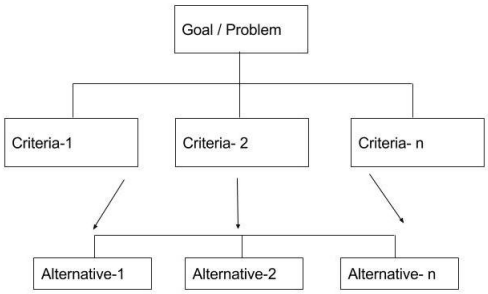

Fig.2.1 Hierarchy of Criteria and Alternatives

Using AHP Process flow, we prpose the following steps to be analysed :

1) *State the objective*: Here the objective is to find the most probable web attack.

2) *Define the criteria*: Criteria for our goal is Data Access, Data Modification, Data Transfer and service unavailability

3) *Pick the alternatives*: i) SQL Injection, ii) CSS iii) MiM iv) DoS and DDoS.

```
Algorithm:
Input:Criteria and Alternatives
Output:Best Alternative
Step 1: Explore out the alternatives and criteria
Step 2: Design the hierarchical model for problem
Step 3: Rank the alternatives on the Scale from
0 to 9
(Matrix formation for alternatives)
Step 4: Calculate Eigen vectors for formed
```

The information mentioned above for our Goal is to finalize the Objective, Criteria and Alternatives and after that this information is arranged into a hierarchy tree shown in fig. 2.2.

The information, i.e. various web threats are then projected, to determine relative ranking of alternatives both qualitative and quantitative manner. Criteria can be compared using informed judgments based on collected information to derive weights and priorities. Judgments are then used to determine the ranking of the criteria.

3.1 Basis for Deciding Pair wise Matrix and Weightage

For deciding the weightage Cyber Crime data from various sources were collected such as Navi Mumbai Cyber Crime cell, Details from newspapers, National Crime Records Bureau data portal- Ministry of Home affairs, Govt. of India, Record of Cyber crime cases registered published by Govt. of Maharashtra and finally data is sourced from various IT professionals, web security experts was taken into consideration.

Navimumbai Cyber Crime Statistics: Navimumbai Cyber Crime data shown in Table 3, there is a drastic rise in the Net banking fraud, Debit / Credit card fraud committed using the data theft, stealing the data online.

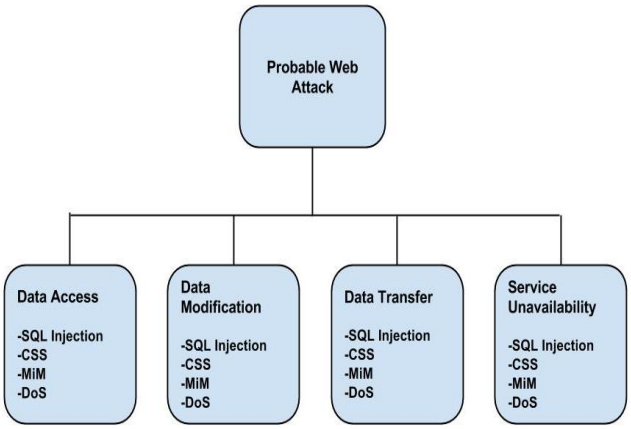

Fig. 2.2: AHP Hierarchical Model for decision making with alternatives and criteria

Table 3: Navi Mumbai Cyber Crime statistics [7]

Type of Crime	2014	2013	2012
Net banking fraud, Debit/credit card fraud	630	361	154
Email Account hacks	65	41	74
Lottery fraud	20	17	19
Face book Scams	120	87	72

From above statistics, it's been observed that more than 75% of the cyber frauds are committed by using SQL Injection, Man-In-Middle attack and Cross Site Scripting.

In News:

i) As per the police sources Credit Card fraud is the most common crime. From year 2012 to 2013, it elevated by 300% (from 8 cases to 32 cases). This year alone, seven cases were registered till March 31, roughly equal to the number of cyber crime cases registered in the year 2013.

ii) For hacking related crime, 32 cases have been registered since the year 2010, with its incidence rising from two in year 2012 to eight in the year 2013. Also, eight cyber crime cases have been registered in the first quarter of this year.

iii) Navi Mumbai has witnessed almost 60% rise in cyber crimes over the last three years [8], with card frauds, online transaction

fraud, data theft topping the list, according to the data obtained from the city police department.

iv) State-wise record of cyber crime cases registered in the year 2013 under various sections of the IT Act shows Maharashtra state on the top with 681 cases in the country, Andhra Pradesh with 635 cases and Karnataka with 513 cases. Total 426 persons were arrested in cyber crime related cases registered under IT Act in Maharashtra, as compared to 296 in Andhra Pradesh and 283 in Uttar Pradesh state [9].

National Crime Records Bureau: According to NCRB records maximum number of cyber crime cases are committed to earn money, Gaining control (Hacking), Illegal Gain (Man-in-Middle attack), Cause Disrepute (DoS and DDoS attacks).

Table 3: Cases registered under Cyber Crimes by Motives during 2013, all India record [10].

Crime Head	Yr	Greed/ Money	Cause Disrepute	Fraud / Illegal Gain	Others	Total
Cyber Crimes By Motives	2013	821	148	1240	2144	5693

Government of Maharashtra Record: Comparative information on Cyber Crime cases registered in Maharashtra state shows rise in the crime of hacking computers, web sites, and damaging computer resources for the year 2011 and 2012. Crime record also shows 192 cases out of 471 registered in the category of Hacking, Data theft, and Unlawful access to the computer system. Source: Cyber crime cases record by Govt. of Maharashtra [11]

The values of the pair wise comparisons for our problem statement are determined as per scale introduced by Saaty [1]. With reference to this scale, the available values for the pair wise comparisons are members of the set: {9, 8, 7, 6, 5, 4, 3, 2,1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9} (see table 3).

The pairwise comparison values are being classified and calculated on the basis of the data from section 3.1. Following Table: 4 can be formulated by considering all the cases which are registered in crime records.

Table 4: Total number of cases recorded in crime reports from 2012-2014

Alternatives	**No. of Cases Recorded**
SQL Injection	911
CSS	1172
MiM	1577
DoS	671

Considering the range of crime records from 300 to 2100 cases, our decision for pairwise value to construct a matrix for criteria and alternatives can be shown as- 300-500: 1, 500-700: 2, 700-900: 3, 900-1100: 4, 1100-1300:5, 1300-1500: 6, 1500-1700: 7, 1700-1900: 8, 1900-2100: 9.

As an illustrative example, consider the Table 5.

By classifying the different alternative into different criteria and by using the above range, we can say Data Access is 4 times as important as Data Modification and Data Modification is 5 times as important as Data Transfer. Same like that other value can be filled.

Table 5: Matrix A: scale to define the importance of the criteria

	Data Access	Data Modification	Data Transfer	Service Unavailability
Data Access	1/1	4/1	3/1	1/2
Data Modification	1/4	1/1	5/3	1/2
Data Transfer	1/3	3/5	1/1	8/3
Service Unavailability	2/1	2/1	3/8	1/1

3.2 Mathematical Formulation

(Steps to be followed for Solving Problem)

The structure of the typical prioritizing the defense mechanism, based on available alternatives considered in this paper. It consists of a number, say M, of alternatives and a number, say N, of decision criteria. Every alternative can be evaluated in terms of the decision criteria and their relative importance (or weight) of each criterion can be estimated as well. Let aij (i =1,2,3,....,m) and N=(1,2,3,....,n) denotes the performance value of i alternative with j criteria.

$$\begin{pmatrix} a_{11} & a_{12} & .... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ a_{31} & a_{32} & ... & a_{3n} \\ ... & ... & ... & .. \\ a_{m1} & a_{m2} & ... & a_{nm} \end{pmatrix}$$

Steps which has to be followed can be listed out as:

Step1: Find out Priority Vectors
Step2: Take successive squared powers of matrix.
Step3: Normalize the row sums. Find the difference between successive row sums
Step4: If Normalized row value is less than a pre-specified value, then Stop else go to Step2.
The comparison matrix can be formulated by the range specified in the section 3.1.

Table 6: Ranking alternatives

	SQL Injection	XSS	MiM	DoS
SQL Injection	1	7/2	5/3	4
XSS	1/5	1	1/2	4
MiM	1/5	3/2	1	3/2
DoS	1/4	1/3	2/7	1

Having a comparison matrix, priority vector matrix can be formulated as below.

Matrix A=

	SQL Injection	XSS	MiM	DoS
SQL Injection	1	3.5	1.8	4
XSS	0.2857	1	0.5	3
MiM	0.5555	1.5	1	1.5
DoS	0.25	0.3333	0.6667	1

Iteration 1 : for eigenvalue calculation

$A^2 =$

3.99	10.8	12.8275	10.8
2.0478	3.996	4.2575	5.441
6.01	7.72	3.961	5.665
4.6238	12.225	10.07	3.975

Sum of rows of matrix A = $a_{i,j}$ =

$$\begin{pmatrix} \sum a_{1,j} \\ \sum a_{2,j} \\ \sum a_{3,j} \\ \sum a_{4,j} \end{pmatrix} = \begin{pmatrix} 38.4175 \\ 15.7423 \\ 23.356 \\ 30.8938 \end{pmatrix}$$

Final Sum of Vector = $\sum a_{j,1} = V_s = 108.4096$

Equation ----------(I)

Eigen Values = $E_i = E_1 =$

$$\begin{pmatrix} \sum a_{1,j} / V_s \\ \sum a_{2,j} / V_s \\ \sum a_{3,j} / V_s \\ \sum a_{4,j} / V_s \end{pmatrix} = \begin{pmatrix} 0.3543 \\ 0.1452 \\ 0.2154 \\ 0.2849 \end{pmatrix}$$

Iteration 2 : Repeat the steps of iteration 1 for computing E_2

Now $A_1 =$

3.99	10.8	12.8275	10.8
2.0478	3.996	4.2575	5.441
6.01	7.72	3.961	5.665
4.6238	12.225	10.07	3.975

$A_1^2 =$

165.066	317.30	256.728	217.45
67.099	137.468	114.936	89.605
89.788	195.590	182.697	151.87
122.383	225.122	191.275	189.30

Sum of the row in the above matrix is E2

$$E_2 = \begin{pmatrix} 0.3524 \\ 0.1507 \\ 0.2284 \\ 0.2688 \end{pmatrix}$$

For concluding to stop iterations....

$E = E_n - E_{n+1}$

$$E = \begin{pmatrix} 0.3524 \\ 0.1507 \\ 0.2284 \\ 0.2682 \end{pmatrix} - \begin{pmatrix} 0.3524 \\ 0.1507 \\ 0.2284 \\ 0.2682 \end{pmatrix} = \begin{pmatrix} 0.0018 \\ -0.0051 \\ -0.0131 \\ 0.01667 \end{pmatrix}$$

If any negative value appears in vector then stop.

3.3 Ranking Based on Criteria: Use the scale to define importance of alternative by criteria, compared with the other alternative continue with comparisons.

3.3.1 Criteria: Data Access

The comparison matrix can be formulated by the range specified in the section 3.1

Table 7: Matrix B1- Data Access

Data Access				
	SQL Injection	XSS	MiM	DoS
SQL Injection	1/1	7/2	9/5	8/2
XSS	2/7	1/1	2/3	3/1
MiM	5/9	3/2	1/1	3/2
DoS	2/8	1/3	2/3	1/1

Scale to define importance of alternative by <<Data Access>> criteria, compared with the other alternatives

Matrix B1 can be arranged from the table 7 , Perform iteration 1 and 2 on matrix B1 to find an eigenvalue of matrix B1.

Equation---------- (II)

$$E_{B1} = \begin{pmatrix} 0.4846 \\ 0.1835 \\ 0.2281 \\ 0.1035 \end{pmatrix} - \begin{pmatrix} 0.4796 \\ 0.1850 \\ 0.2275 \\ 0.1077 \end{pmatrix} = \begin{pmatrix} 0.0050 \\ -0.0016 \\ 0.00061 \\ -0.0041 \end{pmatrix}$$

3.3.2Criteria: Data Modification

The comparison matrix can be formulated in the same way by the range specified in the section 3.1 for the criteria Data Modification.

Table 8: Matrix B2- Data Modification

Data Modification				
	SQL Injection	XSS	MiM	DoS
SQL Injection	1/1	6/2	5/9	3/2
XSS	2/6	1/1	2/8	2/3
MiM	9/5	8/2	1/1	9/2
DoS	2/3	3/2	2/9	1/1

Matrix B2 : scale to define importance of alternative by <<Data Modification>> criteria, compared with the other alternatives

Matrix B2 can be arranged from Table 8. Perform iteration 1 and 2 as below to find an eigenvalue of matrix B2.

Equation ---------- (III)

$$E_{B2}= \begin{pmatrix} 0.2590 \\ 0.1002 \\ 0.4979 \\ 0.1427 \end{pmatrix} - \begin{pmatrix} 0.4796 \\ 0.1850 \\ 0.2275 \\ 0.1077 \end{pmatrix} = \begin{pmatrix} 0.0050 \\ -0.001 \\ 0.0006 \\ -0.004 \end{pmatrix}$$

Iteration 1 Iteration 2

3.3.3 Criteria: Data Transfer

The comparison matrix can be formulated in the same way by the range specified in the section 3.1 for the criteria Data Transfer.

Table 9: Matrix – Data Transfer

Data Transfer				
	SQL Injection	XSS	MiM	DoS
SQL Injection	1/1	2/9	2/3	3/4
XSS	9/2	1/1	8/2	9/4
MiM	3/2	2/8	1/1	2/4
DoS	4/3	4/9	4/2	1/1

Matrix B3 : Scale to define the importance of alternative by <<Data Transfer>> criteria, compared with the other alternatives. Matrix B3 can be arranged from Table 9.Perform iteration 1 and 2 as below to find a eigenvalue of matrix B3.

Equation ---------- (IV)

$$E_{B3}= \begin{pmatrix} 0.120 \\ 0.521 \\ 0.137 \\ 0.220 \end{pmatrix} - \begin{pmatrix} 0.1217 \\ 0.5210 \\ 0.1381 \\ 0.2191 \end{pmatrix} = \begin{pmatrix} -0.0007 \\ -9.6486 \\ -0.0008 \\ 0.00104 \end{pmatrix}$$

Iteration 1 Iteration 2

3.3.4 Criteria: Service Unavailability

The comparison matrix can be formulated in the same way by the range specified in the section 3.1 for the criteria Service Unavailability.

Table 10: Matrix Service Unavailability

Service Unavailability				
	SQL Injection	XSS	MiM	DoS
SQL Injection	1/1	2/4	2/4	2/9
XSS	4/2	1/1	4/3	3/8
MiM	4/2	3/4	1/1	3/7
DoS	9/2	8/3	7/3	1/1

Matrix B4 : scale to define importance of alternative by <<Service Unavailability>> criteria, compared with the other alternatives.

Matrix B3 can be arranged from Table 9. Perform iteration 1 and 2 as below to find an eigenvalue of matrix B4.

Equation----------V

$$E_{B4}= \begin{pmatrix} 0.1032 \\ 0.2142 \\ 0.1911 \\ 0.4913 \end{pmatrix} - \begin{pmatrix} 0.1033 \\ 0.2140 \\ 0.1914 \\ 0.4911 \end{pmatrix} = \begin{pmatrix} -3.9868 \\ 0.00013 \\ -0.0002 \\ 0.00015 \end{pmatrix}$$

Iteration1 Iteration 2

Now we have all alternatives ranking distribution, Considering equation I, and Iteration 1 of the equation II,III,IV and V a final Alternative Ranking Distribution can be shown in fig. 3.

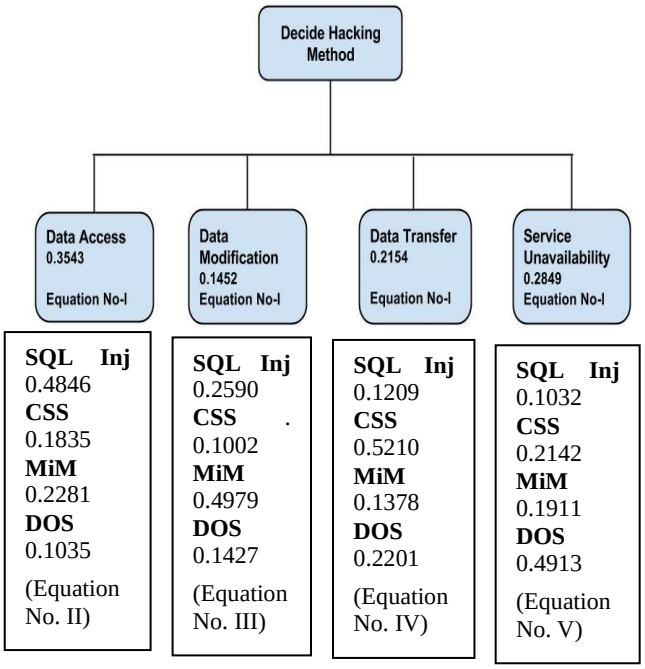

Fig.3.0 Final Alternative Ranking Distribution

Final calculation to find the most vulnerable attack from the four alternatives chosen can be calculated as below by considering Fig 3.0.

Priority Based on Ranking of Criteria and Alternatives

DA= Data Access, DM=Data Modification, DT=Data Transfer, SU= Service Unavailanility.

	DA	DM	DT	SU
SQL Injection	0.4846	0.259	0.1209	0.1032
CSS	0.1835	0.1002	0.521	0.2142
MiM	0.2881	0.4979	0.1378	0.1911
DOS	0.1035	0.1427	0.2201	0.4913

X

0.3544	=	0.2651
0.1452		0.2534
0.2154		0.2376
0.2849		0.2454

Lowest Ranking High Priority

According to Satty [1] results from the priority based model is depend on the ranking and priority calculated. The alternative with least ranking will be having the highest priority to occur. As discussed in the above table, all the four alternatives priorities are very close. The alternative, MiM have the lowest ranking with highest priority. So, Hackers commonly go with Man In the Middle Attack which is having the highest priority and after that DoS and DDoS, CSS and Finally SQL Injection attack

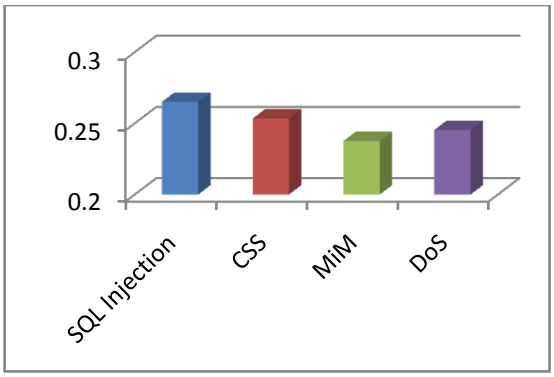

Fig. 3.1 Attack priority- Lowest ranking highest priority

4. CONCLUSION

In this work we used AHP to hack the hacker's mind, i.e. thinking the way a hacker thinks. Here we tried to focus on a few major types of attacks. With the help of AHP method, we zeroed on the most probable attack method that an attacker may use to attack. Through AHP we found that Man-In-Middle attack has most probably used by attacker.

5. REFERENCES

[1] Thomas L. Saaty, "Decision making with the analytic hierarchy process", Int. J. Services Sciences, Vol. 1, No. 1, 2008, Inderscience Enterprises Ltd.

[2] John K. Waters, "More attackers targeting e-commerce and Web apps, says Symantec", ADTMAG,

[3] Thomas L Saaty, "How to Make a Decision: "Analytic Hierarchical Process", European Journal of Operational Research, 48,(1990) 9-26, North Holland.

[4] Evangelos Triantaphyllou, Stuart H. Mann, "Using the Analytic Hierarchy Process For Decision Making In Engineering Applications: Some Challenges", Inter'l Journal of Industrial Engineering: Applications and Practice, Vol. 2, No. 1, pp. 35-44, 1995.

[5] Thomas L Saaty, "Decision-making with the AHP: Why is the Principal Eigenvector Necessary", European Journal of Operational Research, 145 (2003) 85–91, Elsevier -2003.

[6] OWASP Top 10 web application Threats : Accessed online https://www.owasp.org/index.php/Top_10_2013-Introduction

[7] Navimumbai cyber crime record published in Mid-Day , Feb 2015 http://www.mid-day.com/articles/cyber-crime-doubles-in-navi-mumbai-in-2-years/15989157

[8] Rise in cyber crime cases by 60%- Times of India http://timesofindia.indiatimes.com/city/navi-mumbai/Navi-Mumbai-witnesses-spurt-in-cyber-crime-cases/articleshow/44986732.cms

[9] Cyber crime cases continue to rise- Times of India. http://timesofindia.indiatimes.com/india/Cyber-crime-cases-under-IT-Act-continue-to-rise-shows-govt-data/articleshow/46683053.cms

[10] National Crime Records Bureau data portal- Ministry of Home affairs, Govt. of India. https://data.gov.in/catalog/cases-registered-under-cyber-crimes-motives

[11] Government of Maharashtra, Cyber crime cases registered. http://mahacid.com/Chapter-18%20(408-417)%20Computer%20crime,%20Cyber%20crime.pdf