Modeling and Minimization of Cyber Attacks through Optimization Technique

Narander Kumar, Rashmi Singh and Vipin Saxena
Department of Computer Science
Babasaheb Bhimrao Ambedkar University
Lucknow (U.P.),226025, India

ABSTRACT
In the daily routine work on the internet, the people are using the services like email, money transfer, accessing of web pages, social networking, downloads, communication on network, etc. Hackers are hacking the web pages, emails, etc which are reported in the cyber police station. The present work is based upon the cyber attacks in the Indian scenario and different cyber attacks have been identified and these attacks are optimized by applying a well known optimization technique known as Hungarian method which is based upon that the number of person are affected with minimization losses delete. A well known Unified Modeling Language (UML) modeling is also used to design the UML activity model which is validated through a Finite State Machine (FSM) technique and observed that the proposed method is optimized method for getting minimum losses across the network which is based upon distributed computing network.

Keywords
Modeling, Cyber Attacks, Hungarian, Optimization, UML and FSM

1. RELATED WORK
In the present paper, a well known Platform Independent language is used to construct various UML models. UML stands for Unified Modeling Language and invented by Booch et al. [1-2]. They described all the important diagrams related to static and dynamic representation of the research problem. OMG [3-4] is the Object Management Group who has released various versions of UML. The modeling is necessary for representing the research problem in the pictorial way and thereafter coder develops the code for the proposed model. Since, the present work is related to the Cyber Security models therefore let us describe some important contribution done by the researchers in these field. Communal Analysis Suspicion Scoring (CASS) for generating numeric suspicion scores are well described by Phua et al.[5] for the streaming of the credit card applications. Baber et al.[6] stated that computer conditions(tablets and computers) lead to faster performance when compared with paper conditions while there was no difference in content and quality of reports. Cetin et al.[7] described the recent developments in technology used by youngsters which are increasingly creating environments in which students can exhibit bullying behaviors in schools via electronic devices. Cyber bullying and Cyber victim can be used as scale for determining the level of exposure to or exhibiting cyber bullying behaviors among students in high school. Daman and Ozecilik[8] described a novel combination of the two well known meta heuristic approaches, namely the Genetic algorithm and the Scatter search which can be applied to improve the credit card fraud detection solution. Jamieson et al.[9] described a deep understanding of identification of crime by using the concept of hierarchical classes and explained clear structure for crime management. All these are defined as per the current status of law and proposed a solution for the minimization of the crime. Solms and Niekerk[10] described that Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cyber security, on the other hand, is not necessarily only the protection of cyberspace, but also the protection of these function in cyberspace and any of their assets that can be reached via cyberspace. Tehrane et al. [11] described Cyber terrorism is a transnational crime; it should be subjected to universal jurisdiction through multinational cooperation. The most suitable method to counter future transnational crimes such as cyber terrorism is universal jurisdiction. Maskun et al. [12] stated that Internet has become a global phenomenon; numerous advantages and disadvantages (crimes) which are being gotten and committed through the internet. To cope with both advantages and disadvantages, cyber security is needed to guarantee people to use internet safely.

The present work is based upon the identification of the major cyber attacks which are faced by the users in the daily routine work and losses due to attacks are computed and thereafter an optimization technique is used for the minimization of the losses. UML is also used for a model based on the minimization of the losses and the model is also validated through the FSM technique.

2. UML MODELING

A UML activity diagram is designed for the minimization of individual loss to the department and also consolidated loss to the organization. The steps involved for the minimization of losses are summarized below:

Step 1: Identify the types of page which should fit within a rectangle of Cyber Attacks & let us consider there are N;

Step 2: Categorize and fix the Priority of Cyber attacks which can be minimized for loss i.e. arrange in the decreasing order which shows that the maximum loss shall be minimized first;

Step 3: If the prioritized losses are already minimized then go to step 1 else follow the next step 4;

Step 4: Compute % loss to the user;

*Step 5: Design a matrix of N*N order where N is the different types of Cyber Attacks;*

Step 6: Apply the algorithm to optimize the loss due to the Cyber Attacks;

Step 7: Compute the minimization loss to the users and to the organization.

The above steps are represented through UML activity diagram and shown in the figure 1. It consists of six major activities which are controlled by one condition. The Hungarian method is applied after creation of NxN matrix and the cells represent percentage of loss. The data is considered for the twelve major cyber attacks and proposed steps can handle the data upto N numbers of cyber attacks. A mathematical formulation of the problem is also done for the Hungarian method as it supports for N numbers of cyber attacks. After that a matrix for NxN is generated and it can be easily programmed for finding the minimum percentage of loss.

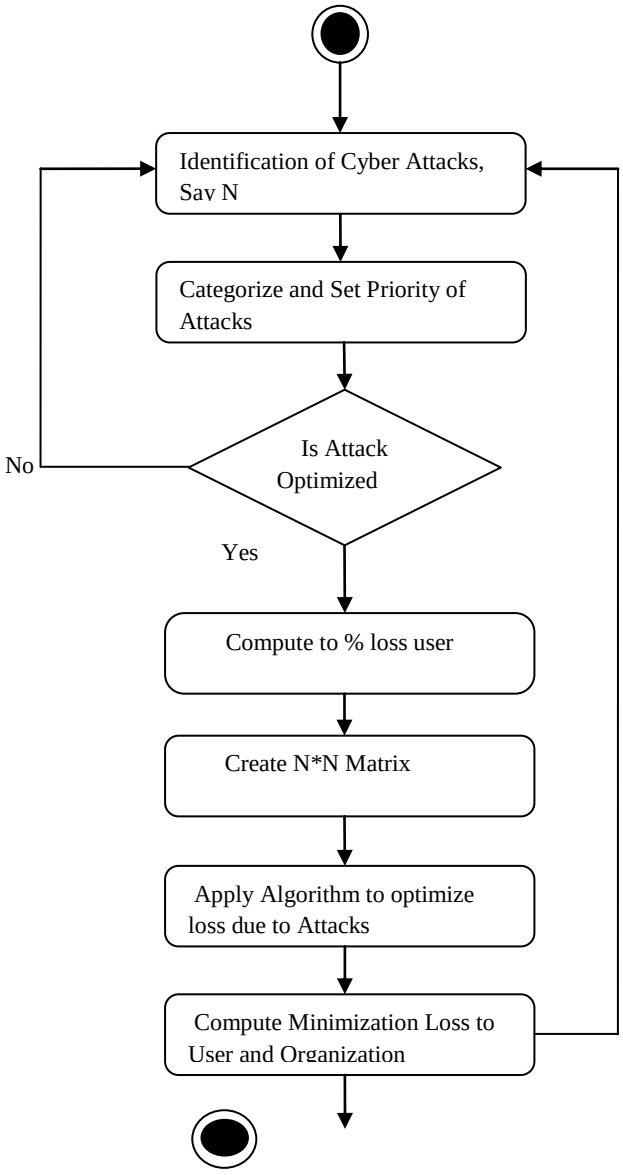

Figure 1 UML Activity Representation

3. MATHEMATICAL FORMULATION

Let Cyber attacks are categorized by the set CA= {CA_1 , CA_2, CA_3 ,……CA_N}. Let these attacks are detected and taken upto N attacks and due to these attacks let losses are L_1,L_2,L_3…….L_N then to minimize these losses the following objective function is formulated

$$Z=\text{Min} \sum_{i=1}^{N} L_i * CA_i$$

Then the problem is converted into N*N matrix and in this case N is covered as N=12 and attacks are shown in table 1.

Table 1. List of Cyber Attacks

Code	Description
CA_1	Stealing of Database
CA_2	Hacking of Websites
CA_3	Job Scams/Frauds
CA_4	Mobile Crimes
CA_5	Antisocial Activities
CA_6	Stealing of Bandwidth
CA_7	Cloning of Debit/Credit Card
CA_8	E-Commerce Fraud
CA_9	Unauthorized Network Access
CA_{10}	Theft of Password
CA_{11}	Identity Theft
CA_{12}	Cyber Blackmailing/Harassment

The different departments are consulted to make loss table as shown in table 2 and it is based upon the sample questionnaire and survey is completed for the 100 users but for computation purpose same size is considered as N=12. The steps for Hungarian method are described below in the object-oriented form:

Step 1:- Let us define obj.A[i][j], where i=1(1)12,j=1(1)12 and store the losses in 12x12 matrix A[i][j];

Step 2:- Select Min A[i][j] for each row i and subtract it from each element of each row of A[i][j] i.e. obj.A[m][j]=obj.A[m][j]-min A[m][j] where m=1(1)12 and update obj.A[i][j];

Step 3:- Select Min A[i][j] for each column j and subtract it from each element of each column of A[i][j] i.e. obj.A[i][n]=obj.A[i][n]-min A[i][n] where n=1(1)12 and update obj.A[i][j];

Step 4:-Cut the lines row wise first & then column wise with coverage of maximum zeros.

Step 5 :- If number of cut lines are equal to the order of matrix then encircle zero in each row for finding the minimum loss and remaining zeros are discarded in that row/column.

Step 6 :- Select minimum element from non cut lines, subtract it from each element and add it at intersection of cut lines, update obj. A[i][j] go to step 4, till number of cut lines are equal to order of matrix N.

Table 2 Data Representation of Cyber Attacks versus Departments

Deptt→ Cyber Attacks↓	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}
CA_1	20	30	20	20	30	40	20	30	40	50	30	20
CA_2	60	70	50	70	50	65	35	45	55	60	65	75
CA_3	10	20	15	25	35	25	15	35	10	20	25	35
CA_4	75	60	70	45	55	60	60	75	65	55	45	50
CA_5	25	35	25	30	40	35	30	25	20	30	35	40
CA_6	15	25	10	15	25	30	25	15	20	25	15	20
CA_7	40	30	35	30	20	25	30	30	25	20	30	20
CA_8	50	60	40	50	40	30	35	45	35	35	40	45
CA_9	15	25	15	25	15	25	25	35	25	35	45	25
CA_{10}	40	50	60	50	40	60	55	65	45	55	65	55
CA_{11}	15	25	15	25	35	30	15	20	25	15	20	30
CA_{12}	40	50	45	55	35	45	50	55	45	35	25	35

Table 3. Final Matrix After Applying Hungarian Method

Deptt→ Cyber Attacks↓	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_{11}	D_{12}
CA_1	0	0	0	0	10	20	0	5	20	30	0	**0**
CA_2	25	25	15	35	15	30	**0**	5	20	25	30	40
CA_3	**0**	0	5	15	25	15	5	20	0	10	15	25
CA_4	30	5	25	**0**	10	15	15	25	20	10	0	5
CA_5	5	5	5	10	20	15	10	0	**0**	10	15	20
CA_6	5	5	0	5	15	20	15	**0**	10	15	5	10
CA_7	20	0	15	10	0	5	10	5	5	**0**	10	0
CA_8	20	20	10	20	10	**0**	5	10	5	5	10	15
CA_9	0	0	0	10	**0**	10	10	15	10	20	30	10
CA_{10}	0	**0**	20	10	0	20	15	20	5	15	25	15
CA_{11}	0	0	**0**	10	20	15	0	0	10	0	5	15
CA_{12}	15	15	20	30	10	20	25	25	20	10	**0**	10

From the above table, minimum loss is computed for each of the department and observed that the minimum loss is to department1 which is just 10%. The overall loss to all the departments is also computed which is 25% for all twelve cyber attacks and for all the departments. These are summarized below in following table:

Cyber Attack	Deptt. No.	Minimum Loss Computed
CA_1	D_{12}	20
CA_2	D_7	35
CA_3	D_1	10
CA_4	D_4	45
CA_5	D_9	20
CA_6	D_8	15
CA_7	D_{10}	20
CA_8	D_6	30
CA_9	D_5	15
CA_{10}	D_2	50
CA_{11}	D_3	15
CA_{12}	D_{11}	25

Grand total = 300

Over all percentage loss to all departments = 25%

GENERATION OR TEST CASES:-

Let us consider the theory of automata for designing the Finite State Machine (FSM) which is defined by M and given by following

$M = (Q, \Sigma, \delta, q_0, F)$

Where

Q = finite set of states;

Σ = finite set of input symbols;

(Alphabets and Numbers);

δ = Transition between two states;

q_0 = Initial state;

F = Final state;

From the above definition of automata, a finite state diagram is represented in the figure 2. In which there are seven states represented as $Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6\}$ and these are according to the activity diagram represented in the figure1 and it is represented in the following table 4.

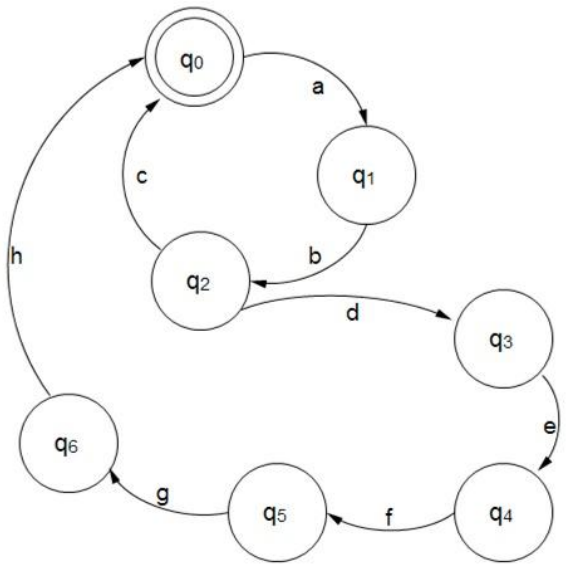

Figure 2 FSM Representation of Activity Diagram

Table 4.Representation of States

Name of State	Description of State
q_0	Identification of Cyber Attack
q_1	Categorize and set priority of Attacks
q_2	Attack optimization
q_3	Compute to % loss user
q_4	Create matrix
q_5	Apply algorithm to optimize loss
q_6	Compute minimum loss to user

Now, the transition is represented by $\delta(q_0, a)$, where a is the set of inputs and inputs are considered as

$\Sigma = \{a, b, c, d, e, f, g, h\}$ and representation is recorded in the following table 5.

Table 5.Representation of Input Symbols

Name of Input	Description of Input
a	List of Cyber Attacks
b	Priority list of Cyber Attacks
c	Not optimized list of Cyber Attacks
d	Optimized list of Cyber Attacks
e	List of losses
f	Resultant matrix with Cyber Attacks and Losses
g	Final optimized matrix
h	Minimum loss result

On the basis of above, a transition table is given below with following figure :→

$\delta(q_0,a) \rightarrow q_1$

$\delta(q_1,b) \rightarrow q_2$

$\delta(q_2,c) \rightarrow q_0$

$\delta(q_2,d) \rightarrow q_3$

$\delta(q_3,e) \rightarrow q_4$

$\delta(q_4,f) \rightarrow q_5$

$\delta(q_5,g) \rightarrow q_6$

$\delta(q_6,h) \rightarrow q_0$

Table 6. A Transition Table

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**
q_0	q_1	-	-	-	-	-	-	-
q_1	-	q_2	-	-	-	-	-	-
q_2	-	-	q_0	q_3	-	-	-	-
q_3	-	-	-	-	q_4	-	-	-
q_4	-	-	-	-	-	q_5	-	-

q_5	-	-	-	-	-	-	q_6	-
q_6	-	-	-	-	-	-	-	q_0

By the use of above grammer different test cases are generated and explained below in brief:-

Valid Test Case 1:- *Cyber attacks losses are not optimized*

It is represented by

$\delta (q_0,a) \rightarrow q_1 \quad => \quad q_0 \rightarrow a\ q_1$

$\delta (q_1,b) \rightarrow q_2 \quad => \quad q_1 \rightarrow b\ q_2$

$\delta (q_2,c) \rightarrow q_0 \quad => \quad q_2 \rightarrow c\ q_0$

After changing the states or removing the non terminals, the string is given by

$q_0 = abc\ q_0 = abc$

This represents that the Cyber Attack losses are not optimized.

Valid Test 2:- *Cyber attacks losses are optimized*

It is represented by

$\delta (q_0,a) \rightarrow q_1 \quad => \quad q_0 \rightarrow a\ q_1$

$\delta (q_1,b) \rightarrow q_2 \quad => \quad q_1 \rightarrow b\ q_2$

$\delta (q_2,d) \rightarrow q_3 \quad => \quad q_2 \rightarrow d\ q_3$

$\delta (q_3,e) \rightarrow q_4 \quad => \quad q_2 \rightarrow e\ q_4$

$\delta (q_4,f) \rightarrow q_5 \quad => \quad q_2 \rightarrow f\ q_5$

$\delta (q_5,g) \rightarrow q_6 \quad => \quad q_2 \rightarrow g\ q_6$

$\delta (q_6,h) \rightarrow q_0 \quad => \quad q_2 \rightarrow h\ q_0$

After changing the states or removing the non terminals, the string is given by

$q_0 = abdefghq_0 = abdefgh$

This represents that the cyber attack losses are optimized which is as per expectation.

4. CONCLUSIONS

From the above work it is concluded that the UML is a powerful modeling language which is used to make design of any kind of the research problem and in the above work, it is used for designing of UML activity diagram for minimization of losses from the cyber attacks. The diagram is converted into the FSM for finding the valid test cases which also validate the proposed model. A well known Hungarian approach is used to minimize the cyber attacks and it is observed that the said attacks give the percentage losses to the corresponding departments. The same work can be extended for the finite numbers of the departments and according to the list of cyber attacks and limitation is that the matrix should be NxN matrix which means that the numbers of attacks should be equal to the numbers of the departments.

5. REFERENCES

[1] Booch G., Rambaugh J., and Jacobson I., "The Unified Modeling Language User Guide", Twelfth Indian Reprint, Pearson Education, 2004. Strategies.

[2] Booch G., Rumbaugh J., and Jacobson I., "The Unified Modeling Language User Guide", China Machine Press,Beijing, 2006.

[3] OMG, "Unified Modeling Language (UML)-Version1.5", OMG document formal/2003-3-01, (2003), Needham, MA.

[4] OMG, "Unified Modeling Language Specification", http://www.omg.org (Accessed on 12th Sept. 2012), 1997.

[5] Phua C., Gayler R., Lee V. and Miles K.S., "On the Communal Analysis Suspicion Scoring for Identity Crime in Streaming Credit Applications". An European Journal of Operational Research, Vol. 195, 2009, pp. 595-612.

[6] Baber C., Smith P., Bulter M., Cross J., and Hunter J., "Mobile Technology for Crime Scene Examination". An International Journal of Human Computer Studies, Vol. 67, 2009 pp. 464-474.

[7] Cetin B., Yaman E., and Peker A., "Cyber Victim and Bullying Scale : A Study of Validity and Reliability". An International Journal of Computer & Education. Vol. 57, 2011, pp. 2261-2271.

[8] Duman E. and Ozcelik M.H., "Detecting Credit Card and Fraud by Genetic Algorithm and Scatter Search". An International Journal of Expert Systems with Applications. Vol. 38, 2011, pp. 13057-13063.

[9] Jamieson R., Land L.P.W., Winchester D., Stephens G., Steel A., Maurushat A., and Sarre R. "Addressing Identity Crime in Crime Management Information Systems: Definitions Classification, and Empirics" Computer Law & Security Review. Vol. 28, 2012, pp 381-395.

[10] Solms R.V. and Niekerk J.V. "From Information Security to Cyber Security".Elsevier publication of Computer & Security. Vol.38, 2013, pp. 97-102.

[11] Tehrani P.M., Manap N.A., and Taji H. "Cyber Terrorism Challenges: The Need For A Global Response to A Multi-Jurisdictional Crime." Elsevier publication of Computer Law &security review. Vol. 29, 2013, pp. 207-215.

[12] Maskun , Manuputty A., Noor S. M., and Sumardi J. "Cyber Security: Rule of Use Internet Safely?". Procedia Social and Behavioural Sciences. Vol. 103, 2013, pp. 255-261.