Minimize Cyber Losses in Cyber World through the Optimization Technique

Narander Kumar
Department of Computer Science, B. B. Ambedkar University (A Central University), Lucknow, UP, India

Priyanka Chaudhary
Department of Computer Science, B. B. Ambedkar University (A Central University), Lucknow, UP, India

ABSTRACT

In the modern era, internet plays crucial role in the human life. Now that time it is a backbone of human life. In Twenty-first century criminals increasingly rely on these technologies and these advance technologies are also increase day by day criminals and their criminals operations. These criminals can easily lift to Internet to carry out such type of traditional crime such as sex trafficking, illicit drug. In addition they also exploit the digital world which facilitate the crime that are often technology credit/debit card fraud intellectual property theft, identity theft, cyber bullying, identify sensitive data. So cyber crime is a very problem in our society by which there is no of information loosed. In this paper, we present an enumeration technique by which we can minimize losses through cyber crime in cyber world. In this technique we find an optimal solution. This is based on the primary data and personal (social) interaction.

Keywords

Keyword: Cybercrime, Hungarian method, Assignment problem, Cyberspace, Info Loss.

1. INTRODUCTION

In 1950, Internet is begin with development of electronic computers. The initial concept is originated packet network system in several computer science laboratories in the United States, Great Britain, and France. As early as the 1960 US Department of Defense awarded contract for packet network system including the development of ARPANET. The first message “login” sent over the ARPANET in 1969, the predecessor of today’s internet. ARPANET was designed as a communication system which provides facility to access information to one researcher computer to another researcher computer around the country. The internet has expanded far beyond the expectations of the individuals from this humble beginning who created it.

Today, internet is most important entity in our daily life. Internet is used for communication, financial transaction, research, real time updates and so on. The rapidly growth of internet, it develop the cybercrime. Cybercrime is most common type of crime act as 2010. Cybercrime is a criminal activity which is done using by the computer and internet. Personal information hacked, website hacked, cyber bullying, copied matter, card fraud, identify theft etc are under the cybercrime. Numbers of information are loosed through the cybercrime day by day. There are many disturbing things happening in cyber space today. It was just a matter of time because unauthorized person discovered advantage of computer and make it increasingly to get proprietary information of financial institution and other institution. Now a day’s computer play highly significant role in modern life so there is needed to keep secure data from unauthorized person.

2. REVIEW OF WORK

Cyber crime is considered to be as a criminal activity that uses the computer or computer network [1]. A common definition of the cyber crime is given as cyber crime is known accessing the computer without owner permission, destroying or modifying computer data and use resource without proper authorization in [2]. An instance of the cyber-crime is referred to be as a cyber-attack. Today internet is the main factor of increasing cyber crime has been discussed in [3]. By the use of internet, cyber crime is danger to the economy is described in [4]. Among the most other type of cyber crime is identify theft is one way by which unauthorized user can take advantage of these system, public defamation, cyber stalking and other social networking sites, child pornography and other type cyber of violation of copyright has been discussed in [5, 6, 7 and 8]. The cyber crime can be categorized into two types in [9] first types where one computer network attack to the other computer network – e.g. virus and second types where a computer network attack to a particular target population - e.g. fraud, identity theft. In an evolution of the internet many companies moved their business in the internet which provides services to the customer in the world wide. Credit card fraud is increasingly in recent year because many company used to request payment by these company through the internet [10].

It is clear that cyber crime in financial sector is a serious problem. In a 2011 PWC survey [11], cyber crime is ranked as the second most type of economic crime for financial sector organization and 38% for accounting of economic crime incident in 2011. A survey [12], 74.5% of financial services respondent categorized in cyber crime as a very high risk. A 2013 Verizon report [13] on data breaches noted that more than one third of all data breaches reported in the 2012 which affected to the financial organization. Now most of the company turns to the cloud computing technology by which we save money. While hype around of the benefit of ‘cloud computing’ increasing, we have faced more challenges to maintaining data, privacy and data security which is the significant vulnerabilities [14, 15]. These vulnerabilities generate a range of question which are relating to capacity of organization, relying on the cloud solution which effectively manage risk. This has become the particular case such as threats faced by the organization have moved increasingly away from indiscriminate malware to more targeted cyber attack tools [16].

From forensic computing perspective it has also been recognized as ‘cloud computing’ pose additional challenges for forensic computing specialists and discoverability and chain of evidence [17]. Progressive has been made in case of prevention of cyber crime. Botnet Detection is emerging as threat. Which are related to the cyber crime prevention and they provide a distributed platform for several illegal activities such as malware dissemination, phishing and click fraud. Cybercrime is becoming a more serious problem [18 and 19]. From the above review, there is a need of such technology which minimizes the total losses of cyberspace users. These are possible through awareness about the cyberspace security concerns and find such factors which will help to minimize the total losses. This work is based on the primary data. The primary data which is collected by the researchers on the basis of personal interactions through questionnaire. After collection the data, researcher applying the statistical approach named Hungarian method to minimize the total losses and find the feasible solution set. Through this solution set researcher find the optimal solution.

The organization of this paper is as follows. **Section 1** presents the Introduction. The review of literature has been given in **section 2**. Methodology presented in the **section 3** with formulas and algorithm as well as calculation related with Hungarian method on the collected data. Results and discussion has been given in **section 4**. **Section 5** presents conclusions and future perspectives.

3. METHODOLOGY

Methodology includes the formulas and algorithm as well as calculation related with assignment problem (Hungarian method) on the collected data as:

3.1 Formulation

Methodology includes the formulas and algorithm as well as calculation related with assignment problem (Hungarian method) on the collected data as:

3.1 Formulation

The Hungarian method is an optimization technique to solves the assignment problem in polynomial time.

Let we take ‘n’ cyber crime suffers by the ‘m’ different person on to one to one basis

Let X_{ij} denote the assignment of facility i by suffered by crime j such that

$$X_{ij} = \begin{cases} 1 & \text{if facility i is assigned to job j} \\ 0 & \text{otherwise} \end{cases}$$

Then, the mathematical model of the assignment problem may be expressed as:

The objective function is to

$$Minimize\, Z = \sum_{i=1}^{n} \sum_{j=1}^{n} c_{i,\,j}\; x_{i,\,j}$$

Where, $x_{i,\,j} = 0$ or 1 and $c_{i,\,j}$ represents the cost of assignment of resource i to activity j.

3.2 Algorithm:

1. Arrange the information in a matrix having "people" on the left and the "activity" along the top, with the "cost" for each pair in the middle.
2. Confirm that the matrix is square by the addition of dummy rows if necessary.
3. Confirm that the matrix is square by the addition of dummy column if necessary.
4. Subtract smallest element in each row & column from the corresponding row (row reduction) to create Zero elements in the cost matrix.
5. Subtract smallest element in each row column for the corresponding column. (Column reduction) create Zero elements in the cost matrix.
6. Cover zero element with minimum no of line if minimum no of line is equal to the no of rows, an optimal solution is possible.
7. If no of line is less than no of row.
8. a. Add the minimum value of uncovered element to the no at intersection of covered line.
9. b. Subtract the minimum value of uncovered element from every uncovered element in the matrix.
10. Again cover the zero elements again.
11. Select a matching value by choosing a set of zeros so that each row or column has only one selected.
12. Apply the matching value to the original matrix, disregarding dummy rows.

3.3 Implementation

In this paradigm we use assignment problem to find optimize solution. Here it create zero in each row and column by subtracting smallest element of the row and column is called row minimization and column minimization

Assignment problem is a special type of problem of the transportation problem in which ‘N’ different crime are suffered by the ‘M’ different person.

Table 1: Different areas of cybercrimes, which are taken in present analysis, are as:

C1	Personal info hacked
C2	Tax fraud
C3	Website hacked
C4	Copied book matter
C5	Audio music copied
C6	Video music copied
C7	Loan fraud
C8	Cyber bullying
C9	Credit/debit card info hacked

Table 2: Different Types of person which are suffered by the cyber crime

P1	Research scholar
P2	PG student
P3	Professional PG Student
P4	UG student
P5	Diploma student
P6	Education dept.
P7	Government employee
P8	Private employee
P9	House women

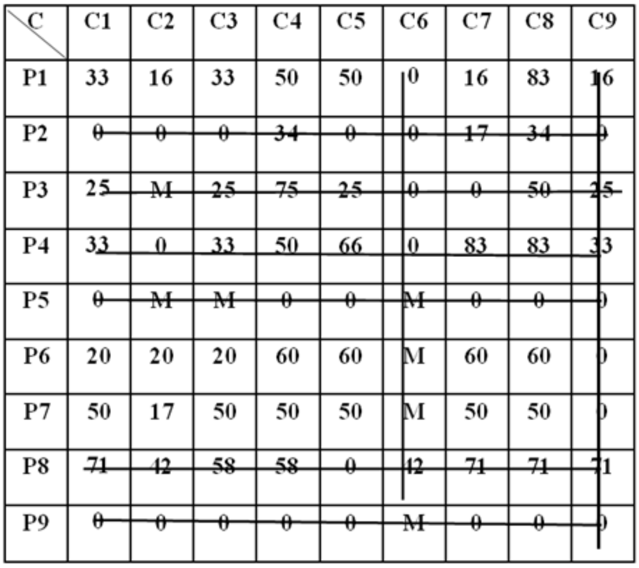
Table 3: The matrix contains data in percentage of cyber loss due to the cyber crime on the basis of primary data collected.

	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	50	33	50	67	67	17	33	100	33
P2	33	33	33	67	33	33	50	67	33
P3	50	M	50	100	50	25	25	75	100
P4	50	17	50	67	83	17	100	100	50
P5	100	M	M	100	100	M	100	100	100
P6	60	60	60	80	100	M	100	100	40
P7	83	50	83	83	83	M	83	83	33
P8	100	71	86	86	29	71	100	100	100
P9	100	100	100	100	100	M	100	100	100

Since assignment problem through Hungarian method is used to assign the workload or job in respect of optimized fashion on the one to one basis. In this paper, we show the percentage of losses in the table 3. Each cell of table 3 shows the percentage of losses. First column represents the different types of person which are suffered due to the cyber crime and row 1 represent different areas of cybercrimes, which are taken in present analysis. With the help of the Hungarian method we minimize these cyber losses which represents by each cell in the table 3. Where M represents (in the table 3) that no one suffered by cyber crime. Now we create a zero value in each row and column by subtracting by minimum no in each row and column. It is called row minimization and column minimization.

In the table 3 the value 17 is the minimum percentage of losses in the first row, we subtract the value 17 in each and every cell in the first row. The value 33 is minimum percentage of losses of second row now subtract the value 33 value in each and every cell in second row. Then repeat this procedure in third row the value 25, and in forth row the value 17, in fifth row the value 100, in sixth row the value 60, in seventh row the value 33, in eighth row the value 29, till last in ninth row the value 100. Find the resultant table 4.

Table 4: After performing theses operation (row minimization)



C	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	33	16	33	50	50	0	16	83	16
P2	0	0	0	34	0	0	17	34	0
P3	25	M	25	75	25	0	0	50	25
P4	33	0	33	50	66	0	83	83	33
P5	0	M	M	0	0	M	0	0	0
P6	20	20	20	60	60	M	60	60	0
P7	50	17	50	50	50	M	50	50	0
P8	71	42	58	58	0	42	71	71	71
P9	0	0	0	0	0	M	0	0	0

In this method there is not requiring to column minimization. After row minimization zero is contained in each row and column. Now we covering all zero's through the minimum horizontal line and vertical line.

Here 6 horizontal lines and 2 vertical line.

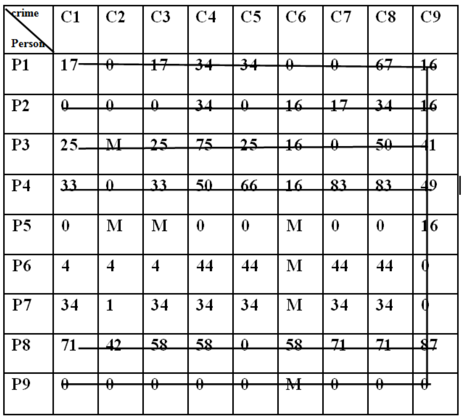
The order of the matrix is 9 x 9. Therefore N ≠ n.

Here N is the no of horizontal line and vertical line and n is order of matrix.

Now in the uncrossed cell, the minimum value of loss is selected and subtracted for the remaining uncrossed cell by the selected minimum value of loss and intersection of horizontal and vertical line the minimum value of loss should be added.

Here value 16 is the minimum loss so 16 is subtract from uncrossed cell and 16 is added in intersection of horizontal and vertical line.

Table 5: Now after performing these operations resultant matrixes



crime Person	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	17	0	17	34	34	0	0	67	16
P2	0	0	0	34	0	16	17	34	16
P3	25	M	25	75	25	16	0	50	41
P4	33	0	33	50	66	16	83	83	49
P5	0	M	M	0	0	M	0	0	16
P6	4	4	4	44	44	M	44	44	0
P7	34	1	34	34	34	M	34	34	0
P8	71	42	58	58	0	58	71	71	87
P9	0	0	0	0	0	M	0	0	0

We covering all zero's through the minimum horizontal line and vertical line.

Here 7 horizontal lines and 1 vertical line.

The order of the matrix is 9 x 9. Therefore N ≠ n.

Here N is the no of horizontal line and vertical line and n is order of matrix.

Now in the uncrossed cell, the minimum loss is selected and subtracted for the remaining uncrossed cell by the selected minimum loss and intersection of horizontal and vertical line the minimum loss should be added.

Here 1 is the minimum loss so 1 is subtracting from uncrossed cell and 1 is added in intersection of horizontal and vertical line.

Table 6: After performing these operations the resultant matrix:-

	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	17	0	17	34	34	0	0	67	17
P2	0	0	0	34	0	16	17	34	17
P3	25	M	25	75	25	16	0	50	42
P4	33	0	33	50	66	16	83	83	50
P5	0	M	M	0	0	M	0	0	17
P6	3	3	3	41	41	M	41	41	0
P7	33	0	33	33	33	M	33	33	0
P8	71	42	58	58	0	58	71	71	88
P9	0	0	0	0	0	M	0	0	1

We covering all zero's through the minimum horizontal line and vertical line.

Here 6 horizontal lines and 2 vertical line.

The order of the matrix is 9 x 9. Therefore N ≠ n.

Now in the uncrossed cell, the minimum loss is selected and subtracted for the remaining uncrossed cell by the selected minimum loss and intersection of horizontal and vertical line the minimum loss should be added.

Here value 3 is the minimum loss so value 3 is subtracting from uncrossed cell and 1 is added in intersection of horizontal and vertical line.

Table 7: After performing these operation the resultant matrix is

	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	17	3	17	34	34	0	0	67	20
P2	0	3	0	34	0	16	17	34	20
P3	25	M	25	75	25	16	0	50	45
P4	30	0	30	47	63	13	80	80	50
P5	0	M	M	0	0	M	0	0	20
P6	0	3	0	38	38	M	38	38	0
P7	30	0	30	30	30	M	30	30	0
P8	7	45	58	58	0	58	71	71	91
P9	0	3	0	0	0	M	0	0	4

Here 9 is the horizontal line and order of matrix is 9. Therefore N = n

Table 8: Condition is satisfied so the optimal assignment can be done.

	C1	C2	C3	C4	C5	C6	C7	C8	C9
P1	17	3	17	34	34	[0]	~~0~~	67	20
P2	[0]	3	~~0~~	34	~~0~~	16	17	34	20
P3	25	M	25	75	25	16	[0]	50	45
P4	30	[0]	30	47	63	13	80	80	50
P5	~~0~~	M	M	[0]	~~0~~	M	~~0~~	~~0~~	20
P6	~~0~~	3	[0]	38	38	M	38	38	~~0~~
P7	30	~~0~~	30	30	30	M	30	30	[0]
P8	7	45	58	58	[0]	58	71	71	91
P9	~~0~~	3	~~0~~	~~0~~	~~0~~	M	~~0~~	[0]	4

From the table 8, P1 is the victim of cyber crime activity and C6 i.e. video music copying the loss percentage is minimum in the first row. Similarly, P2 is the victim/sufferer of the cyber crime activity C1 i.e. personal information hacked is minimum in the second row. So the Table 8 represents the optimal solution set of minimum percentage of losses.

The total minimum percentage of losses

= P1C6 + P2C1 + P3C7 + P4C2 + P5C4 + P6C3 + P7C9 + P8C5 + P9C8

= 17 + 33 + 25 + 17 + 100 + 60 + 33 + 29 + 100

= 414

Primary data collection (Sample size) is 39. Therefore 414/30=10.61. So 10.6 % of minimize the losses percentage of the cyber crime through the assignment problem using Hungarian method.

4. RESULTS AND DISCUSSION

No one can deny that internet can change our life, society and culture. Increasing growth of internet, generate different type of cyber crime .In this paper, we have collect primary data through the different field of person which are suffered from different types of cyber crime. After collecting data we create a matrix with these data and applying assignment problem through Hungarian method on the collected data to minimize the loss caused by cyber crime. We can find that 10.6% losses of cyber crime minimize through the assignment problem.

5. CONCLUSIONS AND FUTURE PRESPECTIVES

Internet and computer is most common entity and used in our society, this technology has develop a new type of crime i.e.; Cybercrime. Cybercrime is major issue in the use of internet. Eradication of cyber crime is very difficult. So prevention is very useful. After using an assignment problem we have find the minimum losses of cyber crime in different areas as mentioned in this paper. We find the feasible solution set of minimum losses from specific areas and then we can find the optimum solution of losses.

For the future use assignment problem handle with different or other areas of implementation and takes more response. So we can use different other technique to used to find minimum losses of cyber crime.

6. REFERENCES

[1] Yanping Zhang, Yang Xiao, Kaveh Ghaboosi, Jingyuan Zhang, Hongmei Deng,," A survey of cyber crimes", In Security and Communication Networks, pp 422-437, John Wiley & Sons New York (2012).

[2] Virginiah Sekgwathe, Mohammad Talib, "Cyber Crime Detection and Protection: Third World Still to Cope-Up", In Proceeding First International Conference, ICeND 2011, Dar-es-Salaam, Tanzania, pp 171-181, Springer Berlin Heidelberg (2011).

[3] Rebecca LeFebvre, "The human element in cyber security: a study on student motivation to act", in proceedings of the 2012 Information Security Curriculum Development Conference, InfoSecCD '12, pp 1-8, ACM New York (2012).

[4] Amber Stabek Paul Watters, Robert Layton, "The Seven Scam Types: Mapping the Terrain of Cybercrime", In Proceedings of the 2010 Second Cybercrime and Trustworthy Computing Workshop, CTC '10, pp 41-51, IEEE Computer Society Washington, DC, USA (2010).

[5] Aideen Keane, "Identity theft and privacy – consumer awareness in Ireland", In International Journal of Networking and Virtual Organizations, pp 620-633, Inderscience Publishers, Geneva, Switzerland (2009).

[6] Baca,M., Cosic, j., Cosic, Z., "Forensic analysis of social networks", In Proceedings of the ITI 2013 35th International Conference, pp 219-223, IEEE, Cavtat (2013)

[7] Alison Ada, "Cyberstalking and Internet pornography: Gender and the gaze", In Ethics and Information Technology, pp 133-14, Kluwer Academic Publishers Hingham, MA, US (2002)

[8] Vukelic, B., Skaron,K., "Cyber crime and violation of copyright", Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention ;pp 1127-1130, IEEE,Opatija (2013)

[9] Ms.Arpana, Dr.Meenal Chauhan, "Preventing cyber crime: A Study regarding Awareness of Cyber Crime in Tricity", International Journal of Enterprise Computing and Business Systems, pp1-10, (2012).

[10] John Akhilomen;" Data Mining Application for Cyber Credit-Card Fraud Detection System"; In Proceeding 13th Industrial Conference, ICDM 2013 New York, USA; pp 218-228; Springer Berlin Heidelberg (2013).

[11] PWC, "Fighting Economic Crime in the Financial Services Sector", Survey, 2012.

[12] Marsh and Chubb, Cyber Risk perceptions: An industry snapshot, Cyber Survey, June 2012.

[13] Verizon, 2013 Data Breach Investigations Report, 2013

[14] Ristenpart et al. in Proceedings of the 14th ACM conference on computer and communications security, pp 103–115, 2009; Pearson in CLOUD'09, pp 44–52, 2009; Vouk in J Comput Inf Technol 4:235–246, (2008).

[15] J. R. Vic Winkler, "Securing the Cloud: Cloud Computer Security Techniques and Tactics", Securing the Cloud: Cloud Computer Security Techniques and Tactics, Syngress Publishing (2011).

[16] Vlasti Broucek , Paul Turner, "Technical, legal and ethical dilemmas: distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—a forensic computing perspective", Journal of Computer Virology and Hacking Techniques, pp 27-33, Springer Paris (2013).

[17] Ruan et al. in Adv Digital Forensics VII: 35–46, 2011; Reilly et al. in Int J Multimedia Image Process 1:26–34, 2013

[18] Feily, M., Shahrestani, A. ; Ramadass, S.," A Survey of Botnet and Botnet Detection", Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on, pp-268-273, IEEE Athens, Glyfada (2009)

[19] Ali Alkaabi, George Mohay, Adrian McCullagh," Dealing with the Problem of Cybercrime", Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates,pp 1-18, Springer Berlin Heidelberg