iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: III Month of publication: March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67399

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Application of Fuzzy Hypergraph in Cyber Security

SaridhaS[1], Ranjani Devi A[2]
[1]AssociateProfessor, [2]PGStudent, PG and Research Department of Mathematics, Cauvery College for Women (Autonomous), Trichy-18

Abstract: The main goal of this paper isto apply hypergraphs in cyber security to identify the type of attack affecting a system based on specific attack causes. Here, system components are represented as edges, while attacks are modeled as vertices for better analysis.
Keywords: Hypergraph, fuzzy hypergraph, fuzzyα-cut hypergraph and cyber security.

I. INTRODUCTION

Hypergraphs were considered useful instruments for presenting the formation of partitions, covers, and clusters and analyzing the structure of a system. Kaufmann introduced the idea of fuzzy hypergraphs, an extension of the concept of hypergraphs in fuzzy theory. However, it turns out that fuzzy partitioning and other systems are not well presented by Kaufmann's definition of fuzzy hypergraphs [5]. The concept of fuzzy hyper graphs has been redefined to help with system analysis and fuzzy partitioning. A-Cut Hypergraph, Dual Fuzzy Hypergraph, Strong Classes, Edge Strength (Class) are some of the useful ideas developed. The proposed fuzzy hyper graph can help provide a visual description of the fuzzy cover or partition. Furthermore, the strength (class) of Edge allows you to choose a strong class of partitions, and by separating the strong class from other parts, you will need less overall data management. The proposed ideas include applications in terms of pattern recognition, circuit clustering, and system analysis.

Section II explains some basic definitions. Cybersecurity threats such as malware, ransomware, and identity have been introduced in Section III. In Section IV, the concept of fuzzy hypergraphs is used in cybersecurity, and the use of fuzzy hypergraphs is identified by systems affected by a particular attack. This can be extended in the domain of automatic theory [2, 3, 4, 5, 6] and in the labeled graphs [7, 8, 9].

II. PRELIMINARIES

In this section some basic notions which are needed for the succeeding sections are discussed.

A. *Definition 2.1*

A hypergraph C can be defined as a pair (A,B), where A is as set of points, and B is a set of hyper lines between the points. Each hyper line is a set of points $A \subseteq P(B)$.

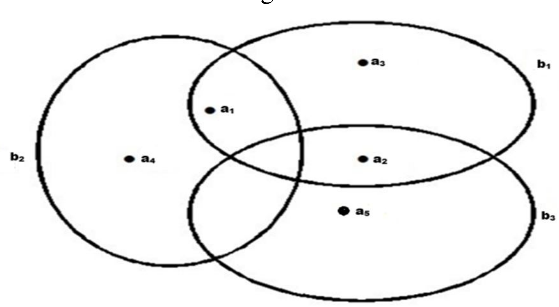
The hypergraph, which is defined as follows:

$C=(A,B)$ where, Ais the set of points, Bis the set of hyper lines.

Example 2.1: Consider a hypergraph $C=(A,B)$ such that $A=\{a_1,a_2,a_3,a_4,a_5\}$, $B=\{b_1,b_2,b_3\}$, where $b_1=\{a_1,a_2,a_3\}$, $b_2=\{a_1,a_5\}$ $b_3=\{a_2,a_4\}$.

The hypergraph, which represents the incident matrices, is displayed as follows:

Figure 2.1



Incidence matrix:

$$\begin{array}{c|ccc} C & b_1 & b_2 & b_3 \\ \hline a_1 & 1 & 1 & 0 \\ a_2 & 1 & 0 & 1 \\ a_3 & 1 & 0 & 0 \\ a_4 & 0 & 0 & 1 \\ a_5 & 0 & 1 & 0 \end{array}$$

B. Definition 2.1

In ordered pair $\hat{C} = (\hat{A}, \hat{B})$ such that is a fuzzy hypergraph

(1) $\hat{A} = \{a_1, a_2, a_3, \ldots\ldots, a_n\}$ a finite set of points, (2) $B = \{b_1, b_2, b_3, \ldots\ldots, b_m\}$

a family of fuzzy subset of $\hat{A}$ (3) $\hat{A}_v = \{(x_u, \mu_v(x_u) \setminus \mu_v(x_u) > 0\}, v = 1,2,3, \ldots\ldots, m,$

(4) $\hat{A}_v \neq \phi, v = 1,2,3\ldots\ldots, m,$ (5) $\cup_v \boldsymbol{sup}(\hat{\boldsymbol{A}}_v) = \boldsymbol{D}, \boldsymbol{v} = \mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots\ldots \boldsymbol{m}$

III. CYBER SECURITY FOR MALWARE, IMPERSONATION AND RANSONWARE:

In this section, various attack such as malware, impersonation, and ransomware, along with their impact on system, are presented.

1) Malware:Malwareisageneraltermthatdescribesanykindofmalicioussoftwarethatdamagestheoperationofyourcomputer,network,or device,andissomethingthatotherwiseexploits,misuses,ordamagesit.Malwareisoftencreatedtostealdata,disruptthesystem,andobtain unauthorizedaccesstosensitiveinformation.
2) Impersonation: An impersonation attack is a type of fraud where attackers pretend to be a trusted individual or entity to trick victims into transferring money, sharing sensitive data, or disclosing login credentials, which can then be used to compromise an organization's systems.
3) Ransomware:Ransomwareisamaliciousprogramthatblocksaccesstofilesorvictims'entiredevicesbyencryptingdataorblockingthesystem.Attackersoftenrequestcryptocurrencypaymentsinreturnforrepairingdecryptionkeysoraccesstoaffectedsystems.Ransomwarecanpenetrateavarietyofdevices,includingcomputers,smartphones,printers,andothernetwork-connectedsystems.Afterinstallation,itcanspreadoverthenetwork,whichcanleadtoawiderangeofdisruptionsforthecompanyandleadtolossofcriticalorsensitiveinformation.Thistypeofattackisparticularlyharmfultobusinesses,healthorganizationsandgovernmentsasitallowscriticalservicestobestoppedandconsiderablefinancialandreputationalcostscanbeconsidered.

IV. FUZZY HYPERGRAPH IN CYBER SECURITY

This section explores the generalization of fuzzy hypergraph, where systems impacted by different attacks are analyzed. Here, A represents the affected systems and is referred to as the set of lines (or hyper lines), while C denotes the attacks and is considered the set of points. This section deals with the fuzzy hyper graph in which causes for cyber security are taken. $\hat{A}$ is treated as attacks and is called the set hyper edges whereas the set C
is treated as causes for cyber attacks and is called the set of points.

A. Definition 4.1

The fuzzy hyper graph is defined as follows:

$\hat{G}_A = (\hat{C}, \hat{A})$ $\hat{C} = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9\}$, $\hat{A} = \{A_1, A_2, A_3\}$ a family of fuzzy subset of C where, $A_1 = \{C_1, C_2, C_3, C_4, C_5, C_6\}$ $A_2 = \{C_1, C_2, C_3, C_7, C_8\}$, $A_3 = \{C_1, C_2, C_9\}$

$$\hat{A}_k = \{(y_1, \mu_k(y_1) \setminus \mu_k(y_1)) > 0\}, k = 1,2,3,\ldots\ldots\ldots,n, \hat{A}_k \neq \phi, k = 1,2,3,\ldots\ldots\ldots,n$$

$$\bigcup_k \sup(\hat{A}_k) = c, k = 1,2,3,\ldots\ldots\ldots,n \qquad \text{--------------------(1)}$$

The lines, also known as hyper lines, $\hat{A}_k$ are fuzzy sets of points. $\mu_k(y_1)$ defines the extent of involvement(membership) of point. Crisp sets $\hat{C}, \hat{A}$ make up other sets. From (4.1), we have,

$$\bigcup_k \sup(\hat{A}_k) = c, k = 1,2,3,.........,n \quad \text{---(2)}$$

By substituting (1) with (2), we can expand the concept of fuzzy hyper graph. The related fuzzy incidence matrix $M_{\hat{A}}$ of fuzzy hyper graph is natural way to express it. The fuzzy matrix element $\alpha_{k,l}$ denotes the degree of participation or membership of y_1 to $\hat{A}_k$ ((i.e,)) $\mu_k(y_1)$ .The diagram with its incidence matrix or the description of hyper lines in the fuzzy hypergraph are utilize, as the hypergraph graphic does not suggest the membership degree of point.

Example:Let us consider a hyper graph $\hat{G}_A = (\hat{C}, \hat{A})$ such that $\hat{C} = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9\}$, $\hat{A} = \{A_1, A_2, A_3\}$,

Where, $\hat{A}_1 = \{(c_1, 0.1), (c_2, 0.2), (c_3, 0.3), (c_4, 0.5), (c_5, 0.6), (c_6, 0.7)\}$,

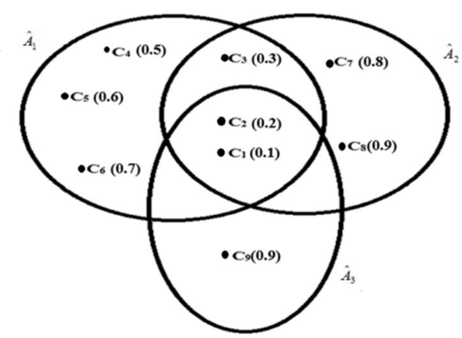
$\hat{A}_2 = \{(c_1, 0.1), (c_2, 0.2), (c_3, 0.3), (c_7, 0.8), (c_8, 0.9)\}$, $\hat{A}_3 = \{(c_1, 0.1), (c_2, 0.2), (c_9, 0.9)\}$

We are going to analysecyber attack scenarios involving phishing, social engineering, vulnerabilities, spyware, worms, viruses, MITM (man-in-the-middle), account takeover (ATO), and compromised credentials using a fuzzy hypergraph.

INCIDENCE MATRIX:

$\hat{G}_A$	$\hat{A}_1$	$\hat{A}_2$	$\hat{A}_3$
C_1	0.1	0.1	0.1
C_2	0.2	0.2	0.2
C_3	0.3	0.3	0
C_4	0.5	0	0
C_5	0.6	0	0
C_6	0.7	0	0
C_7	0	0.8	0
C_8	0	0.9	0
C_9	0	0	0.9

Figure 4.1:



FUZZY α –CUT HYPERGRAPH

The fuzzy α -cut hypergraph $\hat{G}_{A_\alpha}$ is obtained by cutting a fuzzy hypergraph $\hat{G}_A$ at the α level. $\hat{G}_A = (\hat{C}, \hat{A})$

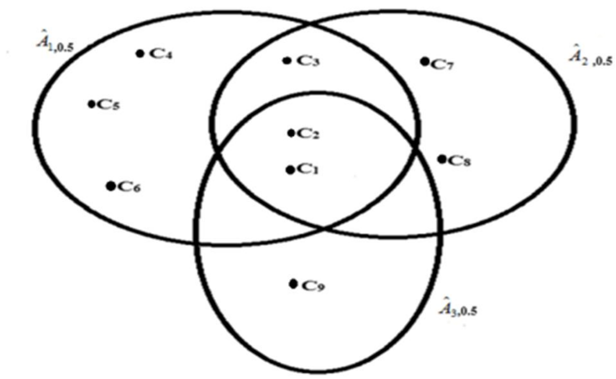
$\hat{C}_\alpha = \{\hat{C}_1, \hat{C}_2, \hat{C}_3, \hat{C}_4, \hat{C}_5, \hat{C}_6, \hat{C}_7, \hat{C}_8, \hat{C}_9\}$, $\hat{A} = \{\hat{A}_1, \hat{A}_2, \hat{A}_3\}$ $\hat{A}_\alpha = \{\hat{A}_{k,\alpha} \mid \hat{A}_{k,\alpha} \neq \phi, k = 1,2,3,.....,m+1\}$,

$\hat{A}_{k,\alpha} = \{x_l \mid \mu_k(x_l) \geq \alpha, k = 1,2,3,.....,m\}$

Now, the lines within the fuzzy α - cut hypergraph are distinct sets.

Example :In the above fuzzy α -cut hypergraph, consider the causes ofcyber security C_1 as phishing, C_2 as social engineering, C_3 as vulnerabilities, C_4 as spyware, C_5 as worms, C_6 as viruses, C_7 as man-in-the-middle (MITM) attacks, C_8 as account takeover (ATO), and C_9 as compromised credentials. The entities $\hat{A}_1, \hat{A}_2, \hat{A}_3$ now represent distinct cyber attack scenarios. The fuzzy hypergraph of the hypergraph at $\alpha = 0.5$ and incidence matrix $M_{\hat{G}_{0.5}}$ as follows:

Figure 4.2



Incidence matrix:

$\hat{G}_A$	$\hat{A}_{1,0.5}$	$\hat{A}_{2,0.5}$	$\hat{A}_{3,0.5}$
C_1	1	1	1
C_2	1	1	1
C_3	1	1	0
C_4	1	0	0
C_5	1	0	0
C_6	1	0	0
C_7	0	1	0
C_8	0	1	0
C_9	0	0	1

The element with larger than 0.5 membership to all lines is contained in the 0.5 - cut hypergraph.

By using the cut hypergraph , Attack 1 , $\hat{A}_{1,0.5}$ from malware, Attack 2 , $\hat{A}_{2,0.5}$ from impersonation, and Attack 3, $\hat{A}_{3,0.5}$ from ransomware. These attacks are analyzed in the context of their relationships using a fuzzy hypergraph to understand their impact and connections to various cyber security scenarios .

V. CONCLUSION

Fuzzy hypergraphs offer a structured way to analyze cybersecurity threats by mapping attacks and their causes. This method categorizes threats like malware, impersonation, and ransomware using fuzzy incidence matrices and α-cut hypergraphs. It helps identify attack patterns and assess their impact on systems. Additionally, it can be extended to automata theory and labeled graphs for broader cybersecurity applications.

REFERENCES

[1] Kaufmann.A,IntroductionCilaThioriedesSous-EnsembleFlous,vol.1,Masson:Paris,1977.

[2] Saridha S,& Vidhya R.(2024). An Application of fuzzy Graph Structure in Human Trafficking. Research Updates in Mathematics and Computer Science Vol. 5, 70-80. https:// doi.org/10.9734/bpi/rumcs/v5/8537

[3] Saridha.S,Jothika.T,"AnIntroduction to Plus Weighted Dendrolanguage and its properties",Volume15,IssueI,Aryabhattajournalofmathematics&Informatics (AJMI), Jan-June 2023, Page No: 93-100, ISSN: 2394-9309.

[4] Saridha. S,Jothika.T,"Construction of DerivationTrees of PlusWeighted ContextFreeGrammars",Volume11,IssueIII,International Journal for Research in Applied Science and Engineering Technology (IJRASET), March 2023, Page No: 1821-1827, ISSN: 2321-9653.

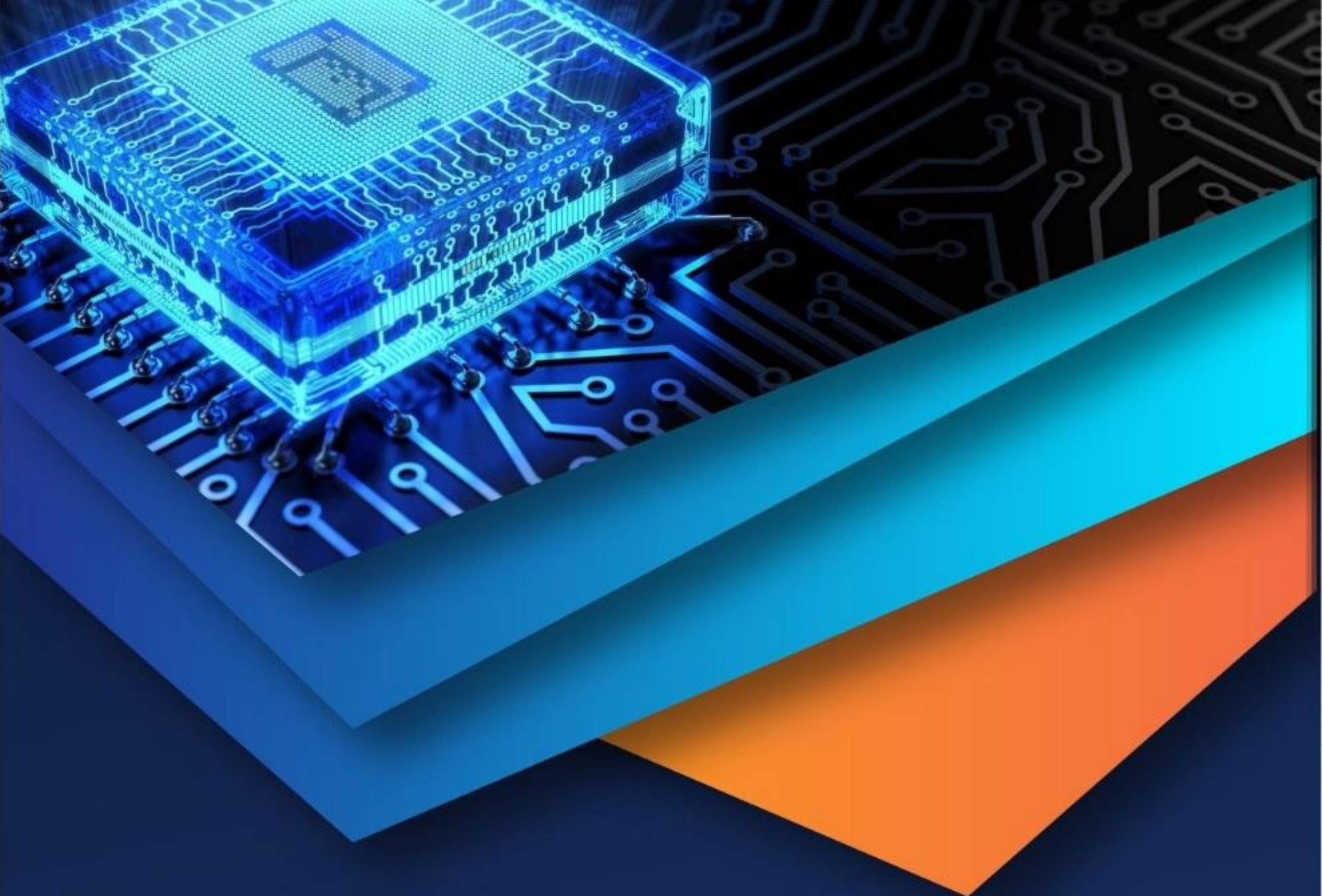
[5] Saridha.S.and Haridha Banu.S,"A New Direction Towards Plus Weighted Grammar",Volume11,IssueII,InternationalJournalforResearchin Applied Science and Engineering Technology (IJRASET), February 2023, Page No: 845-850, ISSN: 2321-9653.

[6] Saridha. S.,HaridhaBanu. S "An innovative Ideas on Plus Weighted Linear Grammar",Volume 15, Issue 2, Aryabhatta journal of mathematics & Informatics(AJMI), Jan-June 2023, Page No: 173-178, ISSN: 2394-9309.

[7] Shalini,P.,Gowri,R.,PaulDhayabaran,D.,An Absolute Differences of Cubic and Square Difference Labeling For Some Families Of Graphs,The International journal of analytical and experimental modal analysis, Volume XI, Issue 10, October 2019, Page no: 538-54

[8] Shalini, P., PaulDhayabaran, D.,A Study on Root Mean Square Labelings in Graphs, International Journal of Engineering Science and Innovative Technology, May 2015, Volume-4, Issue-3, pages 305-309.

[9] Shalini,P.,Paul Dhayabaran,D.,An Absolute Differences of Cubic and Square Difference Labeling, Internationa lJournal of Advanced Scientific and Technical Research, May-June 2015, Issue-5, Volume-3, pages 1-8.



10.22214/IJRASET

INDEX COPERNICUS 45.98

ISRA JIF IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY