GLOBAL
CONFERENCE ALLIANCE INC.

www.globalconference.ca

Proudly Canadian, Truly Global

***<u>Format: Electronic Book</u>***

# 5th Global Conference on Cyber Security and Cloud Engineering 2023

## Conference Proceeding

ISBN: 978-1-7380126-2-6

# Table of Contents

## Content Details:

| **Wade Ghribi (Author)**<br>*King Khalid University* | **Locating hot spot states of cyber crime against children and initiating cyber security measures** |
|---|---|

## Abstract

In digitally connected world, children are the maximum dynamic users of internet and web-based services. Cyber crime is one of the major drawbacks of web. Children are young people and vulnerable to abuse and exploitation of cyber-predators and perpetrators. Cyber criminals involve in online child abuse, child exploitation, possession of child pornography, cyber bullying, exposure to harmful web content, and many more. Cyber crime cases against children data released by the National Crime Records Bureau (NCRB) of India are utilized to analyze and find the hot spot states using the k-means cluster algorithm. The analysis and findings of the study can help government to initiate additional cyber security measures and develop effective strategic plans to control cyber crimes against children.

## Introduction

The daily usage of internet & web increases tremendously around the world in current decade.The www or World Wide Web has significantly made advancement, but unpredictably, one of its assistances is that it makes users close to the world, making us to live in small place. One of the major drawbacks of web is cyber crime, an illegal action that utilizes a computer as a tool or a target. Cyber crimes are escalating gradually, and several users have fallen victims to criminal frauds, hacking, malicious software etc. Some people misuse web, internet and computers to commit frauds & crimes like hacking, email bombing, cyber pornography and cyber stalking.

Cyber criminals also involve in online child abuse, child exploitation, possession of child pornography, cyber bullying, exposure to harmful web content, and many more. Children are habituated to social media platforms such as WhatsApp, Facebook, Instagram, and Snapchat, are easy targets for perpetrators of cybercrime. For example, the criminal may approach a young child online and make online friendship built on the identical likes, interests, and actions. As a result of online friendship, photos and gifts might be exchanged. The criminal attempts to gain the trust of child to acquire what they need from the youngster and exploits children. It is been found that teenagers and young kids are the prime and easy objects for criminal activity as they are innocent, inexperienced, and eager for care and affection.

Due to the COVID-19 pandemic, lockdowns and restrictions, the cyber crimes cases has raised sharply in India and world. According to UNICEF, “online platforms were the most used means by the governments to deliver education while schools remain closed, with 83% of countries [globally] using this method” This result in sharp increase of cyber crime against children. UNICEF also reports “More than a third of young people in 30 countries report being cyber bullied, with 1 in 5 skipping school because of it and Some 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online” (Unicef, Protecting children online, 2023). The reported cyber crime cases against children includes Cyber Blackmailing/ Threatening/ Harassment, Fake Profile, Cyber Pornography/ Hosting or Publishing Obscene Sexual Materials depicting children, Cyber Stalking/ Bullying, Internet Crimes through Online Games etc. Cyber crimes against children incidents have increased 15 times in the last five years (88 in 2017 to 1376 in 2021) and spiked 261% amid the first pandemic-induced lockdown, according to the latest numbers released by the NCRB, India (National Crime Records Bureau NCRB India, 2018-21). Fig 1 shows the total cyber crime cases in India between 2012-21 and Fig 2 presents a pie chart showing the total cyber crime cases against children in India between 2017-21.

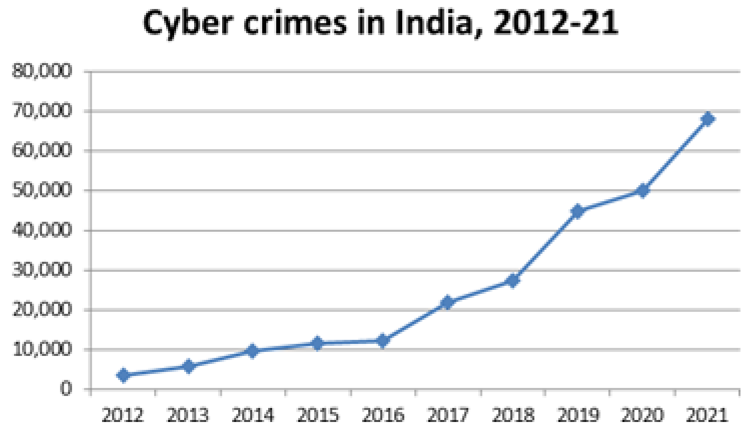


**Fig 1: Cyber crimes cases in India 2012-21**

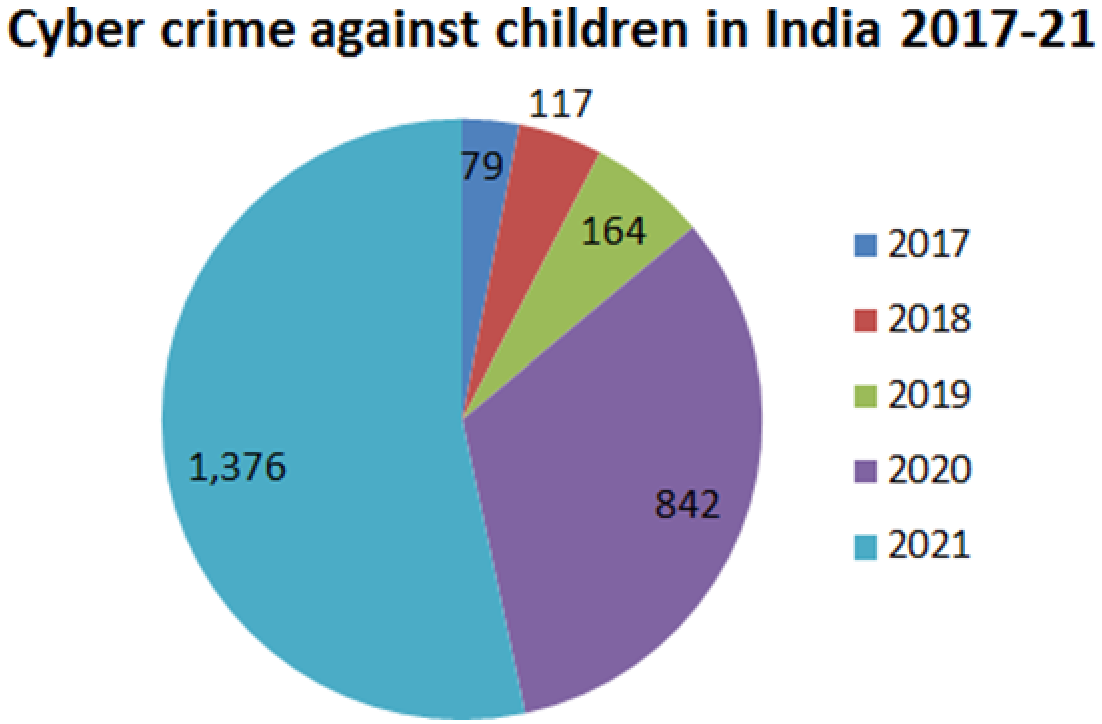


**Fig 2: Cyber crimes cases against children in India 2017-21**

To help children grow up in a safe and nurturing environment, much needs to be done to locate hot spot states of cyber crime against children and initiate additional cyber security measures. The objective of this paper is to evaluate data of cases of cyber crime against children in India using a k- means cluster algorithm and locate hot spot states of crime against children across all the states.

## Background

"Cybercrime refers to any crime performed using a computer or an electronic device, mainly through the Internet" (Deora, R.S. and Chudasama, 2021). As a result of the COVID-19 pandemic, the world has moved to digital channels, resulting in a surge in cybercrime. India experienced an 86 percent rise in cyber-attacks from March to April, 2020. Rani Supriya et al (2022) discuss different types of cybercrime that people are facing and the unique challenges & cyber crime problems. Showkat Ahmad Dar and Naseer Ahmad Lone (2020) discuss different types of cybercrime and major cybercrime cases India. Apoorva Bhangla and Jahanvi Tuli (2021) undertake a study on cyber crime against women and its legal frame work in India.

Children tend to surf the web to access educational information and content for entertainment, to develop their digital skills to acquire new opportunities, or to maintain their online/digital identities and social relationships. However, Children out of their own curiosity, under peer pressure or during their search accidentally might come across content which is not suitable for viewing at their age. Children viewing inappropriate content like sexual or pornographic material, incidences of abuse and violence, content propagating radical/extremist ideologies etc, may leave an impact on their young impressionable minds. Children are also vulnerable to „Online Scams" which are often targeted at adults for coaxing money out. Several scams and false schemes such as encouraging claims to lottery winnings, requesting payments to receive awards, gifts and winnings, websites offering products at cheap prices etc. lure children into accessing these schemes. In most cases, children either end up sharing parents" or guardians" financial information or lead to entrapping their families into bigger scams and ponzi schemes. Thus children and young people are vulnerable to abuse and exploitation at the hands of cyber-predators and perpetrators. The 2020 Child Safety Online Index, a survey of 30 countries conducted during the covid-19 pandemic, ranks India second In terms of the •extent of cyber-risks" faced by children (Sarma.A, 2022).This seems to indicate that children in India face a high volume of risks online.

Cyber bullying and phishing are common cybercrime, is common in our online lives, and children are no exception. Parents urge their children to stay away from online games and internet, but in reality this is not happening. P.N.V Kumar (2016) review the growth of cyber crimes in India and measures taken by the government of India to combat the cyber crimes. P.Datta et al (2020) makes an intensive review on cyber crime in India and finds an increase in cyber fraud cases where victims are mostly children and women in the age group of 20 - 29 years. Farzana Quayyum et al (2021) review cyber security risks for children and summarize the findings on cyber security awareness research for children. Victor Chang et al (2023) discuss cyber security for teenage children and focuses on social media"s impact using a theoretical approach. D.Andrews et al (2020) examine online social media responses and awareness posts on children online safety.

A number of modern technologies and advanced tools are in use to analyze, detect and prevent crimes. Machine learning algorithms & tools are extensively used in criminology field. A systematic document review method for crime prediction has been used by Jenga.K et al. (2023) to collate and synthesize knowledge of machine learning based crime prediction to help agencies of law enforcement and researchers towards control and prevent future crimes. S.Prabakaran and Shilpa Mitra (2018) describe several supervised and unsupervised machine learning algorithmic techniques that can be applied in the field of crime. W.A.Al-Khater et al (2020) explores different types of cyber crimes and discusses their threats against privacy & security, strategies used by cyber criminals in committing cyber crimes, reviews the existing techniques of cybercrime detection & prevention and provides recommendations for the development of a cybercrime detection model. E.C.Ateş et al (2018) examine the sample of child victims of cyber crime in Turkey to find hot spots where the victims live mostly by machine learning method and the generic profile of the victims were discovered. A.AlShabibi and Al-Suqri (2021) investigates the impact of cyber security awareness among children in terms of protecting them in cyber space by reviewing the academic literature. In this paper, we apply a machine learning technique namely k-means cluster algorithm on Indian cyber crime against children dataset to locate hot spot states of crime against children across all the states.

## Methodology

In this paper, we use k-means cluster method of machine learning in WEKA platform to make analyses on the cyber crimes against children dataset to locate hot spot states in India. Fig. 3 shows the overall block diagram for the locating states of cyber crime against children using k-means method in

WEKA.

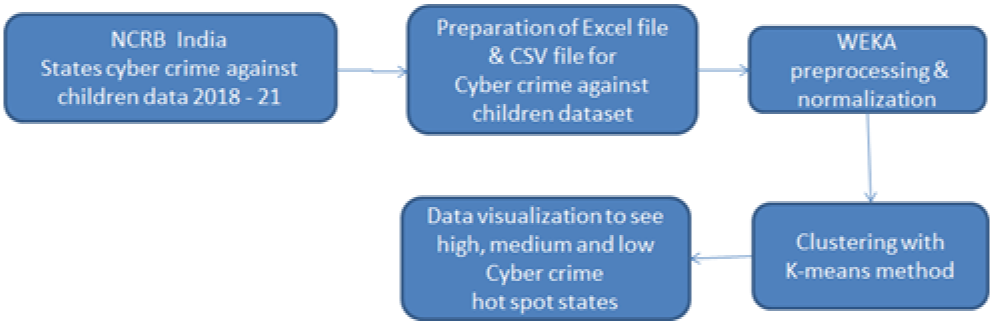


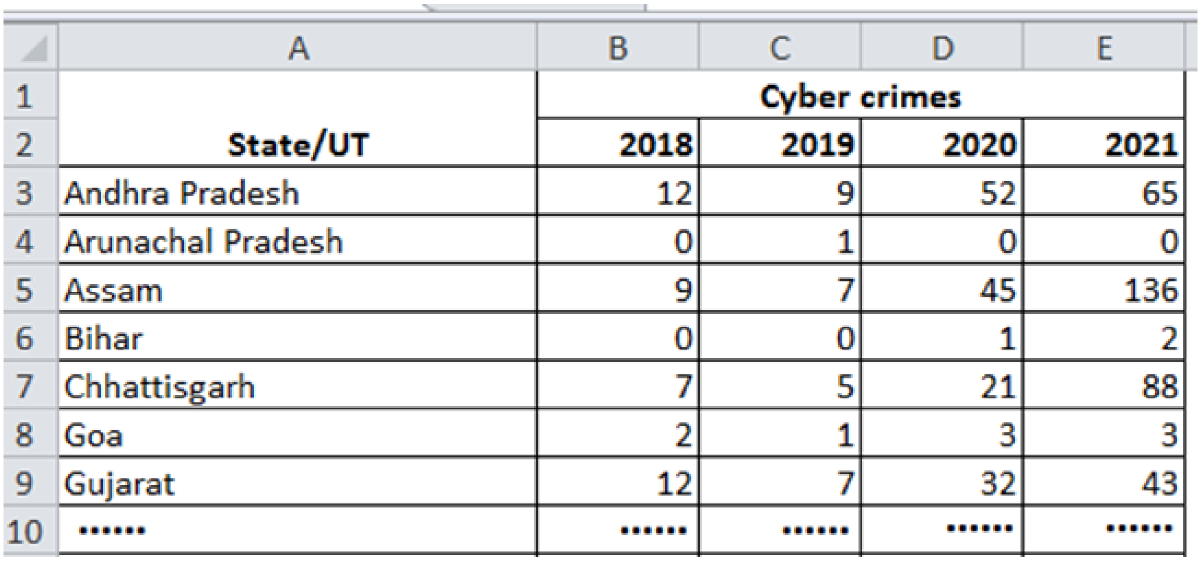
**Fig 3: Block diagram for locating states of cyber crime against children with k-means approach**

The k-means cluster algorithm is used to make groups which do not have any explicitly labeled feature in dataset (L. S. Thota et al, 2015). The k-means cluster algorithm build k groups of data points based on similarity (S. B. Changalasetty et al, 2015). Each data point is assigned to a cluster whose centroid is closest distance to it. The centroid of the groups are updated depending on all data points mean value in the group. The process is repeated until no shifting of data points or set maximum iterations (k-means clustering Wikipedia, 2023). The algorithm aims to minimize the sum of squared distances between each data point and its assigned centroid (S. B. Changalasetty et al, 2015).

WEKA refers Waikato Environment for Knowledge Analysis is developed in Java platform and freely available software. WEKA contains GUI for simple and easy use platform for data mining. WEKA has collection of visualization tools and data mining & machine learning methods & algorithms for data analysis & predictive modeling (Weka machine learning, 2023). In WEKA platform users can perform data preprocessing, classification, clustering, association, visualization, etc. WEKA is a no-code tool, i.e any person in any field can apply machine learning methods to build models without writing programming code (L. S. Thota et al, 2020).

## Experiments, Results and Discussions

Data on cyber crimes cases against children in India from 2018-21 was sourced from the NCRB India (National Crime Records Bureau NCRB India, 2018-21). An Excel file was created to compile the state-wise data on total cyber crimes cases against children in India for each year from 2018-21 as shown in Fig 4.



| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | | Cyber crimes | | | |
| 2 | State/UT | 2018 | 2019 | 2020 | 2021 |
| 3 | Andhra Pradesh | 12 | 9 | 52 | 65 |
| 4 | Arunachal Pradesh | 0 | 1 | 0 | 0 |
| 5 | Assam | 9 | 7 | 45 | 136 |
| 6 | Bihar | 0 | 0 | 1 | 2 |
| 7 | Chhattisgarh | 7 | 5 | 21 | 88 |
| 8 | Goa | 2 | 1 | 3 | 3 |
| 9 | Gujarat | 12 | 7 | 32 | 43 |
| 10 | •••••• | •••••• | •••••• | •••••• | •••••• |

**Fig 4: Excel file showing data of cyber crime cases against children in India, 2018-21**

The resulting Excel file was saved as CSV file, which was then read in the WEKA platform for further processing, analysis, and visualization. After pre-processing, the cyber crime dataset consisted of 120 data points and was used for further analysis. A scatter plot of cyber crime cases against children is shown in Fig. 5.

Clustering of data is done by selecting cluster option in main menu of WEKA, choose simple k-means cluster type algorithm. Select the options for k-means process and press start button. After the k-means clustering is completed, the resulting clusters can be analyzed to determine which states have consistently high, medium or low cyber crime cases. The WEKA output file with generated clusters is shown in Fig 6 showing cluster details & number of states assigned to each cluster. Fig 7 shows WEKA output file with all states assign to the clusters. Fig 8 presents the WEKA cluster visualization with all Indian states grouped into clusters.

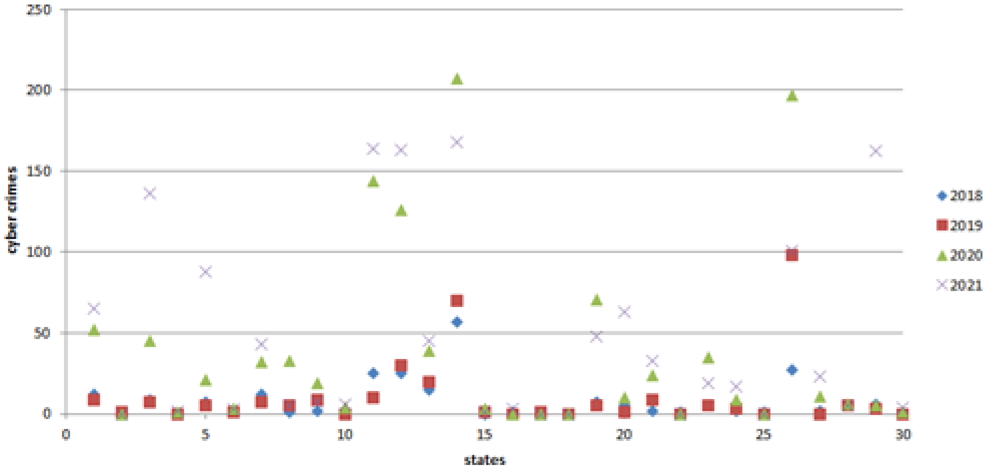
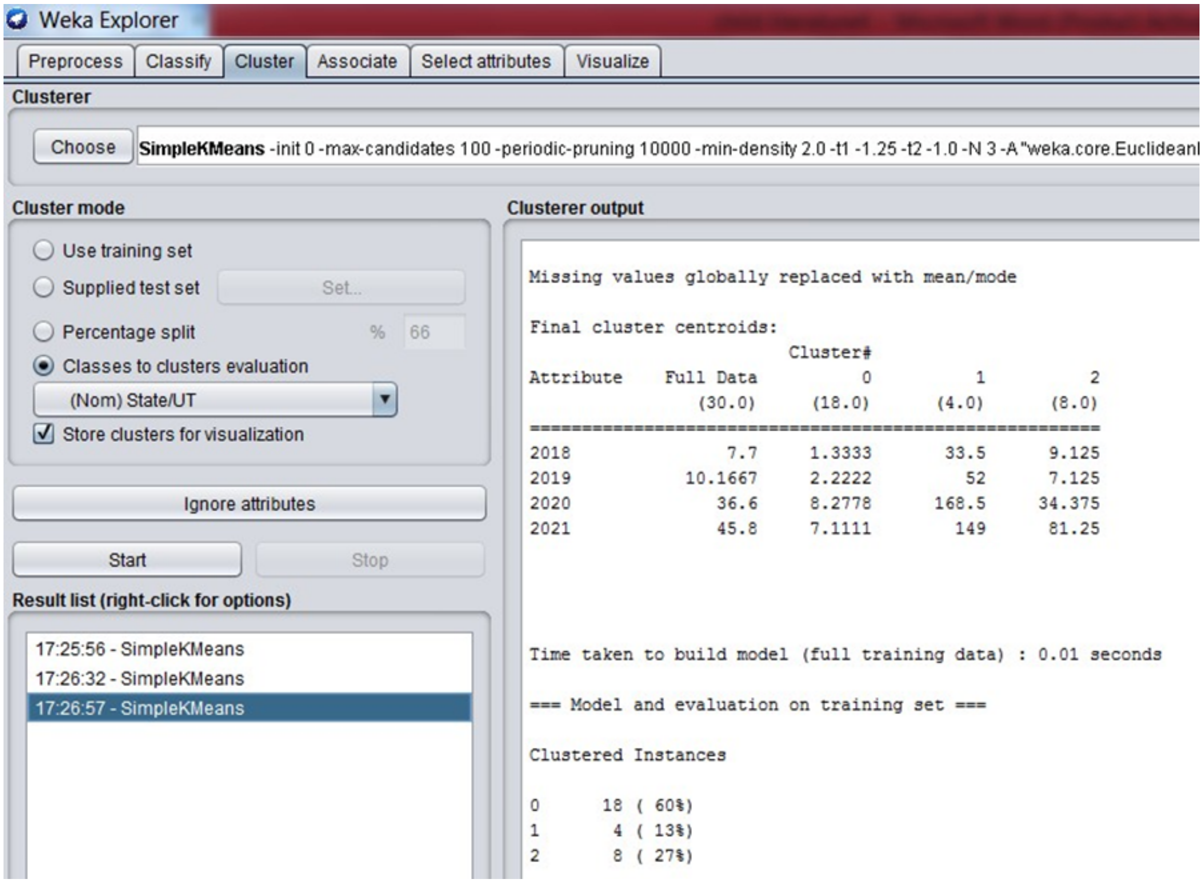


**Fig 5: Scatter plot of data points of cyber crime against children in India, 2018-21**



Clusterer

**SimpleKMeans** -init 0 -max-candidates 100 -periodic-pruning 10000 -min-density 2.0 -t1 -1.25 -t2 -1.0 -N 3 -A "weka.core.Euclidean

Cluster mode

○ Use training set
○ Supplied test set
○ Percentage split % 66
● Classes to clusters evaluation
(Nom) State/UT
☑ Store clusters for visualization

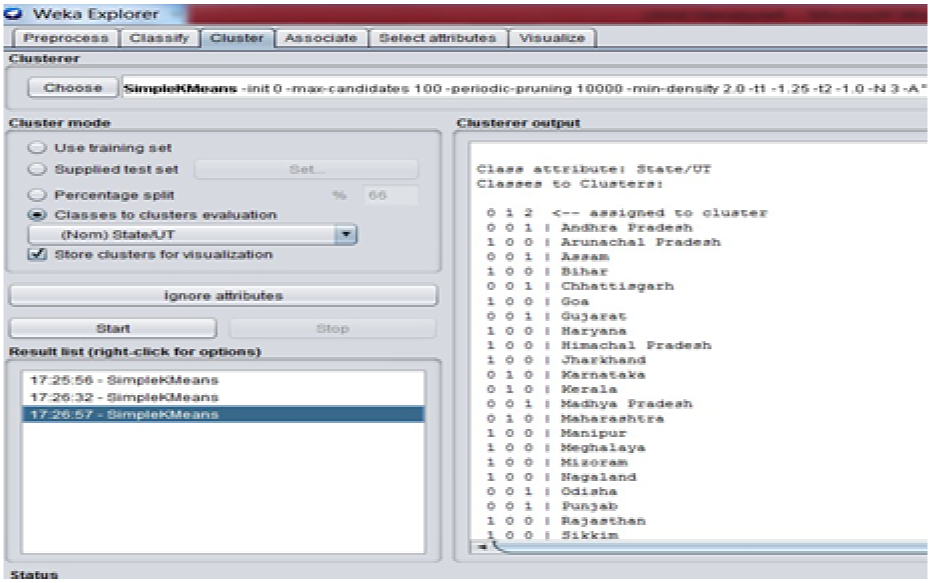
Result list (right-click for options)

17:25:56 - SimpleKMeans
17:26:32 - SimpleKMeans
17:26:57 - SimpleKMeans

Clusterer output

```
Missing values globally replaced with mean/mode

Final cluster centroids:
                         Cluster#
Attribute    Full Data          0          1          2
                (30.0)     (18.0)      (4.0)      (8.0)
========================================================
2018               7.7     1.3333       33.5      9.125
2019           10.1667     2.2222         52      7.125
2020              36.6     8.2778      168.5     34.375
2021              45.8     7.1111        149      81.25




Time taken to build model (full training data) : 0.01 seconds

=== Model and evaluation on training set ===

Clustered Instances

0      18 ( 60%)
1       4 ( 13%)
2       8 ( 27%)
```

**Fig 6: WEKA output file showing cluster details and total assigned states with k-means method**



Clusterer

SimpleKMeans -init 0 -max-candidates 100 -periodic-pruning 10000 -min-density 2.0 -t1 -1.25 -t2 -1.0 -N 3 -A "

Cluster mode

○ Use training set
○ Supplied test set
○ Percentage split % 66
● Classes to clusters evaluation
(Nom) State/UT
☑ Store clusters for visualization

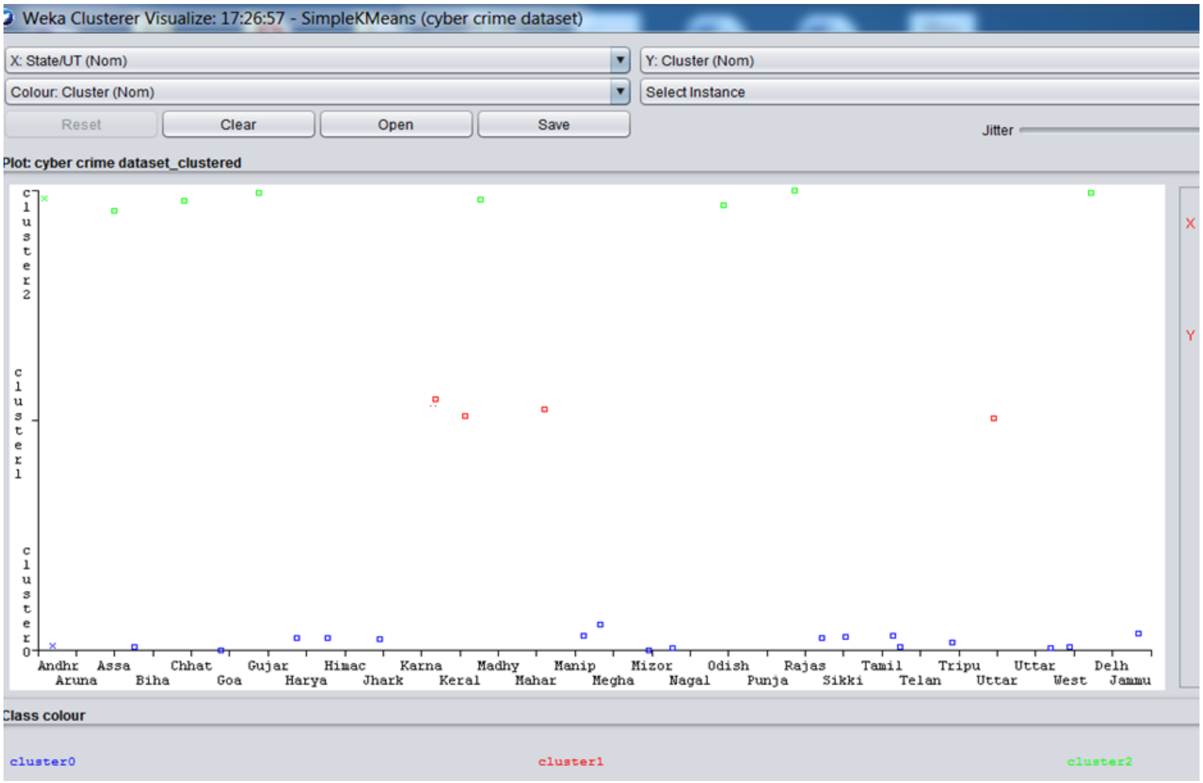
Result list (right-click for options)

17:25:56 - SimpleKMeans
17:26:32 - SimpleKMeans
17:26:57 - SimpleKMeans

Clusterer output

```
Class attribute: State/UT
Classes to Clusters:

 0 1 2  <-- assigned to cluster
 0 0 1 | Andhra Pradesh
 1 0 0 | Arunachal Pradesh
 0 0 1 | Assam
 1 0 0 | Bihar
 0 0 1 | Chhattisgarh
 1 0 0 | Goa
 0 0 1 | Gujarat
 1 0 0 | Haryana
 1 0 0 | Himachal Pradesh
 1 0 0 | Jharkhand
 0 1 0 | Karnataka
 0 1 0 | Kerala
 0 0 1 | Madhya Pradesh
 0 1 0 | Maharashtra
 1 0 0 | Manipur
 1 0 0 | Meghalaya
 1 0 0 | Mizoram
 1 0 0 | Nagaland
 0 0 1 | Odisha
 0 0 1 | Punjab
 1 0 0 | Rajasthan
 1 0 0 | Sikkim
```

**Fig 7: WEKA output file with generated clusters of Indian states with k-means method**



X: State/UT (Nom)

Y: Cluster (Nom)

Colour: Cluster (Nom)

Select Instance

Plot: cyber crime dataset_clustered

Class colour

cluster0 cluster1 cluster2

**Fig 8: WEKA cluster visualization with all clusters Indian states with k-means method**

The k-means method builds three crime clusters as low, medium and high cyber crime states. The cluster_0 result show 18 states having low cyber crime states against children. The cluster_2 results show states as having medium cyber crime states against children. The cluster_1 result shows 4 states (Karnataka, Kerla, Maharastra and Uttar pradesh states) as being high cyber crime states against children. The results show the cluster_1 the cyber crime against children is high when compared with all other Indian states which emphases the official to take extra care and preventive steps to control the cyber crime cases against children.

With these results, specific interventions can be created to address the problem of cyber crimes against children in each state. States in the low cyber crime cluster, on the other hand, may profit from initiatives focused on sustaining their low cyber crime cases. In contrast, states in the high cyber crime cluster may benefit from greater funding for law enforcement and victim support services. Policymakers and law enforcement agencies can use this information to develop effective interventions to prevent and respond to cyber crimes against children in India.

## Conclusion

Today‟s high tech digital surroundings, maintaining sufficient cyber security measures are essential and the paramount way to protect the children. Not only cyber crimes are threats harming the children, but also businesses & government authorities. The government is devoted to laws and policies to make sure all users every time have to an open, trusted, and accountable access to internet. More digital awareness programs in electronic media are required to reach all social media users for preventing or avoiding cyber-crime in India. The users should know self protection mechanism to mitigate cyber security issues before problems occur.

Although the administrative authorities has taken some cyber security initiatives, further more aggressive cyber security measures are required to be taken in the identified hot spot states to protect the children against dangerous cyber crime challenge. Comprehensive cyber security awareness programs in the educational curriculum for children can significantly reduce the spread. Initiating additional cyber security measures and awareness programs by the authorities will assist to maintain a cyber-secure environment and minimize the risks associated with cyber crimes.

## References

A. AlShabibi and M. Al-Suqri (2021). Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. IEEE 22nd International Arab Conference on Information Technology (ACIT) Muscat, Oman. pp. 1-6.

Apoorva Bhangla and Jahanvi Tuli (2021). A study on cyber crime and its legal frame work in India. International journal of law management and humanities. volume 4, issue 2, page 493-504.

D. Andrews, S. Alathur, N. Chetty and V. Kumar (2020). Child Online Safety in Indian Context. 5th International Conference on Computing, Communication and Security (ICCCS) Patna, India. pp.

1-4.

Deora R.S. and Chudasama D.M (2021). Brief study of cybercrimes on an internet. Journal of

Communication Engineering & Systems. 77(1), pp.1-6.

E. C. Ateş, E. Bostanci and M. S. Güzel (2018). Cybercrimes against children in Turkey. IEEE 6th International Symposium on Digital Forensic and Security (ISDFS) Antalya, Turkey. pp. 1-6.

Farzana Quayyum, Daniela S. Cruze, Letizia Jaccheri (2021). Cybersecurity awareness for children: A systematic literature review. Elsevier International Journal of Child-Computer Interaction.

Volume 30.

Jenga, K., Catal, C. & Kar, G (2023). Machine learning in crime prediction. J Ambient Intell Human Comput. Springer.

k-means clustering, Wikipedia (2023). https://en.wikipedia.org/wiki/K-means_clustering

L. S. Thota, A. S. Badawy, S. B. Changalasetty and W. Ghribi (2015). Classify vehicles: Classification or clusterization? IEEE International Conference on Circuits, Power and Computing Technologies

(ICCPCT), Nagercoil, India. pp. 1-7.

L. S. Thota et al, (2020). Rule-based Mining of Juvenile Delinquency. IEEE International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India. pp. 1-4.

National Crime Records Bureau (2018-21). (NCRB), Ministry of home affairs India. Crime in India.

https://ncrb.gov.in/

P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal (2020). A Technical Review Report on Cyber Crimes in India. International Conference on Emerging Smart Computing and Informatics (ESCI) Pune, India. pp. 269-275.

P. N. V. Kumar (2016). Growing cyber crimes in India: A survey. IEEE International Conference on Data Mining and Advanced Computing (SAPIENCE) Ernakulam, India. pp. 246-251.

Rani Supriya, et al, (2022). Cyber crimes in India: a critical analysis. International Journal of Mechanical Engineering. Vol. 7 No. 6.

Sarma, A (2022). A pandemic of abuse: How India is protecting its children online. Observer Research Foundation.

S. B. Changalasetty, A. S. Badawy, L. S. Thota and W. Ghribi (2015). Classification of moving vehicles using k-means clustering. IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India. pp. 1-6.

S. B. Changalasetty, A. S. Badawy, L. S. Thota and W. Ghribi (2015). Moving vehicles classification in WEKA. IEEE International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India. pp. 1-6.

Showkat Ahmad Dar and Naseer Ahmad Lone (2020). Cyber crime in India. Sambodhi, Vol-43 No.04

(VIII)

S Prabakaran and Shilpa Mitra (2018). Survey of Analysis of Crime Detection Techniques Using and Machine Learning. National Conference on Mathematical Techniques and its Applications, IOP Conf. Series. Journal of Physics: Conf. Series 1000.

Unicef (2023). Protecting children online.
https://www.unicef.org/protection/violence-against-children-online

Victor Chang, Lewis Golightly, Qianwen Ariel Xu, Thanaporn Boonmee and Ben S. Liu (2023).

Cybersecurity for children: an investigation into the application of social media. Taylor & Francis Enterprise information systems.

W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, vol. 8, pp.

Weka machine learning (2023) https://www.cs.waikato.ac.nz/ml/weka/