

Exploratory Examination of Cybersecurity-Based Parental Control Systems and Techniques

Prashant Shukla¹, R. Praneeth², Ms. Santhiya P³, Rajasekar P⁴

^{1,2}U.G Student, Department of CSE, Sathyabama Institute of Science and Technology, Chennai

^{3,4} Assistant Professor, School of Computing, Sathyabama Institute of Science and Technology, Chennai

prashantshukla7205@gmail.com¹, rokkampraneeth@gmail.com²,
santhiya.cse@sathyabama.ac.in³, rajasekar.cse@sathyabama.ac.in⁴

Abstract-The application enhances child safety and parental oversight by allowing parents to register and monitor their children's location through geofencing with boundary crossing alerts. It includes access to children's messages and call logs for communication supervision and tracks screen time to monitor usage. In emergencies, children can send voice messages to nearby parents, which are then forwarded to the administrator for action and contacting emergency services if needed. The app's signup and login are secured with AES encryption and decryption, offering a complete safety network that reassures parents and provides a reliable method for children to seek help when feeling unsafe. The study also emphasizes the vitality of studies in the area of online surveillance by parents, indicating a need for continuous improvement and adaptation to emerging challenges. The application aligns with this perspective by incorporating various features that contribute to a more effective and efficient system for Online Parental Guidance.

Keywords - Online Parental Guidance, Parental Monitoring, Child Safety Online, Internet Filtering, Content Restrictions, Online Safety Tools, Screen Time Management

1. OVERVIEW

The widespread use of internet technology enables the easy publication of diverse topics and fosters open communication between users. While the internet offers substantial benefits for children, the presence of objectionable content poses significant risks, with over half of child internet users inadvertently encountering harmful material. Such objectionable content can inflict psychological or mental harm on children, including harassment, guns, illicit substances, hate, betting, and brutality.

Aware of these dangers, business and academics stress the importance of using efficient cyberparental control devices and procedures to parent, supervise, and manage kids' online activity. Online supervision, as defined by earlier research, is the process by which parents regulate their kids' use of online resources, including online communities, networking sites, and the internet as a whole.

elements of cyber supervision that are covered in the research include the responsibilities of families, risks associated with cyber networks, scientific elements, and psychological and legal ramifications. Notwithstanding the importance of study in this field, little is known about the methodologies, strategies, and databases involved in cyberparental control. Filling such these gaps would improve our knowledge of previously underappreciated strategies, tactics, and sets of data.

To achieve this, the study aims to conduct a preliminary investigation into online parental guidance rolls around, strategies, and datasets pertaining to online parenting. It seeks to identify the optimal initiatives, their advantages and disadvantages as well as the sets of data that are now being utilized, providing information for upcoming research in the subject. Given the considerable number of children online and their vulnerability to various risks, studying this field is imperative.

This approach compares information sets, strategies, and tactics for cyberparental control using terms like "removing," "the online world," and "offensive." In order to concentrate on the most articles that have recently appeared in the Wos and Index libraries while eliminating irrelevant paperwork, binary operators such as the logical

GATE are utilized to refine the search outcomes inside the research's purview.

The research project is divided into 7 pieces, with a summary at the start of each. The first section goes over the background of cyberparental control. In turn, techniques for eliminating objectionable information from webpages are covered in Chapters 3 and 4. The field of cyberparental control's existing datasets are examined in Chapter 5. The paper's conclusion, found in Chapter 7, offers guidelines for further research in the area. Chapter 6 examines and recommends an efficient cyberparental supervision system.

2. CONTEXT

The terms "cyber parental control" and "monitoring and mediation by parents" are defined differently by the authors in [1]. The primary goal of controlling kids is to enable parents to track and regulate the actions of their kids both within and outside the home by establishing ground rules [6,7]. The definition of "a set of correlated parenting habits requiring constant surveillance and apprised of the child's motions, spots, and adjustments" is expanded to include surveillance by parents [6]. "Guardianship a mediator" has been used in books since the birth of media, involving interactions between parents or guardians and children concerning media. Parental mediation involves three main levels of restrictions: co-using, evaluative, and restrictive, with the latter being the most stringent [3]. In summary, online parental guidance encompasses a set of interrelated parental behaviours that enable parents or guardians to supervise and manage their kids' internet activity; according to the UN, the term "children" are those under the age of 18 years old, until they achieve majority earlier.

Information extraction techniques are applied to internet materials by online resource producers for classification, categorization, filtering, and recommendation purposes. Search engines, surveillance software, analyzing software, and educational browsers are the four categories of web miners [8]. Children's exposure to undesirable, practical, amusing, and social media websites is limited by educational internet browsers and customized browsers, which limit their access to just instructional webpages. Researchers has utilized this technique to create queries based on

filtering and classification techniques, frequently leveraging Google's specialized query to identify problematic web information . Lookup engines are computer programs intended for regular browsing of the internet. Technology that detects and keeps track of, documents, and examines what kids do online without filtering objectionable content, exposing children to the risks of objectionable material. Some monitoring software includes additional features such as A security program, phone filtering, tracking of movements, and spyware scanning features provide another level of complexity to stop unwanted information. Nevertheless, a major disadvantage of these programs and designs is that kids can use bypass tools to go around them. Filtering frameworks, on the other hand, analyze, classify, and manage visible information for minors by including a protective level to remove undesirable content. In the realm of online regulation by parents, it's the tactic that is most frequently employed. The strategies and tactics used by these filtering frameworks are covered in detail in the chapter that follows.

3. TECHNIQUES FOR BLOCKING OFFENSIVE WEBSITES

Earlier research in the realm computerized screening architectures of cyber guardianship have been used to deal with certain issues in this field. The aforementioned structures combine different methodologies such as website address, keyword, and content-focused methods with machine learning and material screening algorithms. Numerous research have used various techniques, each of which has advantages and disadvantages of that particular method. The first tableau provides a comparative analysis of these methods, highlighting their respective strengths and limitations.

3.1 WEB CONTENT SCREENING

This approach involves the filtration of websites by comparing the supplied Link along with a set of predetermined references. References come in a pair of forms: whitelisting & blacklisted. Webpages that are prohibited are listed on the prohibited list, and webpages that are permitted are listed on the whitelist. The list of sources has a significant impact on this method's efficacy despite its simplicity. With the hundreds of thousands of new

webpages created every day [9], the problem of potentially large failure rates arising from the incompleteness of these references is presented. Numerous settings have seen the application of Location-based screening, such as phishing screening, removal of spam, and sexuality screening [10].

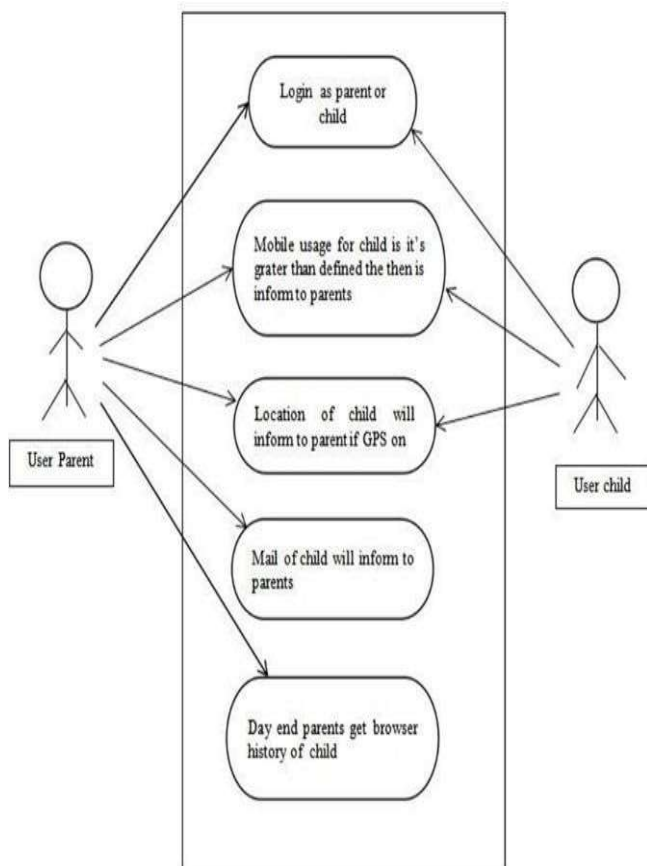


Figure 3.1 Use Case Visualization

3.2 SEPARATING BY TERM

This technique involves the filtration of websites by assessing the content against a specified set of keywords. Identical to the URL-based strategy, this approach is lightweight, and its efficacy relies entirely on the chosen collection of keywords, neglecting the contextual meaning of the terms. For example, the keyword-based approach blocks access to a website if its textual content includes the word "sex," which could be interpreted as referring to a sexual orientation [11]. It is important to note that Intelligent Content Analysis (ICA) can address this limitation. The ICA approach takes into account the context of terms on the document, but because conceptual calculations are difficult, using it causes latency [12]. This method has been used in previous times for text sorting and adultery screening.

3.3 SEPARATING BY CATEGORY

The written method involves the filtration of websites based on their content. This approach has found applications in various areas such as search queries, organization of internet knowledge materials, and details access. This technique has been investigated for a long period; citation offers a thorough overview of web mining in general.

Following that, scholarly works examined the web screening arena using more specificity, delving into computations, advantages, problems, and difficulties. The authors of [20] provide a thorough analysis of web identification and screening. Numerous research have used techniques like topic modeling [13,14], SVM models, and artificial brains [16] to achieve filtering with content.

4. TECHNIQUES FOR REMOVING OFFENSIVE MATERIAL

Given that most web pages are additionally written material and graphic material [21], it section outlines the techniques for filtering each type of content. Table 3.1 provides a comparative analysis of these techniques, detailing the algorithms utilized for each technique, and highlighting the strengths and limitations of these algorithms.

4.1 FILTERING INAPPROPRIATE TEXT

The first step in filtering offensive content is to categorize it; this is done by performing through computational methods for categorization of texts. The goal of text organization is to group written materials into separate groups, which distinguishes it compared to internet categorization in a pair of significant ways. The initial variation is that internet material includes a variety of data kinds (structured, semi-structured, and unstructured), yet the categorization of content is intended to categorize information that is organized. The inclusion of links for additional pages in web content, which is web pages, is another difference. Because of these differences, web categorization and categorization of text are both necessary for efficiently removing offensive language from web pages.

Classifying texts is a useful technique for filtering problematic text in a variety of domains, such as electronic libraries, subject of the topic, issue

removal, language screening, content autonomous categorization, as well as data retrieving [10, 12, 13]. A variety of techniques, including neural network algorithms, K-nearest neighbor strategies, Bayesian n computations, maximum-margin classifier programs, have been created and used in earlier research to improve text categorization [16,17]. When these algorithms are used, problematic text information is filtered more effectively.

4.2 FILTERING INAPPROPRIATE VISUAL CONTENT

The objective of screening objectionable images and videos involves the analysis and classification of these media based on contextual information, a subject extensively studied in previous research over the the previous 20 years. As explained in, visual categorization and screening face several difficulties and problems. Three approaches are employed for visual filtering: whitelist-driven, feature-based, and Pattern-based filtering.

The blacklisted-based method, which uses a list of webpages with inappropriate footage and pictures as part of its prohibited list, is similar to text screening. This method's effectiveness depends on the directory of references, which is frequently insufficient and made worse by an ongoing rise in the total quantity of webpages (more than 100 thousand dollars are included every day [9]). However, this approach can be greater effectiveness if periodic updating for website URLs is included in the system [9]. The method based on keywords yields names for images or videos, descriptions, and surrounding text for comparison with a database containing keywords. Although lightweight, this technique has two primary shortcomings: it uses such phrases to sort out web pages, even if employed for educational purposes, and faces challenges in updating the keyword database due to the substantial daily increase in websites [16]. Lastly, The centered around content perspective examines the information contained in video clips and pictures directly, with the efficiency of analysis influenced by the type of media. Prior study divides all forms of images and videos into 4 groups, which are : multi spectral, unambiguous, colorful, and monochromatic [16].

Out of all these methods, the content-based strategy works well for removing offensive content. Many techniques, such as bag-of-visual term, epidermis

identification, a CNN, or convolutional along with deep studying, subject modeling, and form identification, use the content-driven strategy for footage and clips. Given the wide range of methods and computations, visual and photographic categorization is primarily controlled by four phases: classifiers, collecting features, choosing picking, and preprocessing. By using these procedures and computations, unwanted pictures can be filtered more effectively.

5. SET OF DATA

A set of data is required for testing of every freshly suggested remedies. Within the domain of cyberparental supervision, statistics could contain unacceptable websites next to acceptable ones that are or disagreeable subjects compared to acceptable subjects. In this discipline, a standardized dataset makes it possible to compare and assess fresh and current approaches better. However, contradictory information are frequently used in modern research to evaluate their hypotheses and approaches.

Many existing solutions tailor their datasets to fit their specific model or framework requirements. While some studies have developed noteworthy datasets, such as [17-19], these datasets often focus on specific objectionable topics like xenophobic remarks, violent material, unwanted content, junk mail, and erotica. More comprehensive statistics have been created by additional research [15,20], but none of them are openly accessible. In light of these factors, it is imperative to create a publicly available dataset that includes both problematic and non-objectionable web pages.

6. NETWORK ARCHITECTURE

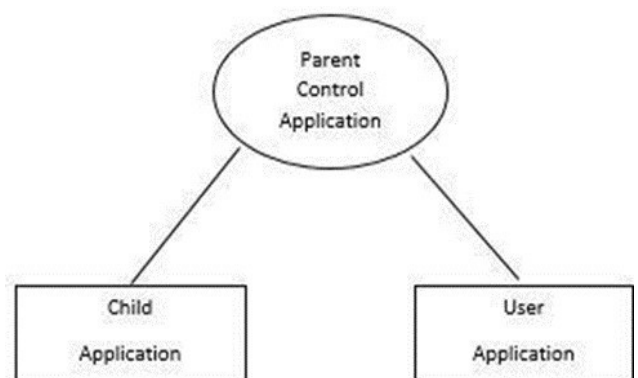


Figure 6.1: System Overview

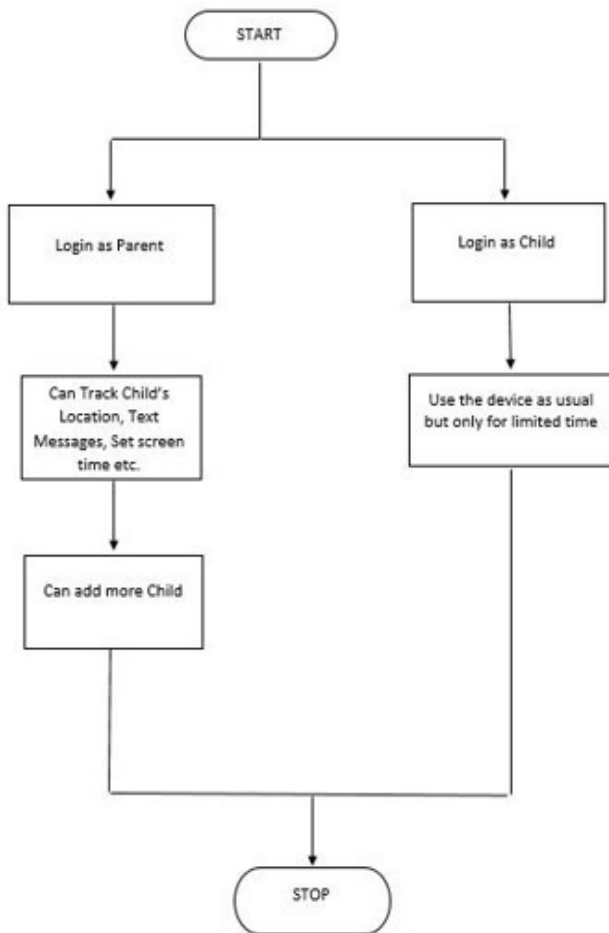


Figure 6.2: System Workflow Chart

7. DISCUSSION

This pilot study highlights the importance of the discipline of cyberparental supervision. The primary emphasis of present-day remedies revolves around the adoption of one of the methods mentioned earlier. However, each method possesses its own set of strengths and weaknesses. Consequently, relying solely on one method may result in the proposal of weak solutions. To address this challenge, the study recommends the exploration of a multi-layer approach, integrating multiples of any of the current techniques. Integrating the high-accuracy content-driven approach and the ultralight Link-based approach is one example.

Web pages usually consist of images as well as text, which together determine the type of webpage they are. Although an internet site can be effectively described by taking into account both linguistic and visual contents [15], the majority of online child protection solutions available today use either linguistic or graphical screening methods. This unique method could result in ineffective

screening. Thus, in order to improve the screening of problematic content, the research recommends combining linguistic and graphic techniques.

While current solutions extensively address the filtering of pornography content, it is crucial to recognize that other objectionable contents also pose risks to children using the Internet. The study urges that other obnoxious areas be included with pornography to create a safe online space for kids. These subjects include cyberbullying, hatred, violence, gambling and drug-related content.

8. FINALLY AND UPCOMING PROJECTS

Children may be at risk from abuse and bullying due to certain online content and activities.

This emphasizes how crucial it is to look into and comprehend studies on cyberparental control and their methodologies.

This study has explored the history of the idea of the "cyberparent," looked closely at the tactics and methods that have been deployed, and closely evaluated the datasets that have been used for training and assessment. These insights help us comprehend methodologies, approaches, and datasets in this field better as they haven't been thoroughly examined before. The advantages and disadvantages of techniques in the research that are on material, key term, and URLs addresses on cyberparental regulation are shown via an unbiased comparison. In this field, the problematic filtering mechanisms that are explored are linked to either visual or textual contents. The datasets that are now being used either don't make them publicly available or concentrate on particular pieces of undesirable content.

Future studies, research, and solutions in the field of cyberparental control must concentrate on developing plans to shield young users from the risks associated with using the Internet. Examples of topic modeling techniques that show promise in improving the efficacy of filtering problematic content include Independent Component Analysis (ICA), LDA, also known as Latent Dirichlet Allocation, and latent semantic examination (LSA) and its extensions. Furthermore, it is noteworthy that existing research on web content filtering lacks a consistent dataset, highlighting the necessity of creating an accessible and standardized dataset with both objectionable and non-objectionable

websites. Standardizing the dataset is essential to enhance the assessment of suggested fixes in this field.

REFERENCES

- [1] Altar Turi, H.H.M., Saadoon, M., and Anuar, N.B. (2020). "A bibliometric study on cyber parental control." Examines trends and patterns in cyber parental control measures.
- [2] Monteiro, A.F.C., Miranda-Pinto, M., and Osório, A.J. (2017). "Reviewing mobile app interventions for children's online safety." Investigates the effectiveness of mobile apps in promoting online safety for children.
- [3] Elsaesser, C., Russell, B., Ohannessian, C.M., and Patton, D. (2017). "Parental roles in preventing adolescent cyberbullying." Explores parental strategies to prevent cyberbullying among adolescents.
- [4] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). "EU Kids Online survey findings on internet risks and safety." Discusses findings from a survey on internet risks and safety among European children.
- [5] Valcke, M., De Wever, B., Van Keer, H., and Schellens, T. (2011). "Long-term study on safe internet use for young children." Examines the long-term effects of safe internet use among young children.
- [6] Dishion, T.J., and McMahon, R.J. (1998). "Parental monitoring for preventing problem behavior." Explores the role of parental monitoring in preventing problem behavior among adolescents.
- [7] Kerr, M., and Stattin, H. (2000). "Parental knowledge and adolescent adjustment." Investigates the relationship between parental knowledge and adolescent adjustment.
- [8] Hilal, S., and Gupta, N. (2013). "Web content mining for children's mobile search." Discusses the role of web content mining in improving children's mobile search experiences.
- [9] Netcraft (2018). "Web server survey." Provides insights into the landscape of web servers as of 2018.
- [10] Thomas, K., Grier, C., Ma, J., Paxson, V., and Song, D. (2011). "Real-time URL spam filtering service." Describes the design and evaluation of a real-time URL spam filtering service.
- [11] Narayanan, B.K., Moses, S., and Nirmala, M. (2018). "Filtering adult content to protect minors online." Discusses strategies for filtering adult content to protect minors online.
- [12] Lee, P.Y., Hui, S.C., and Fong, A.C.M. (2003). "Analysis for web filtering." Presents a structural and content-based analysis for web filtering.
- [13] Duan, J., and Zeng, J. (2013). "Detecting objectionable web content using topic modeling." Discusses the use of topic modeling for detecting objectionable web content.
- [14] Liu, S., and Forss, T. (2015). "Text classification models for web content filtering." Discusses text classification models for filtering objectionable web content.
- [15] Rajalakshmi, R., Tiwari, H., Patel, J., Kumar, A., and Karthik, R. (2020). "Designing a kids-specific URL classifier using neural networks." Presents the design of a URL classifier tailored for children using neural networks.
- [16] Zaidan, A.A., Karim, H.A., Ahmad, N.N., Zaidan, B.B., and Sali, A. (2013). "AI-based anti-pornography system using skin detection." Reviews an automated anti-pornography system using artificial intelligence.
- [17] Ma, J., Saul, L.K., Savage, S., and Voelker, G.M. (2009). "Learning to detect malicious websites from suspicious urls." Discusses a machine learning approach for detecting malicious websites from suspicious urls.
- [18] Rao, R.S., Vaishnavi, T., and Pais, A.R. (2020). "Detecting phishing websites by inspecting urls." Describes a method for detecting phishing websites by inspecting urls.
- [19] Sahingoz, O.K., Buber, E., Demir, O., and Diri, B. (2019). "Machine learning for phishing detection from urls." Discusses the use of machine learning for detecting phishing websites from urls.
- [20] Zhao, C., Zhang, Y., Zang, T., Liang, Z., and Wang, Y. (2018). "Identifying objectionable domain names using passive DNS traffic." Presents a method for identifying objectionable domain names using passive DNS traffic.
- [21] Rohit R, Hasan Firnas I, Abishek M, Albert Mayan J, Dhamodaran S (2023), "Web Application Security Testing Framework using Flask", International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2023, pp. 1646-1652

IJISRT24JAN1891

by Ijisrt24jan1891 Ijisrt24jan1891

Submission date: 31-Jan-2024 06:42PM (UTC+0700)

Submission ID: 2282831661

File name: 1706700417.pdf (559.04K)

Word count: 3305

Character count: 19836

Exploratory Examination of Cybersecurity-Based Parental Control Systems and Techniques

Prashant Shukla¹, R. Praneeth², Ms. Santhiya P³, Rajasekar P⁴

^{1,2}U.G Student, Department of CSE, Sathyabama Institute of Science and Technology, Chennai

^{3,4} Assistant Professor, School of Computing, Sathyabama Institute of Science and Technology, Chennai

prashantshukla7205@gmail.com¹, rokkampraneeth@gmail.com²,
santhiya.cse@sathyabama.ac.in³, rajasekar.cse@sathyabama.ac.in⁴

Abstract-The application enhances child safety and parental oversight by allowing parents to register and monitor their children's location through geofencing with boundary crossing alerts. It includes access to children's messages and call logs for communication supervision and tracks screen time to monitor usage. In emergencies, children can send voice messages to nearby parents, which are then forwarded to the administrator for action and contacting emergency services if needed. The app's signup and login are secured with AES encryption and decryption, offering a complete safety network that reassures parents and provides a reliable method for children to seek help when feeling unsafe. The study also emphasizes the vitality of studies in the area of online surveillance by parents, indicating a need for continuous improvement and adaptation to emerging challenges. The application aligns with this perspective by incorporating various features that contribute to a more effective and efficient system for Online Parental Guidance.

Keywords - Online Parental Guidance, Parental Monitoring, Child Safety Online, Internet Filtering, Content Restrictions, Online Safety Tools, Screen Time Management

1. OVERVIEW

The widespread use of internet technology enables the easy publication of diverse topics and fosters open communication between users. While the internet offers substantial benefits for children, the presence of objectionable content poses significant risks, with over half of child internet users inadvertently encountering harmful material. Such objectionable content can inflict psychological or mental harm on children, including harassment, guns, illicit substances, hate, betting, and brutality.

Aware of these dangers, business and academics stress the importance of using efficient cyberparental control devices and procedures to parent, supervise, and manage kids' online activity. Online supervision, as defined by earlier research, is the process by which parents regulate their kids' use of online resources, including online communities, networking sites, and the internet as a whole.

elements of cyber supervision that are covered in the research include the responsibilities of families, risks associated with cyber networks, scientific elements, and psychological and legal ramifications. Notwithstanding the importance of study in this field, little is known about the methodologies, strategies, and databases involved in cyberparental control. Filling such these gaps would improve our knowledge of previously underappreciated strategies, tactics, and sets of data.

To achieve this, the study aims to conduct a preliminary investigation into online parental guidance rolls around, strategies, and datasets pertaining to online parenting. It seeks to identify the optimal initiatives, their advantages and disadvantages as well as the sets of data that are now being utilized, providing information for upcoming research in the subject. Given the considerable number of children online and their vulnerability to various risks, studying this field is imperative.

This approach compares information sets, strategies, and tactics for cyberparental control using terms like "removing," "the online world," and "offensive." In order to concentrate on the most articles that have recently appeared in the Wos and Index libraries while eliminating irrelevant paperwork, binary operators such as the logical

GATE are utilized to refine the search outcomes inside the research's purview.

The research project is divided into 7 pieces, with a summary at the start of each. The first section goes over the background of cyberparental control. In turn, techniques for eliminating objectionable information from webpages are covered in Chapters 3 and 4. The field of cyberparental control's existing datasets are examined in Chapter 5. The paper's conclusion, found in Chapter 7, offers guidelines for further research in the area. Chapter 6 examines and recommends an efficient cyberparental supervision system.

2. CONTEXT

The terms "cyber parental control" and "monitoring and mediation by parents" are defined differently by the authors in [1]. The primary goal of controlling kids is to enable parents to track and regulate the actions of their kids both within and outside the home by establishing ground rules [6,7]. The definition of "a set of correlated parenting habits requiring constant surveillance and apprised of the child's motions, spots, and adjustments" is expanded to include surveillance by parents [6]. "Guardianship a mediator" has been used in books since the birth of media, involving interactions between parents or guardians and children concerning media. Parental mediation involves three main levels of restrictions: co-using, evaluative, and restrictive, with the latter being the most stringent [3]. In summary, online parental guidance encompasses a set of interrelated parental behaviours that enable parents or guardians to supervise and manage their kids' internet activity; according to the UN, the term "children" are those under the age of 18 years old, until they achieve majority earlier.

Information extraction techniques are applied to internet materials by online resource producers for classification, categorization, filtering, and recommendation purposes. Search engines, surveillance software, analyzing software, and educational browsers are the four categories of web miners [8]. Children's exposure to undesirable, practical, amusing, and social media websites is limited by educational internet browsers and customized browsers, which limit their access to just instructional webpages. Researchers has utilized this technique to create queries based on

filtering and classification techniques, frequently leveraging Google's specialized query to identify problematic web information . Lookup engines are computer programs intended for regular browsing of the internet. Technology that detects and keeps track of, documents, and examines what kids do online without filtering objectionable content, exposing children to the risks of objectionable material. Some monitoring software includes additional features such as A security program, phone filtering, tracking of movements, and spyware scanning features provide another level of complexity to stop unwanted information. Nevertheless, a major disadvantage of these programs and designs is that kids can use bypass tools to go around them. Filtering frameworks, on the other hand, analyze, classify, and manage visible information for minors by including a protective level to remove undesirable content. In the realm of online regulation by parents, it's the tactic that is most frequently employed. The strategies and tactics used by these filtering frameworks are covered in detail in the chapter that follows.

3. TECHNIQUES FOR BLOCKING OFFENSIVE WEBSITES

Earlier research in the realm computerized screening architectures of cyber guardianship have been used to deal with certain issues in this field. The aforementioned structures combine different methodologies such as website address, keyword, and content-focused methods with machine learning and material screening algorithms. Numerous research have used various techniques, each of which has advantages and disadvantages of that particular method. The first tableau provides a comparative analysis of these methods, highlighting their respective strengths and limitations.

3.1 WEB CONTENT SCREENING

This approach involves the filtration of websites by comparing the supplied Link along with a set of predetermined references. References come in a pair of forms: whitelisting & blacklisted. Webpages that are prohibited are listed on the prohibited list, and webpages that are permitted are listed on the whitelist. The list of sources has a significant impact on this method's efficacy despite its simplicity. With the hundreds of thousands of new

webpages created every day [9], the problem of potentially large failure rates arising from the incompleteness of these references is presented. Numerous settings have seen the application of Location-based screening, such as phishing screening, removal of spam, and sexuality screening [10].

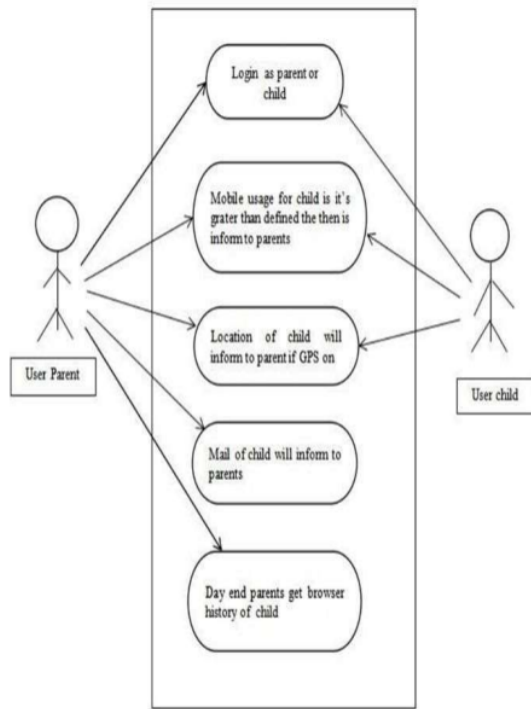


Figure 3.1 Use Case Visualization

3.2 SEPARATING BY TERM

This technique involves the filtration of websites by assessing the content against a specified set of keywords. Identical to the URL-based strategy, this approach is lightweight, and its efficacy relies entirely on the chosen collection of keywords, neglecting the contextual meaning of the terms. For example, the keyword-based approach blocks access to a website if its textual content includes the word "sex," which could be interpreted as referring to a sexual orientation [11]. It is important to note that Intelligent Content Analysis (ICA) can address this limitation. The ICA approach takes into account the context of terms on the document, but because conceptual calculations are difficult, using it causes latency [12]. This method has been used in previous times for text sorting and adultery screening.

3.3 SEPARATING BY CATEGORY

The written method involves the filtration of websites based on their content. This approach has found applications in various areas such as search queries, organization of internet knowledge materials, and details access. This technique has been investigated for a long period; citation offers a thorough overview of web mining in general.

Following that, scholarly works examined the web screening arena using more specificity, delving into computations, advantages, problems, and difficulties. The authors of [20] provide a thorough analysis of web identification and screening. Numerous research have used techniques like topic modeling [13,14], SVM models, and artificial brains [16] to achieve filtering with content.

4. TECHNIQUES FOR REMOVING OFFENSIVE MATERIAL

Given that most web pages are additionally written material and graphic material [21], itsection outlines the techniques for filtering each type of content. Table 3.1 provides a comparative analysis of these techniques, detailing the algorithms utilized for each technique, and highlighting the strengths and limitations of these algorithms.

4.1 FILTERING INAPPROPRIATE TEXT

The first step in filtering offensive content is to categorize it; this is done by performing through computational methods for categorization of texts. The goal of text organization is to group written materials into separate groups, which distinguishes it compared to internet categorization in a pair of significant ways. The initial variation is that internet material includes a variety of data kinds (structured, semi-structured, and unstructured), yet the categorization of content is intended to categorize information that is organized. The inclusion of links for additional pages in web content, which is web pages, is another difference. Because of these differences, web categorization and categorization of text are both necessary for efficiently removing offensive language from web pages.

Classifying texts is a useful technique for filtering problematic text in a variety of domains, such as electronic libraries, subject of the topic, issue

removal, language screening, content autonomous categorization, as well as data retrieving [10, 12, 13]. A variety of techniques, including neural network algorithms, K-nearest neighbor strategies, Bayesian n computations, maximum-margin classifier programs, have been created and used in earlier research to improve text categorization [16,17]. When these algorithms are used, problematic text information is filtered more effectively.

4.2 FILTERING INAPPROPRIATE VISUAL CONTENT

The objective of screening objectionable images and videos involves the analysis and classification of these media based on contextual information, a subject extensively studied in previous research over the the previous 20 years. As explained in, visual categorization and screening face several difficulties and problems. Three approaches are employed for visual filtering: whitelist-driven, feature-based, and Pattern-based filtering.

The blacklisted-based method, which uses a list of webpages with inappropriate footage and pictures as part of its prohibited list, is similar to text screening. This method's effectiveness depends on the directory of references, which is frequently insufficient and made worse by an ongoing rise in the total quantity of webpages (more than 100 thousand dollars are included every day [9]). However, this approach can be greater effectiveness if periodic updating for website URLs is included in the system [9]. The method based on keywords yields names for images or videos, descriptions, and surrounding text for comparison with a database containing keywords. Although lightweight, this technique has two primary shortcomings: it uses such phrases to sort out web pages, even if employed for educational purposes, and faces challenges in updating the keyword database due to the substantial daily increase in websites [16]. Lastly, The centered around content perspective examines the information contained in video clips and pictures directly, with the efficiency of analysis influenced by the type of media. Prior study divides all forms of images and videos into 4 groups, which are : multi spectral, unambiguous, colorful, and monochromatic [16].

Out of all these methods, the content-based strategy works well for removing offensive content. Many techniques, such as bag-of-visual term, epidermis

identification, a CNN, or convolutional along with deep studying, subject modeling, and form identification, use the content-driven strategy for footage and clips. Given the wide range of methods and computations, visual and photographic categorization is primarily controlled by four phases: classifiers, collecting features, choosing picking, and preprocessing. By using these procedures and computations, unwanted pictures can be filtered more effectively.

5. SET OF DATA

A set of data is required for testing of every freshly suggested remedies. Within the domain of cyberparental supervision, statistics could contain unacceptable websites next to acceptable ones that are or disagreeable subjects compared to acceptable subjects. In this discipline, a standardized dataset makes it possible to compare and assess fresh and current approaches better. However, contradictory information are frequently used in modern research to evaluate their hypotheses and approaches.

Many existing solutions tailor their datasets to fit their specific model or framework requirements. While some studies have developed noteworthy datasets, such as [17-19], these datasets often focus on specific objectionable topics like xenophobic remarks, violent material, unwanted content, junk mail, and erotica. More comprehensive statistics have been created by additional research [15,20], but none of them are openly accessible. In light of these factors, it is imperative to create a publicly available dataset that includes both problematic and non-objectionable web pages.

6. NETWORK ARCHITECTURE

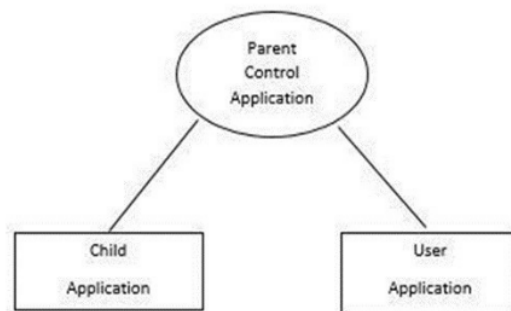


Figure 6.1: System Overview



Figure 6.2: System Workflow Chart

7. DISCUSSION

This pilot study highlights the importance of the discipline of cyberparental supervision. The primary emphasis of present-day remedies revolves around the adoption of one of the methods mentioned earlier. However, each method possesses its own set of strengths and weaknesses. Consequently, relying solely on one method may result in the proposal of weak solutions. To address this challenge, the study recommends the exploration of a multi-layer approach, integrating multiples of any of the current techniques. Integrating the high-accuracy content-driven approach and the ultralight Link-based approach is one example.

Web pages usually consist of images as well as text, which together determine the type of webpage they are. Although an internet site can be effectively described by taking into account both linguistic and visual contents [15], the majority of online child protection solutions available today use either linguistic or graphical screening methods. This unique method could result in ineffective

screening. Thus, in order to improve the screening of problematic content, the research recommends combining linguistic and graphic techniques.

While current solutions extensively address the filtering of pornography content, it is crucial to recognize that other objectionable contents also pose risks to children using the Internet. The study urges that other obnoxious areas be included with pornography to create a safe online space for kids. These subjects include cyberbullying, hatred, violence, gambling and drug-related content.

8. FINALLY AND UPCOMING PROJECTS

Children may be at risk from abuse and bullying due to certain online content and activities.

This emphasizes how crucial it is to look into and comprehend studies on cyberparental control and their methodologies.

This study has explored the history of the idea of the "cyberparent," looked closely at the tactics and methods that have been deployed, and closely evaluated the datasets that have been used for training and assessment. These insights help us comprehend methodologies, approaches, and datasets in this field better as they haven't been thoroughly examined before. The advantages and disadvantages of techniques in the research that are on material, key term, and URLs addresses on cyberparental regulation are shown via an unbiased comparison. In this field, the problematic filtering mechanisms that are explored are linked to either visual or textual contents. The datasets that are now being used either don't make them publicly available or concentrate on particular pieces of undesirable content.

Future studies, research, and solutions in the field of cyberparental control must concentrate on developing plans to shield young users from the risks associated with using the Internet. Examples of topic modeling techniques that show promise in improving the efficacy of filtering problematic content include Independent Component Analysis (ICA), LDA, also known as Latent Dirichlet Allocation, and latent semantic examination (LSA) and its extensions. Furthermore, it is noteworthy that existing research on web content filtering lacks a consistent dataset, highlighting the necessity of creating an accessible and standardized dataset with both objectionable and non-objectionable

2 websites. Standardizing the dataset is essential to enhance the assessment of suggested fixes in this field.

REFERENCES

- [1] Altar Turi, H.H.M., Saadoon, M., and Anuar, N.B. (2020). "A bibliometric study on cyber parental control." Examines trends and patterns in cyber parental control measures.
- [2] Monteiro, A.F.C., Miranda-Pinto, M., and Osório, A.J. (2017). "Reviewing mobile app interventions for children's online safety." Investigates the effectiveness of mobile apps in promoting online safety for children.
- [3] Elsaesser, C., Russell, B., Ohannessian, C.M., and Patton, D. (2017). "Parental roles in preventing adolescent cyberbullying." Explores parental strategies to prevent cyberbullying among adolescents.
- [4] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). "EU Kids Online survey findings on internet risks and safety." Discusses findings from a survey on internet risks and safety among European children.
- [5] Valcke, M., De Wever, B., Van Keer, H., and Schellens, T. (2011). "Long-term study on safe internet use for young children." Examines the long-term effects of safe internet use among young children.
- [6] Dishion, T.J., and mcmahon, R.J. (1998). "Parental monitoring for preventing problem behavior." Explores the role of parental monitoring in preventing problem behavior among adolescents.
- [7] Kerr, M., and Stattin, H. (2000). "Parental knowledge and adolescent adjustment." Investigates the relationship between parental knowledge and adolescent adjustment.
- [8] Hilal, S., and Gupta, N. (2013). "Web content mining for children's mobile search." Discusses the role of web content mining in improving children's mobile search experiences.
- [9] Netcraft (2018). "Web server survey." Provides insights into the landscape of web servers as of 2018.
- [10] Thomas, K., Grier, C., Ma, J., Paxson, V., and Song, D. (2011). "Real-time URL spam filtering service." Describes the design and evaluation of a real-time URL spam filtering service.
- [11] Narayanan, B.K., Moses, S., and Nirmala, M. (2018). "Filtering adult content to protect minors online." Discusses strategies for filtering adult content to protect minors online.
- [12] Lee, P.Y., Hui, S.C., and Fong, A.C.M. (2003). "Analysis for web filtering." Presents a structural and content-based analysis for web filtering.
- [13] Duan, J., and Zeng, J. (2013). "Detecting objectionable web content using topic modeling." Discusses the use of topic modeling for detecting objectionable web content.
- [14] Liu, S., and Forss, T. (2015). "Text classification models for web content filtering." Discusses text classification models for filtering objectionable web content.
- [15] Rajalakshmi, R., Tiwari, H., Patel, J., Kumar, A., and Karthik, R. (2020). "Designing a kids-specific URL classifier using neural networks." Presents the design of a URL classifier tailored for children using neural networks.
- [16] Zaidan, A.A., Karim, H.A., Ahmad, N.N., Zaidan, B.B., and Sali, A. (2013). "AI-based anti-pornography system using skin detection." Reviews an automated anti-pornography system using artificial intelligence.
- [17] Ma, J., Saul, L.K., Savage, S., and Voelker, G.M. (2009). "Learning to detect malicious websites from suspicious urls." Discusses a machine learning approach for detecting malicious websites from suspicious urls.
- [18] Rao, R.S., Vaishnavi, T., and Pais, A.R. (2020). "Detecting phishing websites by inspecting urls." Describes a method for detecting phishing websites by inspecting urls.
- [19] Sahingoz, O.K., Buber, E., Demir, O., and Diri, B. (2019). "Machine learning for phishing detection from urls." Discusses the use of machine learning for detecting phishing websites from urls.
- [20] Zhao, C., Zhang, Y., Zang, T., Liang, Z., and Wang, Y. (2018). "Identifying objectionable domain names using passive DNS traffic." Presents a method for identifying objectionable domain names using passive DNS traffic.
- [21] Rohit R, Hasan Firmas I, Abishek M, Albert Mayan J, Dhamodaran S (2023), "Web Application Security Testing Framework using Flask", International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2023, pp. 1646-1652

ORIGINALITY REPORT

2%

SIMILARITY INDEX

1%

INTERNET SOURCES

2%

PUBLICATIONS

1%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to International University of
Malaya-Wales

Student Paper

1%

2

Hamza H. M. Altarturi, Nor Badrul Anuar. "A
preliminary study of cyber parental control
and its methods", 2020 IEEE Conference on
Application, Information and Network
Security (AINS), 2020

Publication

1%

3

Mirza Rayana Sanzana, Mostafa Osama
Mostafa Abdulrazic, Jing Ying Wong, Tomas
Maul, Chun-Chieh Yip. "The potential of deep
learning in dynamic maintenance scheduling
for thermal energy storage chiller plants",
Elsevier BV, 2024

Publication

<1%

Exclude quotes

Off

Exclude matches

Off

Exclude bibliography

On

FINAL GRADE

GENERAL COMMENTS

/0

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

Reviewer's Review Points for Paper id **IJISRT24JAN1891**

Stage 1 Review: -

1: - Paper plagiarism is 2% at Turnitin which was checked on the date of 31 January 2024

Stage 2 Review: -

Does the paper contain the Paper Title ?	Yes
Does the paper contain the Abstract ?	Yes
Does the paper contain the Introduction ?	Yes
Does the paper contain the Conclusion ?	Yes
Does the paper contain the References ?	Yes
Is Paper Title original ?	Yes
Is the paper Abstract original ?	Yes

Is paper Conclusion original ?	Yes
Is the paper contains all the title of Figures / Tables ?	Yes
Is paper in English language ?	Yes
Submitted paper topic related to IJISRT topics ?	Yes
Is the author describe the objective of the research ?	Yes
Is the author provide the results of the research ?	No
Is the author provide a Literature Review of previous papers ?	No



Yours sincerely,
*Chief-in-Editor International Journal of Innovative Science and Research
Technology(IJISRT)*
www.ijisrt.com
editor@ijisrt.com
ISSN No: - 2456-2165



Prashant Shukla <prashantshukla7205@gmail.com>

Research paper submission

1 message

Prashant Shukla <prashantshukla7205@gmail.com>

Mon, Feb 5, 2024 at 12:32 PM

To: conferenceiccet@gmail.com

Name:- Prashant Shukla

Email:- prashantshukla7205@gmail.com

Mobile:- 9155414435

Location:- Chennai, india

Title:- Exploratory Examination of Cybersecurity-Based Parental Control
Systems and Techniques



final pdf.pdf

560K

Exploratory Examination of Cybersecurity-Based Parental Control Systems and Techniques

3 messages

prof prince <conferenceiccet@gmail.com>
To: Prashant Shukla <prashantshukla7205@gmail.com>

Thu, Feb 8, 2024 at 1:53 PM

Dear Author/s,

We are happy to inform you that your paper, submitted for the ICCET 2024 conference has been **Accepted** based on the recommendations provided by the Technical Review Committee. By this mail you are requested to proceed with Registration for the Conference. Most notable is that the Conference must be registered on or before **FEBRUARY 29, 2024** from the date of acceptance.

www.iccet.in

Kindly fill the **registration form**, **declaration form** which is attached with the mail and it should reach us on above mentioned days.

Instructions to fill the forms:

- Ensure to send **payment screenshots** and send all the details once the payment has been done to the account.
- All the above completed details should be mailed to conferenceiccet@gmail.com
- Please send a soft copy of the RESEARCH PAPER in word format only.


NOTE: - Send Abstract and Full paper separately in word format only.

We reserve the right to reject your paper if the registration is not done within the above said number of days.

Paper id: ICCET240278

ICCET 2024
www.iccet.in
9600034378

2 attachments

 **Registration Instructions & Declaration form - 12TH ICCET 2024.doc**
126K

 **Registration form - ICCET 2024.xls**
32K

prof prince <conferenceiccet@gmail.com>
To: Prashant Shukla <prashantshukla7205@gmail.com>, Rokkam Praneeth <rokkampraneeth@gmail.com>

Thu, Feb 8, 2024 at 1:58 PM

Dear Author/s,

We are happy to inform you that your paper, submitted for the ICCET 2024 conference has been **Accepted** based on the recommendations provided by the Technical Review Committee. By this mail you are requested to proceed with Registration for the Conference. Most notable is that the Conference must be registered on or before **FEBRUARY 29, 2024** from the date of acceptance.

www.iccet.in

Kindly fill the **registration form**, **declaration form** which is attached with the mail and it should reach us on above mentioned days.

Instructions to fill the forms:

- Ensure to send **payment screenshots** and send all the details once the payment has been done to the account.
- All the above completed details should be mailed to conferenceiccet@gmail.com

- Please send a soft copy of the RESEARCH PAPER in word format only.

NOTE: - Send Abstract and Full paper separately in word format only.

We reserve the right to reject your paper if the registration is not done within the above said number of days.

Paper id: ICCET240279

ICCET 2024
www.iccet.in
9600034378

2 attachments



Registration form - ICCET 2024.xls
32K



Registration Instructions & Declaration form - 12TH ICCET 2024.doc
126K

Prashant Shukla <prashantshukla7205@gmail.com>
To: santhiya.cse@sathyabama.ac.in

Thu, Feb 8, 2024 at 2:00 PM

[Quoted text hidden]

2 attachments



Registration form - ICCET 2024.xls
32K



Registration Instructions & Declaration form - 12TH ICCET 2024.doc
126K



Prashant Shukla <prashantshukla7205@gmail.com>

Paper Submission Notification

1 message

Ijisrt digital library <editor@ijisrt.com>
Reply-To: "ijisrt@gmail.com" <ijisrt@gmail.com>
To: prashantshukla7205@gmail.com
Cc: ijisrt@gmail.com

Wed, Jan 31, 2024 at 4:56 PM

Hello Author ,

Greetings of the day

Paper ID :- "IJISRT24JAN1891"

Paper Title :- "Exploratory Examination of Cybersecurity-Based Parental Control Systems and Techniques"

Congratulations.....

We are happy to inform you that your research paper has been "Submitted" for publishing in "International Journal of Innovative Science and Research Technology".

For the most updated information on the publication, please check the official website at www.ijisrt.com . For any query reply us .

Yours sincerely,
Editor-in-Chief
International Journal of Innovative Science and Research Technology(IJISRT)
www.ijisrt.com
ISSN No :- 2456-2165
Impact Factor :- 7.176

Paper Acceptance Notification for Paper ID "IJISRT24JAN1891"

1 message

Ijisrt digital library <editor@ijisrt.com>

Fri, Feb 2, 2024 at 2:57 PM

Reply-To: "ijisrt@gmail.com" <ijisrt@gmail.com>

To: prashantshukla7205@gmail.com

Cc: ijisrt@gmail.com

Hello Author ,

Greetings of the day

Paper ID: "IJISRT24JAN1891"**Paper Title: "EXPLORATORY EXAMINATION OF CYBERSECURITY-BASED PARENTAL CONTROL SYSTEMS AND TECHNIQUES"**

Congratulations.....

We are happy to inform you that your research paper has been "Accepted" for publishing in "International Journal of Innovative Science and Research Technology". After completion of the registration processes, your research paper will be available on IJISRT official website in Volume 9 - 2024 - Issue 1 - January.

Registration Amount :- 1500/- (INR)**Submit Publication Fee :-**

You can Pay by Debit Card / Credit Card / Net Banking . For Submit Registration Fee click at given Link.

<https://ijisrt.com/ijisrt-payment-gateway>**OR****Bank Details :-**

A/C Number:- 677105500289

A/C Holder Name:- IJISRT

IFSC Code:- ICIC0006771

Bank :- ICICI

A/C Type :- Current

OR**You can make payment by UPI / VPA also. UPI / VPA ID is**

ijisrt@ibl

(Important) In order to the complete registration you must finish following steps.

1. Download and complete the Copyright Form enclosed in this mail. In the Attachment , you will get Pdf/.Doc both Format. You can download as per suitable format.
2. Login and submit Copyrightform, Payment Slip and Paper (.doc, .docx) till the last date.

Important Dates:-**Last Date For Submission of Registration Fee ,Copyright Form and Paper :- 05/02/2024(DD/MM/YYYY)**

For any query please login to account and use Help & Support.

Click here for [Login](#).

Thanks.

Yours sincerely,

Editor-in-Chief

International Journal of Innovative Science and Research Technology(IJISRT)

www.ijisrt.com

ISSN No :- 2456-2165

Impact Factor :- 7.176

2 attachments



1624772649.pdf

40K



1624772649.docx

117K