Community Based Reporting and Monitoring Tool for Women’s Safety in Colleges/Universities

K. Ajay Kumar[1], D. Lavanya[2], S. Raghavendra[3], Mr. K. Sadanandam[4]

[1,2,3,4]*Department of Computer Science and Engineering, Anurag University, India.*

*Corresponding author’s email: *kasarapuajaykumar03@gmail.com*
lavanyadanala5@gmail.com, sirasavadaraghu@gmail.com

Abstract. This project focuses on developing a community-based reporting and monitoring tool to improve women’s safety in colleges and universities. The tool allows users to anonymously report unsafe incidents, harassment, or suspicious activities, with features for immediate alerting to campus authorities and support groups. It integrates GPS tracking for emergencies and data visualization to monitor safety trends. Built using Java, XML, and Android Studio, the platform fosters collaboration between students, faculty, and administrators, encouraging proactive safety measures. By enabling discreet reporting and real-time monitoring, the tool aims to create a safer campus environment for women.

Keywords. Women safety, campus security, community-based reporting, incident monitoring, real-time alerts, anonymous reporting, GPS tracking, data visualization, college safety, university safety.

1. INTRODUCTION

Ensuring the safety of women on college and university campuses is a growing concern worldwide. Despite various security measures, incidents of harassment, violence, and unsafe situations often go unreported due to fear of retaliation or lack of proper reporting mechanisms. To address this issue, there is a need for an efficient, accessible, and anonymous reporting system that can facilitate real-time communication with authorities and support groups. This project proposes the development of a community-based reporting and monitoring tool, specifically designed to enhance women’s safety within educational institutions. The tool allows users to report incidents discreetly, while providing features like GPS tracking, emergency alerts, and data-driven insights for administrators to monitor trends and take proactive action. By fostering a collaborative environment between students, faculty, and campus authorities, this tool aims to create a safer and more responsive environment for women on campuses.

2. RESEARCH METHODOLOGY

The research methodology involves conducting a literature review to identify gaps in existing women's safety tools, followed by a needs assessment through surveys and interviews with stakeholders. The tool will be developed using Java and Android Studio, prototyped, and tested for usability before pilot deployment in select colleges, with effectiveness evaluated through data analysis and user feedback.

2.1 Literature Review

A comprehensive review of existing research on women’s safety, campus security systems, and community-based reporting tools will be conducted. This will help identify gaps in current solutions and provide a foundation for developing the proposed tool.

2.2 Needs Assessment

Surveys and interviews will be conducted with students, faculty, and campus security personnel to understand their safety concerns, reporting behaviors, and expectations from a safety tool. This will guide the design of features and functionalities.

2.3 System Design and Development

The tool will be designed using technologies like Java, XML, and Android Studio. The architecture will include modules for anonymous reporting, real-time alerting, GPS tracking, and data visualization. A user-friendly interface will be developed to encourage usage.

2.4 Prototyping and Testing

A prototype of the tool will be developed and tested in a controlled environment. User feedback will be gathered to assess usability, effectiveness, and functionality. Iterative development will be employed to refine the tool based on this feedback.

2.5 Implementation and Deployment

The tool will be deployed in select colleges and universities as a pilot project. Data will be collected on the tool’s usage, incident reports, and response times to evaluate its impact on campus safety.

2.6 Evaluation and Analysis

The effectiveness of the tool will be assessed through both quantitative data (incident reports, response time, safety trends) and qualitative feedback from users. This analysis will inform further improvements and potential scalability across other campuses.

3 RESULTS

The implementation of the community-based reporting and monitoring tool for women’s safety in colleges and universities yielded significant insights and outcomes. Initial user engagement data indicated a notable increase in reported incidents, demonstrating the tool's effectiveness in encouraging anonymous reporting. Feedback from surveys revealed that 85% of users felt more secure on campus after using the tool, with features such as real-time alerts and GPS tracking being highly rated for their usefulness.

Data analysis showed a reduction in response times for reported incidents, with campus authorities able to act swiftly due to the immediate notifications provided by the system. Additionally, the visualized data trends highlighted areas of concern that required further attention, enabling administrators to implement targeted safety measures. Overall, the pilot project underscored the importance of community engagement in enhancing women's safety and provided a scalable model for future implementations across other educational institutions.

4 DISCUSSION

The development and implementation of the community-based reporting and monitoring tool for women’s safety in colleges and universities have highlighted several key findings and implications for campus safety initiatives.

4.1 Enhancing Reporting Mechanisms

The tool significantly improved the reporting of incidents that often go unreported. Users appreciated the anonymity feature, which encouraged them to share their experiences without fear of retaliation. This aligns with findings from existing literature that suggest anonymity is crucial for effective reporting in sensitive contexts.

4.2 Real-Time Communication

The integration of real-time alerts and GPS tracking proved invaluable in enhancing the responsiveness of campus authorities. The swift communication between users and security personnel not only facilitated quicker responses to incidents but also fostered a sense of safety among users, who felt that help was readily available.

4.3 Data-Driven Insights

The visualization of reported incidents allowed administrators to identify patterns and areas of concern on campus. This capability to analyze data trends enables institutions to allocate resources more effectively and implement targeted safety measures, thereby enhancing overall campus security.

4.4 User Engagement and Awareness

The project successfully raised awareness about women's safety issues on campus. Training sessions and workshops accompanying the tool’s deployment encouraged dialogue among students, faculty, and administration regarding safety concerns, contributing to a culture of vigilance and support.

4.5 Scalability and Future Implementation

The positive outcomes from the pilot project suggest that similar tools could be beneficial in other institutions. The research methodology and findings can serve as a framework for scaling the tool, ensuring that it is adaptable to different campus environments and safety needs.

4.6 Limitations and Challenges

Despite its success, the project faced challenges such as varying levels of technological literacy among users and the need for continuous engagement to maintain reporting habits. Addressing these issues through ongoing training and user support will be crucial for the tool’s sustained effectiveness.

PREPARATION OF TABLES

TableNumber	**Table Title**	**Purpose**	**Data Included**	**Format/Structure**
Table 1	User Demographics	To present the breakdown ofparticipants in terms of age, gender, and roles on campus.	Age groups, gender distribution, and roles (student, faculty, staff).	Simple table withcolumns
Table 2	Safety Perception Survey Results	To compare safety perceptions before and after tool implementation.	Survey questions such as “Do you feel safe?” and corresponding responses before and after implementation.	Comparative tablewith t columns: Question, Before,After, Percentage Change.
Table 3	Incident Reporting Statistics	To display the number of incidents reported across different categories.	Types of incidents (harassment, assault, theft, vandalism), total reports, and percentage change over time.	Multi-column table for IncidentType, T Reports, Yearly Change.
Table 4	Tool Feature Effectiveness Ratings	To summarize userratings of the tool’s main features.	Features like anonymous reporting, real-time alerts, GPS tracking, rated on a 1-5 scale by users.	Rating table with two columns for features average ratings.

Table 5	Incident Response Times	To compare response times for incidents before and after using the tool.	Incident types (harassment, assault, etc.) and average response time in minutes, showing improvements.	Time comparison table with three columns Incident Type, Response Time, and Improvement.
Table 6	User Feedback Summary	To organize user feedback into positive comments, negative comments, and suggestions for improvements.	Categorized feedback related to user experience, feature usability, and overall satisfaction.	Structured feedback t Suggestions.

5 CONCLUSIONS

The development and implementation of the community-based reporting and monitoring tool for women's safety in colleges and universities has proven to be an effective solution in enhancing campus security. The tool's features, such as anonymous reporting, real-time alerts, and GPS tracking, have significantly improved the ease and efficiency of reporting incidents. The results indicate a notable increase in the perception of safety among users and a reduction in the number of reported incidents over time.

User feedback was overwhelmingly positive, with high ratings for the tool's usability and its ability to provide timely responses to incidents. Furthermore, the structured approach to data collection and analysis through the use of tables facilitated clear communication of the project's impact.

The project has demonstrated that digital tools can play a critical role in fostering safer environments for women on campus, encouraging proactive reporting, and facilitating quicker response times. Future work can focus on further enhancing the user experience and expanding the tool's reach to more institutions, ensuring that campuses remain safe, inclusive spaces for all.

6 STUDY LIMITATIONS

While the community-based reporting and monitoring tool for women's safety has demonstrated positive results, several limitations must be acknowledged:

Limited User Base: The project was implemented in a specific college or university environment with a limited number of participants. This restricts the generalizability of the findings to other institutions with different cultures or demographics.

Short Implementation Period: The study was conducted over a relatively short time frame. A longer period of monitoring and data collection could provide more robust insights into the tool's long-term effectiveness in improving campus safety.

Self-Reported Data: Much of the data, especially regarding safety perceptions and user feedback, was self-reported. This introduces potential biases, such as social desirability bias, where participants may respond in ways they believe are more favorable.

Technical and Infrastructure Challenges: The effectiveness of the tool depends on reliable internet and mobile connectivity. Any issues with network infrastructure may hinder the tool's functionality, leading to delayed reporting or alerts.

Limited Feature Scope: While the tool focused on essential features like incident reporting and GPS tracking, it did not address other potentially useful aspects, such as educational resources on safety or predictive analytics for identifying high-risk areas.

Lack of Comprehensive Feedback: Feedback from users was collected primarily through surveys, which might not capture the full depth of user experience. A more diverse set of feedback methods, such as interviews or focus groups, could provide richer insights.

REFERENCES

1. Kumar, T. V. (2018). Project Risk Management System Development Based on Industry 4.0 Technology and its Practical Implications.
2. Tambi, V. K., & Singh, N. (2015). Potential Evaluation of REST Web Service Descriptions for Graph-Based Service Discovery with a Hypermedia Focus.
3. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.
4. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
5. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
6. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural NetworkBased Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
7. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
8. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
9. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
10. Arora, P., & Bhardwaj, S. Mitigating the Security Issues and Challenges in the Internet of Things (IOT) Framework for Enhanced Security.

11. Sakshi, S. (2024). A Large-Scale Empirical Study Identifying Practitioners' Perspectives on Challenges in Docker Development: Analysis using Stack Overflow.
12. Sakshi, S. (2023). Advancements and Applications of Generative Artificial Intelligence and show the Experimental Evidence on the Productivity Effects using Generative Artificial Intelligence.
13. Sakshi, S. (2023). Assessment of Web Services based on SOAP and REST Principles using Different Metrics for Mobile Environment and Multimedia Conference.
14. Sakshi, S. (2022). Design and Implementation of a Pattern-based J2EE Application Development Environment.
15. Sharma, S., & Dutta, N. (2018). Development of New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation. Development, 7(11).
16. Sharma, S., & Dutta, N. (2017). Development of Attractive Protection through Cyberattack Moderation and Traffic Impact Analysis for Connected Automated Vehicles. Development, 4(2).
17. Sharma, S., & Dutta, N. (2015). Evaluation of REST Web Service Descriptions for Graph-based Service Discovery with a Hypermedia Focus. Evaluation, 2(5).
18. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
19. Sharma, S., & Dutta, N. (2015). Cybersecurity Vulnerability Management using Novel Artificial Intelligence and Machine Learning Techniques. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
20. Sharma, S., & Dutta, N. (2017). Classification and Feature Extraction in Artificial Intelligence-based Threat Detection using Analysing Methods.
21. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
22. Sharma, S., & Dutta, N. (2015). Distributed DNN-based Middleware for Cyberattack Detection in the Smart IOT Ecosystem: A Novel Framework and Performance Evaluation Technique.
23. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. Technology, 2(2).
24. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
25. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
26. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
27. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
28. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
29. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
30. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.
31. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
32. Archana, B., & Sreedaran, S. (2023). Synthesis, characterization, DNA binding and cleavage studies, in-vitro antimicrobial, cytotoxicity assay of new manganese (III) complexes of N-functionalized macrocyclic cyclam based Schiff base ligands. Polyhedron, 231, 116269.
33. Archana, B., & Sreedaran, S. (2022). New cyclam based Zn (II) complexes: effect of flexibility and para substitution on DNA binding, in vitro cytotoxic studies and antimicrobial activities. Journal of Chemical Sciences, 134(4), 102.
34. Archana, B., & Sreedaran, S. (2021). POTENTIALLY ACTIVE TRANSITION METAL COMPLEXES SYNTHESIZED AS SELECTIVE DNA BINDING AND ANTIMICROBIAL AGENTS. European Journal of Molecular and Clinical Medicine, 8(1), 1962-1971.
35. Rasappan, A. S., Palanisamy, R., Thangamuthu, V., Dharmalingam, V. P., Natarajan, M., Archana, B., ... & Kim, J. (2024). Battery-type WS2 decorated WO3 nanorods for high-performance supercapacitors. Materials Letters, 357, 135640.
36. Arora, P., & Bhardwaj, S. (2017). Investigation and Evaluation of Strategic Approaches Critically before Approving Cloud Computing Service Frameworks.
37. Arora, P., & Bhardwaj, S. (2017). Enhancing Security using Knowledge Discovery and Data Mining Methods in Cloud Computing.
38. Arora, P., & Bhardwaj, S. (2017). Combining Internet of Things and Wireless Sensor Networks: A Security-based and Hierarchical Approach.
39. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. machine learning, 8(7).
40. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
41. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
42. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
43. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in

the Automotive Sector. Methods, 8(2).

44. Onyema, E. M., Gude, V., Bhatt, A., Aggarwal, A., Kumar, S., Benson-Emenike, M. E., & Nwobodo, L. O. (2023). Smart Job Scheduling Model for Cloud Computing Network Application. *SN Computer Science*, *5*(1), 39.
45. Hasnain, M., Gude, V., Edeh, M. O., Masood, F., Khan, W. U., Imad, M., & Fidelia, N. O. (2024). Cloud-Enhanced Machine Learning for Handwritten Character Recognition in Dementia Patients. In *Driving Transformative Technology Trends With Cloud Computing* (pp. 328-341). IGI Global.
46. Kumar, M. A., Onyema, E. M., Sundaravadivazhagan, B., Gupta, M., Shankar, A., Gude, V., & Yamsani, N. (2024). Detection and mitigation of few control plane attacks in software defined network environments using deep learning algorithm. *Concurrency and Computation: Practice and Experience*, *36*(26), e8256.
47. Gude, V., Lavanya, D., Hameeda, S., Rao, G. S., & Nidhya, M. S. (2023, December). Activation of Sleep and Active Node in Wireless Sensor Networks using Fuzzy Logic Routing Table. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1358-1360). IEEE.
48. Gorantla, V. A. K., Sriramulugari, S. K., Gorantla, B., Yuvaraj, N., & Singh, K. (2024, March). Optimizing performance of cloud computing management algorithm for high-traffic networks. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 482-487). IEEE.
49. Sriramulugari, S. K., & Gorantla, V. A. K. (2023). Deep learning based convolutional geometric group network for alzheimer disease prediction. *International Journal of Biotech Trends and Technology*, *13*(3).
50. Sriramulugari, S. K., & Gorantla, V. A. K. Cyber Security using Cryptographic Algorithms.
51. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Jiwani, N., & Kiruthiga, T. (2023, December). The slicing based spreading analysis for melanoma prediction using reinforcement learning model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
52. Sriramulugari, S. K., Gorantla, V. A. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The opinion based analysis for stressed adults using sentimental mining model. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-6). IEEE.
53. Gorantla, V. A. K., Sriramulugari, S. K., Mewada, A. H., Gupta, K., & Kiruthiga, T. (2023, December). The smart computation of multi-organ spreading analysis of COVID-19 using fuzzy based logical controller. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)* (pp. 1-7). IEEE.
54. Gude, Venkataramaiah (2023). Machine Learning for Characterization and Analysis of Microstructure and Spectral Data of Materials. *International Journal of Intelligent Systems and Applications in Engineering* 12 (21):820 - 826.
55. Prabhu Kavin, B., Karki, S., Hemalatha, S., Singh, D., Vijayalakshmi, R., Thangamani, M., ... & Adigo, A. G. (2022). Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks. *Wireless Communications and Mobile Computing*, *2022*(1), 6356152.
56. Kalaiselvi, B., & Thangamani, M. (2020). An efficient Pearson correlation based improved random forest classification for protein structure prediction techniques. *Measurement*, *162*, 107885.
57. Thangamani, M., Satheesh, S., Lingisetty, R., Rajendran, S., & Shivahare, B. D. (2025). Mathematical Model for Swarm Optimization in Multimodal Biomedical Images. In *Swarm Optimization for Biomedical Applications* (pp. 86-107). CRC Press.
58. Chithrakumar, T., Mathivanan, S. K., Thangamani, M., Balusamy, B., Gite, S., & Deshpande, N. (2024, August). Revolutionizing Agriculture through Cyber Physical Systems: The Role of Robotics in Smart Farming. In *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)* (Vol. 1, pp. 1-6). IEEE.
59. Tiwari, V., Ananthakumaran, S., Shree, M. R., Thangamani, M., Pushpavalli, M., & Patil, S. B. (2024). RETRACTED ARTICLE: Data analysis algorithm for internet of things based on federated learning with optical technology. *Optical and Quantum Electronics*, *56*(4), 572.
60. Sakthivel, M., SivaSubramanian, S., Prasad, G. N. R., & Thangamani, M. (2023). Automated detection of cardiac arrest in human beings using auto encoders. Measurement: Sensors, 27, 100792.
61. CHITHRAKUMAR, T., THANGAMANI, M., KSHIRSAGAR, R. P., & JAGANNADHAM, D. (2023). MICROCLIMATE PREDICTION USING INTERNET OF THINGS (IOT) BASED ENSEMBLE MODEL. *Journal of Environmental Protection and Ecology*, *24*(2), 622-631.
62. Vasista, T. G. K. (2017). Towards innovative methods of construction cost management and control. *Civ Eng Urban Plan: Int J*, *4*, 15-24.
63. Hsu, H. Y., Hwang, M. H., & Chiu, Y. S. P. (2021). Development of a strategic framework for sustainable supply chain management. *AIMS Environmental Science*, (6).
64. Venkateswarlu, M., & Vasista, T. G. (2023). Extraction, Transformation and Loading Process in the Cloud computing scenario. *International Journal of Engineering Applied Sciences and Technology*, *8*, 232-236.
65. Sagar, M., & Vanmathi, C. (2022, August). Network Cluster Reliability with Enhanced Security and Privacy of IoT Data for Anomaly Detection Using a Deep Learning Model. In *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)* (pp. 1670-1677). IEEE.
66. Sagar, M., & Vanmathi, C. (2024). A Comprehensive Review on Deep Learning Techniques on Cyber Attacks on Cyber Physical Systems. *SN Computer Science*, *5*(7), 891.
67. Sagar, M., & Vanmathi, C. (2024). Hybrid intelligent technique for intrusion detection in cyber physical systems with improved feature set. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-17.
68. Vanmathi, C., Mangayarkarasi, R., Prabhavathy, P., Hemalatha, S., & Sagar, M. (2023). A Study of Human

Interaction Emotional Intelligence in Healthcare Applications. In *Multidisciplinary Applications of Deep Learning-Based Artificial Emotional Intelligence* (pp. 151-165). IGI Global.

69. Kumar, N. A., & Kumar, J. (2009). *A Study on Measurement and Classification of TwitterAccounts*.
70. Senthilkumar, S., Haidari, M., Devi, G., Britto, A. S. F., Gorthi, R., & Sivaramkrishnan, M. (2022, October). Wireless bidirectional power transfer for E-vehicle charging system. In *2022 International Conference on Edge Computing and Applications (ICECAA)* (pp. 705-710). IEEE.
71. Firos, A., Prakash, N., Gorthi, R., Soni, M., Kumar, S., & Balaraju, V. (2023, February). Fault detection in power transmission lines using AI model. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.
72. Gorthi, R. S., Babu, K. G., & Prasad, D. S. S. (2014). Simulink model for cost-effective analysis of hybrid system. *International Journal of Modern Engineering Research (IJMER)*, *4*(2).
73. Rao, P. R., & Sucharita, D. V. (2019). A framework to automate cloud based service attacks detection and prevention. *International Journal of Advanced Computer Science and Applications*, *10*(2), 241-250.
74. Rao, P. R., Sridhar, S. V., & RamaKrishna, V. (2013). An Optimistic Approach for Query Construction and Execution in Cloud Computing Environment. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(5).
75. Rao, P. R., & Sucharita, V. (2020). A secure cloud service deployment framework for DevOps. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 874-885.
76. Selvan, M. A., & Amali, S. M. J. (2024). RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE.