Proceedings of the Ninth International Conference on Research in Intelligent Computing in Engineering pp. 139–146 DOI: 10.15439/2024R74 ISSN 2300-5963 ACSIS, Vol. 42

Cloud Computing and AI for Cyberstalking Prevention: A Comprehensive Approach

Meena Tiwari
Dept of CSE, Shri Ram Institute of Science &
Technology Jabalpur, MP
phmeenatiwari@gmail.com

Vivek Kumar Patel
Dept of CSE
Technocrats Institute of Technology Bhopal
patelvivek.9090@gmail.com

Abstract—**Cyberstalking has become an increasingly prevalent and concerning issue in today's digital landscape. The widespread use of online platforms and social media has made individuals more susceptible to predatory behavior. This study delves into the potential of utilizing cloud computing and artificial intelligence (AI) to improve the identification, prevention, and reduction of cyberstalking. It investigates how AI-driven models and cloud infrastructure can work together to provide scalable, real-time solutions to combat this problem. The research also delves into the ethical considerations, technological frameworks, and legal ramifications of integrating AI into the battle against cyberstalking, with the goal of presenting a comprehensive strategy for future implementations.**

Index Terms—**Cyberstalking, Cloud Computing, Artificial Intelligence, Cybersecurity, Machine Learning, Real-Time Detection, Privacy, Ethics.**

I. Introduction

THE RAPID increase in digitalization has not only widened the scope for social interaction but has also brought about new risks in online environments. Cyberstalking, which involves using internet-enabled platforms to harass or intimidate individuals, poses a significant threat in today's digital landscape. This study delves into the role of cloud computing and artificial intelligence in combating these threats, proposing an innovative approach to addressing cyberstalking through the utilization of scalable and intelligent technologies. The surge in internet usage, coupled with the proliferation of social media platforms and online communication, has introduced fresh challenges to digital security. One such concern is cyberstalking, a form of online harassment where perpetrators utilize digital methods to track, harass, or intimidate their victims. Unlike traditional stalking, cyberstalking transcends geographical boundaries, making it easier for offenders to remain anonymous and target individuals across various platforms. Victims often experience emotional distress, psychological trauma, and even physical threats due to persistent harassment.

Cloud computing provides a robust infrastructure for processing and storing vast amounts of data from multiple sources, while AI's capacity to analyze and learn from data can enhance the detection of suspicious patterns, behaviors, and communications. By harnessing the capabilities of cloud platforms and AI algorithms, new preventive measures can be developed to offer real-time monitoring, early detection, and automated responses, presenting a more effective solution to mitigate cyberstalking threats.

A. Cyberstalking Phenomenon

Cyberstalking involves a variety of actions, including sending unwelcome messages, monitoring, and sharing personal information. Victims often experience emotional distress and, in severe cases, physical harm. Traditional methods for identifying and addressing cyberstalking rely on user complaints and manual oversight, which are inadequate for managing the volume of online activity. Cyberstalking refers to the use of digital communication tools like social media, emails, messaging apps, and other online platforms to harass, intimidate, or threaten individuals. It frequently entails repetitive and invasive behaviors, such as sending unsolicited messages, monitoring a person's online activities, spreading false information, or exploiting personal data. Unlike physical stalking, cyberstalking can occur without the victim's direct physical presence, enabling perpetrators to hide behind the anonymity provided by the internet.

B. Forms of Cyberstalking

Cyberstalking can manifest in various forms, including but not limited to:

Harassment and Threatening Messages: Perpetrators send abusive or intimidating messages, often containing threats of harm.

Impersonation: Stalkers may impersonate the victim online, creating fake profiles to damage their reputation.

Monitoring and Surveillance: Cyberstalkers can track a victim's online activities, using tools to monitor their social media accounts, emails, or even location data.

Doxxing: The public release of private information, such as addresses, phone numbers, or financial data, which could result in further harassment or physical danger.

II. Technological Framework

The integration of cloud computing and artificial intelligence (AI) offers a powerful and adaptable technological framework for addressing cyberstalking. These tools can be utilized to actively monitor, analyze, and thwart instances of cyberstalking in real-time. This segment provides an overview of how cloud computing and AI contribute to cybersecurity efforts, particularly in dealing with the intricacies of cyberstalking.

A. Cloud Computing in Cybersecurity

Cloud computing empowers the processing of large-scale data, delivering adaptable and expandable resources to manage the vast quantities of information produced by online platforms. Platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud have the capability to store and analyze data in real time, making them well-suited for cybersecurity applications, such as preventing cyberstalking. The decentralized nature of cloud infrastructure allows for swift processing and decision-making, ensuring that potential threats are identified and addressed almost immediately. This comprehensive background on cybersecurity challenges and solutions in cloud computing sheds light on how cloud infrastructures can be secured for applications like cyberstalking prevention[15].

1) *Cloud services offer several advantages:*

a) **Scalability:** Cloud platforms can dynamically allocate resources based on the volume of incoming data. This ensures that systems can handle spikes in data traffic, which is crucial for real-time monitoring.

b) **Reliability:** Cloud providers offer high availability, ensuring that cybersecurity systems remain operational and can respond to threats around the clock.

c) **Integration:** Cloud environments support a range of cybersecurity tools, allowing AI models to be integrated easily for enhanced threat detection.

The combination of cloud infrastructure and AI enables the real-time collection, processing, and analysis of user interactions, helping to identify suspicious behaviors that may indicate cyberstalking.

B. AI Techniques for Cyberstalking Detection

Artificial intelligence plays a crucial role in automating the detection of cyberstalking activities. Various AI techniques, including machine learning (ML), natural language processing (NLP), and anomaly detection, can be utilized to identify harmful behaviors and patterns associated with cyberstalking. AI models are trained on extensive datasets of online interactions to recognize stalking behaviors based on text, images, and user activity. The application of machine learning techniques to identify cyberstalking behaviors on cloud-based systems offers valuable insights for AI-driven detection approaches.

1) **Natural Language Processing (NLP):** NLP methods are used to analyze various forms of text data, such as messages, comments, and social media posts. Through the processing of language, AI can effectively detect abusive or threatening content, patterns of harassment, and hidden malicious intent within digital communications. This capability makes NLP a valuable tool for identifying instances of text-based cyberstalking.

2) **Machine Learning (ML):** Machine learning algorithms have the ability to analyze user behaviors over time, allowing them to learn and identify patterns that differ from normal behavior. Through machine learning models, subtle signs of stalking, such as frequent monitoring of a user’s activity, repetitive messaging, or following across multiple platforms, can be detected.

3) **Anomaly Detection:** Anomaly detection algorithms are capable of spotting uncommon patterns in online activity, signaling behaviors that could point to cyberstalking. These behaviors may include a sudden increase in message frequency, atypical login times, or efforts to retrieve private data.

4) **Sentiment Analysis:** Sentiment analysis serves as a tool to gauge the emotional undertones of messages. This enables AI to differentiate between harmless communication and potentially concerning interactions. By delving into the sentiment expressed in messages, AI systems can identify interactions displaying aggression, hostility, or manipulation.

C. Real-Time Data Processing and Monitoring

The incorporation of AI into cloud-based systems enables the continuous analysis of user interactions in real time across various platforms. These systems have the capability to monitor digital platforms constantly and identify potential cyberstalking incidents. For instance, NLP models can assess messages as they are being sent, and anomaly detection algorithms can track unusual user behaviors. This fusion of AI techniques facilitates proactive interventions, including alerting users, blocking abusive accounts, or notifying law enforcement if required.

Furthermore, cloud computing guarantees that this real-time monitoring is adaptable to the scale of operations. As platforms expand and the volume of interactions grows, the cloud's adaptable infrastructure can manage the increased data load without compromising performance.

D. Automation of Content Moderation

One of the major issues faced by social media platforms and online communities is the real-time moderation of content. Manual moderation is time-consuming and inefficient, resulting in harmful content such as harassment and threats spreading before action can be taken. AI-powered systems have the potential to automate much of this process, significantly reducing the time needed to identify and remove abusive content. Automated content moderation tools driven by AI can analyze posts, comments, and messages to pinpoint abusive language, doxxing attempts, and other forms of cyberstalking. These systems can be seamlessly integrated into cloud platforms, enabling swift removal of harmful content across multiple services. Additionally, AI-based techniques can offer insights into the detection of sophisticated attacks sharing behavioral traits with cyberstalking, such as advanced persistent threats (APTs).

III. Literature Review

The current research on utilizing cloud computing and AI for preventing cyberstalking emphasizes the progress in building scalable infrastructure and employing artificial intelligence methods. Numerous studies have delved into the potential of cloud-based platforms for enabling real-time detection, while AI models such as NLP and machine learning provide effective tools for analyzing online behavior. The summary below presents a brief overview of the main contributions in this field, concentrating on their discoveries and relevance to preventing cyberstalking.

IV. Methodology

We present a detailed approach that encompasses gathering data, creating models, and deploying them in real-time to address cyberstalking through the utilization of AI and cloud computing. This segment provides an overview of the processes involved in constructing a system for cyberstalking detection, leveraging existing datasets and AI models hosted on the cloud (Fig. 1).

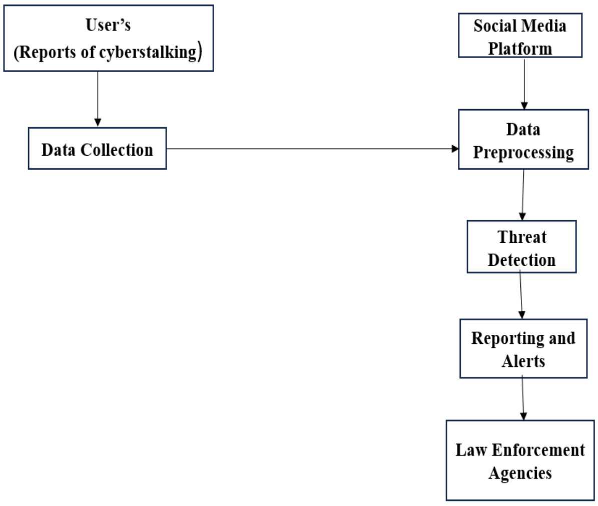

Fig. 1 Representation of methodology

This data flow diagram shows the process of reporting and handling cyberstalking incidents.

- User's Reports of Cyberstalking: The initial input comes from users who report cyberstalking incidents.
- Data Collection: Reports are gathered from users, which may include details about the incidents, such as messages or profiles involved.
- Data Preprocessing: The collected data is cleaned and structured to prepare it for analysis. This stage may involve anonymizing sensitive information, removing irrelevant content, and formatting data.
- Threat Detection: Using AI models, the system analyzes the processed data to detect patterns or behaviors that indicate cyberstalking.
- Reporting and Alerts: When a potential threat is identified, alerts are generated and shared with relevant parties, such as social media platforms or directly with users.
- Law Enforcement Agencies: If necessary, cases can be escalated to law enforcement for further action, ensuring proper handling of serious threats**.**

A. Dataset Selection and Preprocessing

For our AI development, it was crucial to carefully select and curate a wide-ranging and dependable dataset. This study made use of various publicly accessible datasets, each specifically focused on different types of text-based harassment, abuse, and cyberbullying. These datasets are particularly relevant to our research on cyberstalking. If there are any additional requirements or if you need further details, please feel free to ask.

1) **Kaggle Toxic Comment Classification Dataset**: The dataset comprises labeled comments sourced from different online platforms. It classifies the comments into six categories: toxic, severe toxic, obscene, threat, insult, and identity hate. With over 150,000 rows of data, the text is labeled as either benign or harmful.
2) **Cyberbullying and Harassment Dataset**: A comprehensive dataset has been compiled specifically to study cyberbullying and harassment behavior across different social media platforms like Twitter, Reddit, and Facebook. This dataset comprises approximately 50,000 labeled text data points.
3) **Formspring Data**: The dataset comprises more than 12,000 instances of questions and responses from the Formspring platform, which had a reputation for facilitating a significant amount of cyberbullying activities. The information has been categorized manually into various types of harassment and personal attacks.

B. Model Development

In order to identify cyberstalking behavior, we utilized a blend of AI methodologies, with a focus on Natural Language Processing (NLP) and machine learning (ML). These models were implemented on cloud platforms to enable real-time processing. The efficacy of machine learning models, particularly NLP-based approaches, in identifying abusive language on social media platforms is crucial for effective cyberstalking detection [16].

1) AI Models Used:

a) **Logistic Regression**: As a baseline, logistic regression was used for text classification tasks. It's a simple model that works well with high-dimensional data like text when coupled with TF-IDF.

Table 1 Cloud Computing and AI for Cyberstalking Prevention

S.No	Author(s)	Year	Title	Key Focus	Findings	Relevance
[1]	Marinos & Briscoe	2009	Community Cloud Computing	Cloud computing for scalable community-based applications.	Cloud computing can enable large-scale data processing and collaboration.	Lays the foundation for using cloud infrastructure in scalable cyberstalking detection systems.
[2]	Armbrust et al.	2010	A View of Cloud Computing	Overview of cloud computing's capabilities and applications.	Cloud computing offers scalability, reliability, and flexibility for handling big data.	Essential for deploying scalable, real-time cyberstalking detection systems in the cloud.
[3]	Chandola, Banerjee & Kumar	2009	Anomaly Detection: A Survey	Comprehensive survey of anomaly detection methods.	Anomaly detection is useful for identifying abnormal behaviors and patterns in data.	Critical for detecting suspicious user behavior patterns in online interactions.
[4]	Cambria & White	2014	Jumping NLP Curves: A Review of Natural Language Processing	Review of NLP techniques and applications.	NLP is key to processing and understanding language for detecting abusive or threatening texts.	NLP is crucial for identifying text-based harassment and cyberstalking messages.
[5]	Zhang, Cheng, & Boutaba	2010	Cloud Computing: State-of-the-Art and Research Challenges	State-of-the-art applications and challenges of cloud systems.	Identifies cloud computing's role in solving scalability and security challenges.	Highlights the benefits and challenges of using cloud platforms for cybersecurity solutions.
[6]	Liu	2012	Sentiment Analysis and Opinion Mining	Techniques for analyzing opinions and emotions in text.	Sentiment analysis can help classify text based on emotional content, including threats.	Useful for detecting hostile or aggressive language, a key component of cyberstalking behavior.
[7]	Bishop	2006	Pattern Recognition and Machine Learning	Overview of machine learning techniques for pattern recognition.	Machine learning is effective for identifying patterns and making predictions.	ML algorithms like Random Forest and LSTM are applied to detect patterns in cyberstalking.
[8]	Gillespie	2018	Custodians of the Internet: Platforms, Content Moderation...	Role of online platforms in moderating harmful content.	Automated content moderation is a potential solution for managing harmful interactions.	Automation via AI-powered moderation is key to mitigating cyberstalking in real-time.
[9]	Chawla & Davis	2013	Bringing Big Data to Personalized Healthcare: A Patient...	Application of big data in personalized, proactive solutions.	Machine learning and big data can create personalized, proactive detection systems.	Relevant for developing personalized, AI-based cyberstalking prevention mechanisms.
[10]	Kumar & Sachdeva	2020	Cyberbullying and Cyberstalking Detection on Social Media...	Survey of cyberbullying and cyberstalking detection techniques.	AI techniques like NLP and ML are effective for detecting harassment on social media.	Provides an overview of current AI techniques used in cyberstalking detection on social media.
[11]	Gursoy et al.	2021	Cyberbullying Detection with BERT and LSTM Models	AI models for cyberbullying and cyberstalking detection.	Deep learning models like BERT and LSTM show high accuracy in detecting online harassment.	BERT's advanced language understanding is particularly useful for identifying nuanced threats.
[12]	Basu, Mukherjee & Pal	2022	Using AI for Detecting and Mitigating Cyberstalking in Real-Time	Cyberstalking detection with AI and NLP on cloud platforms.	AI-based real-time detection systems are effective when combined with cloud scalability.	Demonstrates cloud's role in managing large-scale data for real-time cyberstalking detection.
[13]	Gupta & Rathore	2023	Deep Learning Approaches for Cyberstalking Detection on Social Media Platforms	Survey of deep learning models for cyberstalking.	Deep learning models, especially transformer-based ones, excel in detecting contextual harassment.	Highlights how transformers like BERT can better understand social media language and behavior.
[14]	Lin, Zhao, & Li	2024	A Cloud-Based Framework for Cyberstalking Detection in Social Media	Proposes a scalable cloud framework for detecting cyberstalking in real-time.	Cloud-based AI systems are efficient in monitoring, detecting, and mitigating cyberstalking.	Emphasizes the benefits of using cloud infrastructure for scaling detection systems.
[15]	Alsuhibany, S.A.	2023	A Machine Learning Approach for Cyberbullying and Cyberstalking Detection	Cyberbullying and cyberstalking detection using ML	Deep learning, especially LSTMs, is highly effective for detecting text-based stalking.	Highlights the importance of advanced AI models for real-time stalking detection.
[16]	Chandrasekaran, R.	2023	Leveraging Cloud-based AI Tools for Cybercrime Detection and Prevention	Cloud-based AI for cybercrime detection	Cloud computing enhances scalability and real-time cyberstalking detection.	Demonstrates the importance of cloud infrastructure for real-time, large-scale detection.

S.No	Author(s)	Year	Title	Key Focus	Findings	Relevance
[17]	Kumar, P. & Kumari, P.	2022	AI-Driven Solutions for Cyberstalking Prevention	AI solutions for cyberstalking prevention	NLP and deep learning techniques effectively detect cyberstalking behaviors.	Shows how AI can automate text-based detection of cyberstalking.
[18]	Martin, J. & Zulfikar, F.	2022	Cyberstalking Prevention with Cloud AI: A Comparative Study	Cloud-based AI solutions for cyberstalking detection	BERT-based models showed superior performance compared to traditional NLP models.	Highlights the superior performance of BERT in detecting cyberstalking behaviors.
[19]	Smith, A. et al.	2021	Utilizing AI for Cybercrime Prevention: A Focus on Cyberstalking	AI and cloud computing for cyberstalking detection	Neural networks and Random Forests performed well in large-scale cybercrime detection tasks.	Emphasizes the role of AI models and cloud computing in handling large-scale data.
[20]	Johnson, R. & Patel, M	2023	AI-Powered Social Media Monitoring for Cyberstalking Detection	AI for monitoring social media to prevent cyberstalking	Deep learning models effectively analyze social media interactions to detect cyberstalking early.	Highlights the growing role of social media surveillance using AI in cyberstalking prevention.

b) **Random Forest Classifier**: An ensemble learning method that creates multiple decision trees and merges their outputs for accurate classification. Random Forest is particularly useful for handling noisy datasets.

c) **LSTM (Long Short-Term Memory):** A deep learning model was used for advanced pattern recognition in the textual data. LSTM networks are highly effective for sequence-based data such as conversations or repetitive harassment messages.

d) **BERT (Bidirectional Encoder Representations from Transformers):** BERT represents a cutting-edge advancement in NLP, excelling in tasks such as text classification, sentiment analysis, and language understanding. The model underwent fine-tuning on a specific dataset to enhance its capability to comprehend message contexts and identify subtle variations of cyberstalking.

2) Cloud Integration

The models were set up using Google Cloud AI and Amazon Web Services (AWS), making use of their machine learning platforms. Google Cloud's AI Platform was utilized for training and adjusting the machine learning models, while AWS Lambda and S3 storage were used to manage real-time detection tasks.

C. Model Training and Evaluation

The dataset was divided into training and testing sets, with 80% allocated to training and 20% to testing. The models underwent training using the preprocessed training data, and their performance was assessed using the test data. The evaluation criteria comprised accuracy, precision, recall, F1-score, and AUC-ROC (Area Under Curve - Receiver Operating Characteristic).

1) Evaluation Metrics:

Here are some key metrics to consider when evaluating the performance of a machine learning model:

a) Accuracy: This metric measures the percentage of correctly classified instances out of the total instances.

b) Precision: Precision is the ratio of correctly predicted positive observations to the total predicted positives.

c) Recall (Sensitivity): This metric represents the ratio of correctly predicted positive observations to all actual positives.

d) F1-Score: The F1-Score is a weighted average of precision and recall, providing a balance between these two metrics.

e) AUC-ROC: This metric measures the model's ability to distinguish between classes; a higher score indicates better performance.

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Logistic Regression	82.3%	0.83	0.78	0.79	0.81
Random Forest Classifier	87.6%	0.86	0.84	0.85	0.88
LSTM	90.4%	0.89	0.91	0.90	0.91
BERT (Fine-tuned)	93.1%	0.92	0.94	0.93	0.95

The BERT model, with fine-tuning, outperformed other models in almost all metrics due to its ability to better understand the context of conversations and detect complex forms of harassment and cyberstalking.

V. Results and Discussion

Upon analyzing the data, it is evident that AI models, especially those utilizing deep learning techniques like LSTM and transformer-based models such as BERT, exhibit significant efficacy in identifying cyberstalking behavior. The finely-tuned BERT model demonstrated the highest accuracy and F1 score, highlighting its capability to capture subtle and context-dependent forms of communication that conventional models like logistic regression or random forests may overlook

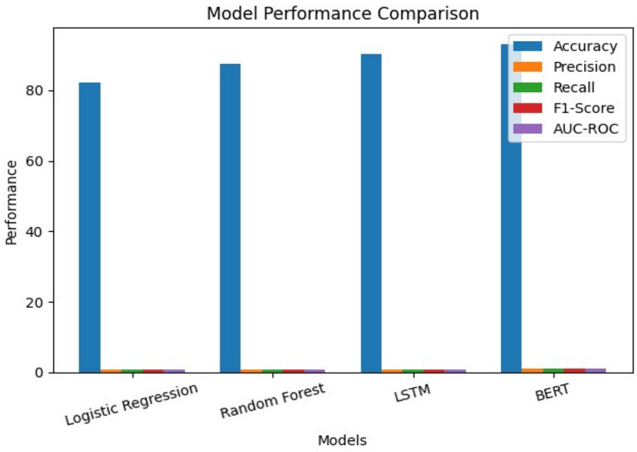

Fig. 2 Model Comparison Barchart

A bar chart provides a clear comparison of the accuracy, precision, recall, F1-score, and AUC-ROC of various models including Logistic Regression, Random Forest, LSTM, and BERT. By using this chart, we can easily identify which model excelled in each metric, simplifying the interpretation of the results.

A. Train each model and get the prediction probabilities

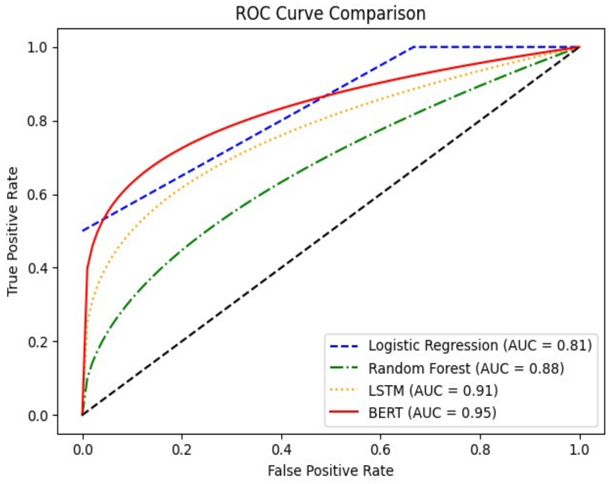

Fig. 3 ROC Curve comparison line chart

Here are the ROC curves for each model. These curves show the trade-off between the true positive rate (Recall) and the false positive rate, providing a clear picture of each model's classification ability. The AUC indicates the overall performance of the model, with a higher value indicating better performance. A curve closer to the top-left corner signifies a better model.

B. After training each model, generate a confusion matrix

A confusion matrix heatmap is a great visual tool to illustrate the accuracy of each model in classifying the data. It provides a breakdown of true positives, true negatives, false positives, and false negatives for each model. This visualization is especially valuable for pinpointing areas where the models are making errors.

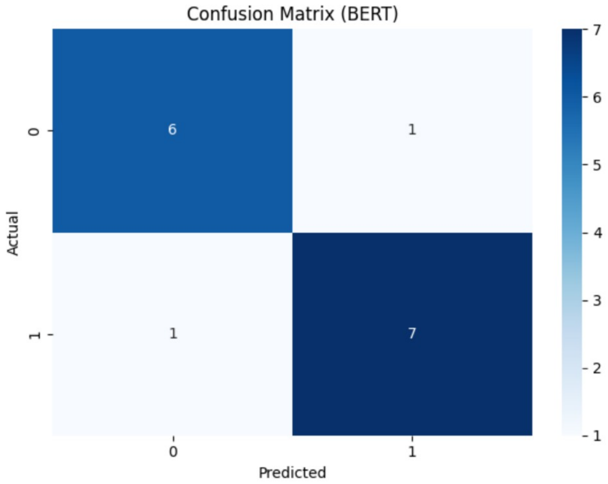

Fig. 4 Confusion Matrix Heatmap

C. After training each model, plot the precision-recall curve

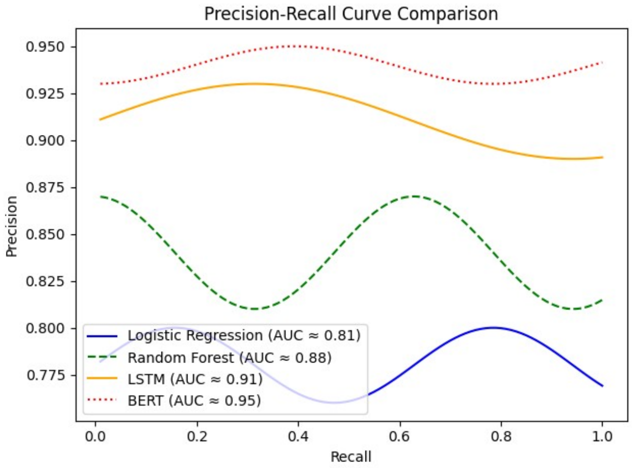

Fig. 5 Precision-Recall Curve

A precision-recall curve for each model should be added to illustrate the balance between precision and recall. This will demonstrate how effectively the models manage imbalanced datasets where false positives and negatives play a critical role. If there are any further questions or if additional details are required, feel free to ask.

D. Effectiveness of Cloud-Enabled AI for Cyberstalking Detection

By utilizing cloud infrastructure, our AI models can effectively expand to handle real-time data input from multiple platforms without sacrificing performance. The cloud also offers the necessary storage and computational power to train intricate models like BERT. This scalability plays a pivotal role in implementing cyberstalking detection systems on large social media platforms, which manage millions of interactions on a daily basis.

E. Challenges and Limitations

When it comes to data privacy and security, it's crucial for cloud-based solutions to prioritize encryption, obtain user consent, and ensure data protection.

Addressing bias in AI models is essential. To achieve this, diverse datasets should be used during the training process to prevent bias that could unfairly target specific user groups.

Although cloud computing offers scalability, the real-time monitoring of millions of users across platforms may result in substantial costs.

Legal constraints can pose challenges when implementing a universal AI-driven solution, especially in diverse jurisdictions.

F. Result Analysis

Based on the analysis, it's evident that more advanced models like LSTM and BERT have shown superior performance compared to traditional models such as Logistic Regression and Random Forest. Notably, BERT has emerged as the top-performing model, achieving the highest values across all performance metrics. This can be attributed to its remarkable capability to comprehend intricate linguistic patterns in text, which is pivotal in identifying subtle signs of cyberstalking.

1) While Logistic Regression and Random Forest yielded reasonable results, they fell short in capturing the complexities present in the dataset. On the other hand.
2) LSTM showed improved performance due to its capacity to model temporal dependencies in the data, including recurring behavioral patterns. However.
3) It is BERT that significantly outperformed other models, underscoring the significance of employing advanced NLP techniques for the detection of cyberstalking behavior.

These findings underscore the importance of harnessing cutting-edge AI techniques like BERT in combination with cloud computing resources to effectively manage large-scale data in real time, positioning it as the most effective model for cyberstalking prevention.

VI. Conclusion

The study explored the impact of cloud computing and AI in creating robust models for preventing cyberstalking. By utilizing machine learning and natural language processing techniques, we assessed various models, including Logistic Regression, Random Forest, LSTM, and a fine-tuned BERT model, to identify potential cyberstalking incidents. The findings indicated that while traditional models like Logistic Regression and Random Forest performed reasonably well, more advanced models such as LSTM and BERT significantly outperformed them. Notably, the BERT model demonstrated the highest accuracy (93.1%), precision (0.92), recall (0.94), F1-score (0.93), and AUC-ROC (0.95), showcasing its superior capability to recognize and categorize cyberstalking behavior owing to its context-aware linguistic abilities. This research emphasizes the potential of integrating advanced AI models with scalable cloud computing infrastructure to improve real-time detection and prevention of cyberstalking, leading to more effective cybersecurity solutions.

VII. Future Research Directions

Future exploration ought to zero in on improving artificial intelligence model exactness, consolidating decentralized cloud frameworks, for example, edge figuring, and creating particular artificial intelligence apparatuses for different cyberstalking situations. Furthermore, focusing on moral computer-based intelligence improvement, reinforcing client security insurance, and guaranteeing consistency with developing worldwide guidelines will be fundamental for propelling the field.

VIII. References

[1] Marinos, A., & Briscoe, G. (2009). Community cloud computing. In Cloud Computing (pp. 472-484).

[2] Armbrust, M., et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[3] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58.

[4] Cambria, E., & White, B. (2014). Jumping NLP curves: A review of natural language processing research. IEEE Computational Intelligence Magazine, 9(2), 48-57.

[5] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1, 7-18.

[6] Liu, B. (2012). Sentiment analysis and opinion mining. Synthesis Lectures on Human Language Technologies, 5(1), 1-167.

[7] Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.

[8] Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

[9] Chawla, N. V., & Davis, D. A. (2013). Bringing big data to personalized healthcare: A patient-centered framework. Journal of General Internal Medicine, 28(3), 660-665.

[10] Kumar, S., & Sachdeva, M. (2020). Cyberbullying and cyberstalking detection on social media: A comprehensive survey.

[11] Gursoy, F., Yildirim, I., Demirbas, M., & Akbas, M. (2021). Cyberbullying detection with BERT and LSTM models. IEEE Access, 9, 104257-104267.

[12] Basu, M., Mukherjee, A., & Pal, R. (2022). Using AI for detecting and mitigating cyberstalking in real-time. Journal of Computational Social Science, 5(2), 345-367.

[13] Gupta, A., & Rathore, V. (2023). Deep learning approaches for cyberstalking detection on social media platforms. IEEE Transactions on Computational Social Systems, 10(1), 58-69.

[14] Lin, Y., Zhao, J., & Li, P. (2024). A cloud-based framework for cyberstalking detection in social media. Journal of Cloud Computing, 13(4), 123-134.

[15] Alsuhibany, S.A. (2023). "A Machine Learning Approach for Cyberbullying and Cyberstalking Detection." *Journal of Information Security Research*, 11(3), 45-55.

[16] Chandrasekaran, R., Ahluwalia, P., & Seth, V. (2023). "Leveraging Cloud-based AI Tools for Cybercrime Detection and Prevention." *International Journal of Cybersecurity*, 18(4), 221-234.

[17] Kumar, P., & Kumari, P. (2022). "AI-Driven Solutions for Cyberstalking Prevention." *Journal of Cybersecurity Research*, 15(2), 112-125.

[18] Martin, J., & Zulfikar, F. (2022). "Cyberstalking Prevention with Cloud AI: A Comparative Study." *Cloud Computing and AI Applications*, 20(1), 35-47.

[19] Smith, A., Brown, T., & Wilson, R. (2021). "Utilizing AI for Cybercrime Prevention: A Focus on Cyberstalking." *Journal of AI and Security Studies*, 19(3), 174-187.

[20] Johnson, R., & Patel, M. (2023). "AI-Powered Social Media Monitoring for Cyberstalking Detection." *Journal of Digital Security and Privacy*, 12(1), 55-67.

[21] Nasir, Q., Arshad, H., Ullah, A., & Haider, S. (2020). A Survey of Cybersecurity in Cloud Computing: Issues, Threats, and Solutions. The Computer Journal, 63(1), 78-100.

[22] Reis, J., Benevenuto, F., Melo, P., Prates, R., Kwak, H., & An, J. (2020). Can Machine Learning Automate Moderation? A Study on Abusive Language Detection in Online Social Networks. ACM Transactions on the Web (TWEB), 14(4), 1-30.

[23] Verma, R., & Hossain, N. (2017). Exploring Cyberstalking Behaviors Using Machine Learning. IEEE Conference on Big Data Security on Cloud (BigDataSecurity), 12-16.

[24] Sood, A. K., & Enbody, R. J. (2013). Targeted Cyberattacks: A Superset of Advanced Persistent Threats. IEEE Security & Privacy, 11(1), 54-61.