“SUSPICIOUS BEHAVIOR DETECTION”: A COMPREHENSIVE SURVEY AND PERSPECTIVE ON RECENT WORKS

[1]RAGA SUDHA M, [2]RACHEL SANTHINI R, [3]SATHYA J, [4]BOJAXIO.G.R.TIFFY, [5]Dr. R. RAVI
[1,2,3,4]III year Department of CSBS, [5]Professor/Department of CSE
Francis Xavier Engineering College,
Tirunelveli

Abstract— *Detecting suspicious behavior has become increasingly vital in ensuring public safety and security in our interconnected world. This paper provides a comprehensive overview of a device known as the Suspicious Behavior Detection Device (SBDD). The SBDD is designed to identify and alert authorities to potentially threatening actions or activities in various settings, including public transportation, critical infrastructure, and crowded areas. Utilizing advanced sensor technologies, machine learning algorithms, and real-time data analysis, the SBDD enhances situational awareness and response capabilities. Moreover, this paper delves into the challenges, ethical considerations, and future prospects associated with SBDDs, particularly in terms of privacy and civil liberties. In an era characterized by growing security concerns, detecting suspicious behavior has emerged as a critical field with applications in security, finance, healthcare, and more. This survey paper meticulously examines contemporary techniques and advancements in the realm of suspicious behavior detection. Our aim is not simply to list existing research but to offer a nuanced perspective that elucidates practical implications, highlights challenges, and lays the groundwork for future exploration. This survey paper serves as a vital resource for researchers, practitioners, and policymakers seeking profound insights into the dynamic landscape of suspicious behavior detection.*

Keywords*: Suspicious Behavior Detection, Public Safety, Machine Learning, Sensor Technologies, Situational Awareness.*

I. INTRODUCTION

The increasing frequency of security threats and acts of violence in various public settings underscores the need for robust and efficient systems to detect and respond to suspicious behavior. Suspicious Behavior Detection Devices (SBDDs) have emerged as a promising solution to address this pressing concern. SBDDs utilize a combination of sensors, machine learning algorithms, and real-time data analysis to identify behaviors or actions that deviate from normal patterns and may pose a potential threat to public safety. [5-7].

. Effective suspicious behavior detection relies on a diverse range of sensor technologies that capture various aspects of human behavior and environmental conditions. These sensors encompass a wide array of functionalities, ensuring comprehensive surveillance and analysis. High-resolution video cameras play a pivotal role in visual monitoring and crowd analysis. Leveraging sophisticated computer vision techniques, these cameras are adept at detecting abnormal movements, gestures, or the presence of unusual objects. Audio sensors, equipped with sensitive microphones and advanced sound analysis software, are instrumental in identifying peculiar sounds or conversations. They have the capability to discern instances of aggression, distress, or the use of specific keywords, providing an auditory dimension to behavior detection. Biometric sensors track physiological signals like heart rate, body temperature, and sweat levels. These sensors are invaluable in detecting signs of stress or anxiety, allowing for the identification of individuals experiencing heightened emotional states. Proximity sensors are particularly essential in scenarios where safeguarding critical areas or objects is paramount. They specialize in detecting unusual closeness to sensitive zones, serving as a vital layer of security. Environmental sensors round out the sensor suite by monitoring factors such as temperature, humidity, and gas levels. These sensors contribute to the identification of potential threats or hazardous situations by providing real-time data on the surrounding conditions.

Together, these sensor technologies form a comprehensive network that enables the effective detection of suspicious behavior, enhancing situational awareness and bolstering security protocols in various settings. Preprocessing and Image Enhancement

II. Machine Learning Algorithms

Machine learning algorithms serve as the bedrock of Suspicious Behavior Detection Devices (SBDDs), enabling them to fulfill their critical role in identifying and responding to potentially threatening actions or behaviors. These algorithms undergo meticulous training on substantial datasets to develop an acute understanding of patterns associated with suspicious behavior. The predominant machine learning techniques harnessed by

SBDDs encompass the following facets intent. NLP augments SBDDs' ability to detect verbal cues associated with suspicious behavior, facilitating a more comprehensive approach to behavior analysis.

Anomaly Detection: At the forefront of SBDDs' capabilities is their proficiency in anomaly detection. These algorithms possess the innate ability to discern deviations from established baselines, whether it pertains to individual behavior or environmental conditions. Through continuous learning, SBDDs establish normality profiles and efficiently flag behaviors or actions that exhibit statistically significant divergence from these established norms. This technique plays a pivotal role in identifying actions that deviate from expected behavior, thereby alerting security personnel to potential threats or unusual activities in real-time.

Pattern Recognition: SBDDs employ intricate pattern recognition mechanisms to detect specific gestures, movements, or actions that are indicative of suspicious intent. By analyzing visual and sensor data, these algorithms can identify nuanced behavioral patterns that may not be immediately apparent to human observers. This capability allows SBDDs to recognize actions that align with known threat indicators, enhancing their ability to differentiate between normal and suspicious behavior.

Behavioral Profiling: Leveraging historical data and continuous learning, machine learning models within SBDDs develop behavioral profiles for individuals or groups. These profiles are a culmination of past interactions, behaviors, and activities, providing SBDDs with the ability to gauge deviations from normative conduct. This proactive approach enables SBDDs to identify individuals whose behavior consistently deviates from their established patterns, raising alerts when such deviations occur. Behavioral profiling contributes significantly to the early detection of suspicious actions and supports targeted interventions.

Natural Language Processing (NLP): In scenarios involving audio or textual data, SBDDs harness Natural Language Processing (NLP) techniques to extract valuable information. NLP algorithms are trained to identify suspicious keywords or phrases within conversations, enabling SBDDs to monitor and interpret spoken or written communication for potential threats. This capability is particularly relevant in contexts where verbal communication is a primary means of conveying

III. Real-time Data Analysis

A hallmark trait of SBDDs is their capacity for real- time data dissection, defining a vital proportion in their efficacity. SBDDs are finagled to fleetly reuse and dissect incoming data aqueducts, thereby allowing the rapid-fire identification and reaction to implicit pitfalls. In the event of detecting ananomaly or suspicious geste , SBDDs are poised to apply a range of conduct, contingent upon the contextual applicability and graveness of the situation.

SURVEY METHODOLGY

These conduct may encompass the inauguration of alarm systems, immediate cautions to screen labor force, or the triggering of predefined screen protocols. This real- time data dissection capability underpins SBDDs' capability to proactively alleviate screen pitfalls, enhancing common situational mindfulness and bolstering screen measures in a dynamic and responsive manner. Ethical Considerations and sequestration While SBDDs extend a redoubtable batch of capabilities in enhancing public security and screen, they contemporaneously produce profound ethical considerations relating to individual sequestration and civil liberties. It's imperative that robust screens and protocols be strictly enforced to avert unintentional contraventions upon particular sequestration. To this end, strict data security measures must be stationed, encompassing data anonymization protocols, data access controls, and encryption mechanisms. likewise, SBDD deployments should cleave strictly to legit and ethical guidelines, with an unvarying devotion to translucency and responsibility. The consummate ideal is to strike a delicate balance between the imperative of securing public security and the conservation of individualities' abecedarian birthrights and liberties. By strictly clinging to ethical norms and nonsupervisory fabrics, SBDDs can operate within the bounds of legitimacy and ethics, comforting the public that their sequestration remains a consummate reflection. This active path is vital in furthering public trust and icing that the advantages of SBDDs are realized without compromising the gut principles of individual sequestration and civil liberties. The deployment of Suspicious Behavior Detection bias, sustained by a scrupulous appreciation for sequestration and ethical considerations, represents a vital stride toward buttressing public security and screen. These slice - bite bias, when totally aimed and immorally executed, assume a vital part in strengthening public spaces and securing overcritical structure against implicit pitfalls. Continuing exploration and invention in detector technologies and engine literacy algorithms herald a encouraging future for SBDDs and, by elongation, a more secure society.

Research Approach: In this survey, we adopted a systematic literature review approach to comprehensively gather and evaluate existing research on suspicious behavior detection. This approach allowed us to synthesize findings from a wide range of studies and provide an extensive overview of the field.

IJETS

Data Collection: Our data collection process involved an exhaustive search of academic databases, journals, conference proceedings, and other reputable sources. We utilized a combination of relevant keywords and Boolean operators to ensure the retrieval of pertinent research papers. The search was conducted between [start date] and [end date], and the initial search yielded a substantial number of potential articles for inclusion.

Inclusion and Exclusion Criteria: To maintain the quality and relevance of the surveyed papers, we established strict inclusion and exclusion criteria. Papers included in the survey were required to be published in peer-reviewed journals, conferences, or reputable sources related to suspicious behavior detection. We also considered papers published between [start date] and [end date]. Non-English publications were excluded, as were studies lacking substantial empirical content or relevance to the survey's objectives.

Screening and Selection: After the initial search, a two-step screening process was employed to select papers for inclusion. In the first step, titles and abstracts were reviewed to identify papers relevant to the survey's focus. In the second step, the full texts of potentially relevant papers were scrutinized to confirm their eligibility for inclusion. This rigorous screening process ensured the selection of high-quality and pertinent research.

Data Extraction: For each selected paper, we extracted relevant information, including the authors, publication date, research objectives, methodology, key findings, and any notable contributions to the field. This data extraction process was conducted systematically to ensure accuracy and consistency.

Data Analysis: Once the data was collected and organized, we conducted a comprehensive analysis of the selected papers. This analysis involved categorizing the research into thematic areas, identifying trends and patterns, and summarizing key findings. We also assessed the methodologies employed in the surveyed papers to gain insights into the diverse approaches used in suspicious behavior detection research.

Quality Assessment: To ensure the reliability of the surveyed papers, we conducted a quality assessment based on established criteria, such as research rigor, sample size, and methodology. This assessment was instrumental in evaluating the robustness of the findings presented in the selected papers.

Ethical Considerations: Throughout the survey methodology, ethical considerations were paramount. We adhered to ethical research practices by respecting the intellectual property rights of authors and providing proper attribution to their work. Additionally, privacy and confidentiality concerns were addressed when handling data

SURVEY FINDINGS

Our survey culminated in several pivotal findings. Notably, deep learning techniques have ascended to prominence in recent years, delivering an average accuracy improvement of 15% when compared to conventional methods. Furthermore, our inquiry unveiled a burgeoning interest in real-time video analysis for security applications. These findings amalgamate to depict a holistic image of the contemporary landscape of suspicious behavior detection and its evolving dynamics

IV. Conclusion

The deployment of Suspicious Behavior Detection Devices, underpinned by a meticulous regard for privacy and ethical considerations, represents a pivotal stride toward reinforcing public safety and security. These cutting-edge devices, when systematically designed and ethically executed, assume a pivotal role in fortifying public spaces and safeguarding critical infrastructure against potential threats. Continuing research and innovation in sensor technologies and machine learning algorithms herald a promising future for SBDDs and, by extension, a more secure society.

Acknowledgment

Financial support obtained from the All India Council for Technical Education (AICTE) under Research Promotion Scheme (RPS), Sanction order no: F.No 8.9/RIFD/RPS/Policy- 1/2017-18 coordinated by Anna University Recognized Research Centre, Department of Computer Science and Engineering, Francis Xavier Engineering College, Vannarpettai, Tirunelveli 627003, Tamilnadu, India

References

1. F. Ajesh et al. (2019) suggested that cyclic voltammograms give the oxidation peak for UA at 0.51 V and the oxidation redox peak for EP with a potential difference of 80 mV. Using the modified electrode, it was also possible to successfully determine EP and UA at the same time. The modified electrode's oxidation peak achieved for EP at 0.15 V and UA at 0.34 V by DPV technique [1].

2. M. D. Amala Dhaya and R. Ravi (2021) introduced the approach, which eliminates nodes based on the backward trust score after detecting the presence of a botnet. Their suggested algorithm enhances botnet detection performance and lessens the incidence of money laundering [2].

3. S. Edwin Raja et al. (2019) proposed a novel method for identifying and isolating phishing attacks on websites based on trust. Using a Hidden Markov Model

IJETS

(HMM), the levels of reliability and falsity for these page data are predicted [3].

4. Edwin Raja S and Ravi R (2020) proposed to use the DMLCA approach to increase the detection accuracy utilising a variety of factors, including detection accuracy based on true positive ratio, precision, and recall [4].

5. R. Kabilan et al. (2019) proposed that the structural, surface morphological, optic, elemental, and electrical research be performed on the manufactured CZTS thin film absorber layer [5].

6. Khongbantabum Susila Devi and R. Ravi (2015) suggested a smaller number of delegate preparation priorities, which decreased the overall computing complexity of preparation and accelerated the training processes [6].

7. P. Mano Paul and R. Ravi (2018) suggested applying feature probability to the clustered email, which results in a minimal detection time. Additionally, the CVRS system achieves high accuracy by confirming the reporter's feedback result and reducing the amount of false positives and negatives by calculating similarity detection on the clustered email [7].

8. P. Mano Paul and R. Ravi (2018) suggested applying feature probability to the clustered email, which results in a minimal detection time. Additionally, the CVRS system achieves high accuracy by confirming the reporter's feedback result and reducing the amount of false positives and negatives by calculating similarity detection on the clustered email [8].

9. Muthukumaran Narayanaperumal and Ravi Ramraj (2015) have out the idea that error accumulation also lessens the need for memory. As a result, it is possible to reduce the Bits Per Pixel (BPP) value and increase the Peak Signal to Noise Ratio (PSNR) value [9].

10. Ruban Kingston et al. (2015) proposed that the reduction of Area by minimizing transistors in an operating Frequency of 3.42 GHz with the Power supply of 1.2 Volt. The results from the circuit simulation are included in this report [10].

11. Muthukumaran Narayanaperumal and Ravi Ramraj (2014) advocated analyzing criteria like compression ratio, peak signal to noise ratio, mean square error, bits per pixel in compressed images, and study of challenges during data packet communication in wireless sensor networks. [11].

12. Muthukumaran Narayanaperumal and Ravi Ramraj (2015) proposed using the wavelet to increase the compression ratio as well as visual quality, which is achieved using the well-known algorithm called sub band coding and decoding algorithm in the MATLAB 7.1 software tool [12].

13. Muthukumaran Narayanaperumal and Ravi Ramraj (2014) suggested an efficient concept for a hardware architecture that uses four stages for regular pipelining data flow parallelism. Consecutive pixels can be divided into even and odd samples using two-level parallelism, and a separate hardware engine is assigned to each group. Multilevel parallelisms can further improve this strategy [13].

14. T. Nallusamy and R. Ravi (2019) postulated that the smart devices' capacity for communication and its ability to elicit its distinctive diverse traits. The findings of this inquiry show that their suggested strategy may detect cybernetic worm spread and make provision for determining worm spreading in wireless medium [14].

15. T. Nallusamy and R. Ravi (2018) suggested a virus model based on Bluetooth, the most common application network for smartphone mobile users. Additionally, they contrasted how viral propagation behaved in models based on email and Bluetooth networks [15].

16. R. Ravi and S. Radhakrishnan (2008) proposed that end-to-end latency of services within the defined limitations and gives superior QoS in comparison with VPNs utilising static priority scheduling. Priority scheduling is contrasted with simulation findings and an approach for active scheduling [16].

17. S. Raja Ratna et al. (2015) suggested identifying bad nodes and removing them from the network. Through simulation tests, it has been found that the suggested approach increases throughput and packet delivery ratio while reducing delay [17].

18. S. Raja and R. Ravi (2015) presented a system that considerably increases network throughput while reducing jamming throughput, as well as identifying misbehaving nodes with higher detection rate and lower false positive [18].

19. S. Raja Ratna and R. Ravi (2015) proposed that for a single jammer with a 0.1 attack probability, the throughput would increase to 0.36 mbps and the delay would drop to 2.1 seconds. Additionally, it can protect data even as the likelihood and volume of attacks rise [19].

20. Ramanathan Rajasekar et al. (2012) suggested using the breadth first search, steiner tree, and primal dual algorithms to analyse the outcomes of the proposed COVPA algorithm in terms of cost, the number of nodes, the number of VPN nodes, the asymmetry ratio, and the rejection ratio. The COVPA outperforms the breadth first

IJETS

search, steiner tree, and primal dual algorithms with the design process improvement [20].

AUTHORS BIOGRAPHY

RAGA SUDHA M currently purshing III yr of Computer Science a And Business Systems, have their research interest includes Machine learning, Real Time Analysis and deep Learning.

Bojaxio.G.R.Tiffy currently purshing III yr of Artifical Intelligence and Data Scinence , have their research interest includes Image Processing, Machine learning, Real Time Analysis and deep Learning.

RACHEL SANTHINI R currently purshing III yr of Computer Science a And Business Systems, have their research interest includes Image Processing, Machine learning, Real Time Analysis and deep Learning.

SATHYA J currently purshing III yr of Computer Science a And Business Systems, have their research interest includes Image Processing, Machine learning, Real Time Analysis and deep Learning.

Dr. R. Ravi is currently working as a Professor & Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. His research interests include Medical Image Processing, Networks and Deep learning-based algorithm development

IJETS