iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 14 **Issue:** III **Month of publication:** March 2026

**DOI:** https://doi.org/10.22214/ijraset.2026.78770

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

# Telegram: The New Dark Web for Stealer Logs

Mr. Devendra Bodkhe, Yash Kamath, Mridula Kandalgaonkar, Anisha Karkera
*Artificial Intelligence & Data Science, Thakur College of Engineering & Technology, Mumbai, Maharashtra*

***Abstract:*** ***In a world where data fuels global innovation and identity, its exploitationhas becomeoneofthemostcritical threatsofour time. Cybercriminal activity has rapidly shifted from the Dark Web to platforms like Telegram, where stolen data is traded in the form of stealer logs containing emails, passwords, cookies, and financial details. Existing solutions either focus on large public breaches or lack structured, real-time monitoring of these smaller leaks.In this work, we propose a system that monitors Telegram groups, extracts stealer logs, and preprocesses the data to remove duplicates and normalize key fields. The cleaned data is stored in a searchable database and visualized through a Django-based dashboard, enabling queries by email, username, or domain. Our findings reveal recurring patterns such as password reuse and token leakage. This framework converts unorganized leaks into actionable intelligence and sets the foundation for future work in automation, machine learning–based classification, and real-time alerting.***

***Keywords: Data Breach Monitoring, Dark Web Monitoring, Telegram Cybercrime Leaked Credentials, Identity Theft, Encrypted networks, Breached Records, Link analysis, Monitoring challenges, Cybersecurity.***

## I. INTRODUCTION

In this hyper-connected era, data has become one of the fuels that helps run the global economy. Concurrently, it has been a prime target for malicious attackers. Unauthorized exposure of sensitive data either accidently or through deliberate attacks has beenanincreasingthreat tothe corporate viability, national security and individual privacy. Identity theft occurs when someone unlawfully acquires and uses our sensitive data like name, Social Security number, credit card numbers , login credentials etc. for financial gain or for committing frauds. Identity thieves strive to gather as much information as possible to exploit it, which may involve opening fraudulent credit accounts, applying for loans under false pretenses, making unauthorized purchases, or engaging in other criminal activities. Over time, security threats have evolved. Two decades ago, almost half of all data breaches (45%) were caused by lost or stolen physical devices like laptops or flash drives, while only 10% were attributed to “hacked electronic systems.” Today, breaches are often caused by a variety of malicious actions, from phishing attempts to insider threats. [1] IBM's 2025 Cost of a Data Breach Report highlights that global average cost per data breach has reached $4.44 million. Their analysis of the root causes points to Malicious Insiders accounting for nearly 9% of the breaches. [1]

Once the data is exposed, the compromised information enters a complex underground where it is sold , traded and weaponized . For decades, the prominent arena for such activities were Dark Web Marketplaces.The Dark Web is well known for its anonymity. Its operations are predicated on anonymity-enhancing technologies, most notably The Onion

Router (Tor) which involves encrypting data in multiple layers and passing it through a randomized circuit of nodes.[2] Within this ecosystem, Dark Web marketplaces function similarly to regular E-commerce sites. For building trust in this trustless environment, many marketplaces incorporate features such as vendor reputation, user reviews and ratings. This supports a thriving black market for a wide range of compromised data, including Financial data, personal and corporate data , and Access Credentials and Cyber-Arms.

However, the arena for such illicit activities is going through a paradigm shift. The messaging application Telegram has emerged as a powerful and functionally distinct alternative. Unlike Dark Web which requires specialized software like the Tor browser and a degree of technical knowledge, Telegram is accessible on mainstream mobile and desktop platforms and offers a lower barrier to entry, democratizing access to cybercrime. [3]

Cybercrime operates on Telegram not through centralized marketplaces but through public and private channels, automated bots, and groups.

*1)* Channels broadcast stolen data and data dumps to large audiences.
*2)* Bots automate transactions, handle payments, and deliver stolen files instantly.
*3)* Groups allow threat actors to collaborate, negotiate, and share tactics.

While Telegram's privacy is not as strong as Tor's network-level anonymity, its application-level features such as end-to-end encryption, self-destructing messages, and hidden phone numbers provide enough secrecy for illicit activities. [4]

Moreover, nowadays, the Dark Web and Telegram are not mutually exclusive competitors but are forming a symbiotic relationship.Many criminals use Dark Web forums to establish credibility and then direct customers to Telegram for faster transactions and communication. This hybrid approach combines legitimacy of Dark Web with the speed and scalability of Telegram, making a flexible and robust cybercrime ecosystem.

A significant playerin this ecosystem are stealer logs. These logs are generated when stealer malware infects a device and secretly collects sensitive information such as usernames, passwords, session cookies, and other personal data. This data is gathered from sources like saved browser credentials, keyloggers, or password managers. Once collected, the stolen data is sent to the attacker which often ends up in Telegram groups or Dark Web marketplaces, where it is traded or sold.

Despite telegram becoming more and more well-known as a cybercrime hub,the focus of current academic research and commercial breach detection technologies is on traditional Dark Web marketplaces and large-scale, publicly reporteddata breaches.The granular, high-velocity flow of credentials observed in stealer logs published within semi-private Telegram groups is sometimes overlooked by services like Have I Been Pwned [5], which excel at tracking huge instances. A significant research void is thus created. The data being leaked directly through Telegram, including the kinds of information, the services that are being targeted, and the changing trends within this ecosystem, has not been well examined. As a result, unless they are abused, people and organizations frequently aren't aware of the imminent threats posed by these new, actionable credentials.

This research addresses this gap by proposing and developing a system for the periodic, manual monitoring and analysis of stealer logs shared within specialized Telegram groups. Instead of attempting real-time, automated scraping, our project focuses on a controlled methodology involving manual data extraction, parsing, and organization. The collected data is stored and structured within a local, queryable database

## II. LITERATURE REVIEW

Mainstream online forums have increasingly given way to encrypted and partially accessible platforms like Telegram due to the exponential rise in cybercrime. In order to comprehend how malevolent actors, arrange, disseminate, and utilize stolen data, researchers have started to investigate these developing ecosystems. Stealer logs, which are obtained through malware infestations and contain private data including login details, passwords, cookies, and access tokens, have been a major area of study in this field. The fact that these datasets are frequently exchanged in covert Telegram conversations underscores the platform's expanding significance in cybercrime networks.

One of the most thorough large-scale investigations of cybercriminal behavior on Telegram, encompassing numerous channels and groups, was offered by DarkGram [11]. Their research showed that Telegram has developed into a major distribution center for illegal digital assets, such as malware samples, compromised accounts, and stealer records. From phishing toolkitsto credential leaks, the writers highlighted the scope and diversity of the actions. The study did not, however, give a comprehensive, systematic methodology for tracking and querying stolen data; instead, it was primarily observational and provided macro-level findings. This disparity emphasizes the requirement for systems that can gather, classify, and examine stolen data more thoroughly. As research focused on Telegram has increased, there has also been a wider examination of credential leaks that demonstrates their real-world consequences. Gupta et al. [12] looked into how stolen authentication credentials were used in follow-up cyberattacks. Their research, published in Sensors, underscores the persistent dangers associated with reusing credentials, inadequate password practices, and slow response efforts. The results highlight the need for tools capable of not only identifying but also providing context for compromised data, which can help recognize trends in credential theft. However, their study did not specifically examine Telegram as a distribution method, leaving opportunities for initiatives like ours to investigate this unique and important threat landscape. Understanding stealer logs has also been aided by industry reports. For instance, ZeroFox [13] gave a summary of the production and exchange of stealer logs in underground networks. According to their investigation, attackers frequently combine logs into sizable databases and then sell or disseminate them on forums and messaging apps like Telegram. Although useful, these reports usually only include superficial threat intelligence and don't follow the same methodical approach as scholarly studies. Furthermore, they hardly ever offer publicly available, queryable datasets, which leaves an absence between theoretical understanding and useful monitoring instruments.

The problem of collecting and monitoring data on underground platforms was examined in early works like Kaur and Clancy [14]. They looked at ways to identify and gather Personally Identifiable Information (PII) from both the dark web and the surface web. Their research pointed out the technical challenges in scraping, validating, and classifying leaked data. Likewise, Almeida et al. [15]

suggested a forensic method for analyzing Telegram channels that distribute data leaks. While both studies advanced data extraction techniques, they did not offer easy-to-use systems forquerying leaked data,particularly in the case of stealer logs.

Recent research has looked into how Telegram is used for cybercrime. Kuznetsov et al. [16] studied how encrypted messaging platforms help with illegal activities and suggested ways to detect suspicious groups. Kumar and Singh [17] examined large-scale information leaks on Telegram. They pointed out how different types of datasets, such as credentials, personal information, and financial data, are shared systematically in both public and private groups. While both studies show the extent of leaks on Telegram, they do not offer structured databases or visual analytic dashboards. These tools are necessary for long term monitoring and usefulness to stakeholders.

Kunduru et al. [18] examined the potential and difficulties of obtaining malicious activity data from messaging platforms from a wider cybersecurity standpoint, stressing that although these platforms offer insightful information, the absence of organized surveillance mechanisms is still a significant drawback. Simultaneously, CIRCL [19] investigated the idea of "Stealer Logs as a Service," showing how cybercriminals have made the distribution and sale of credentials they have stolen into a commodity. Although their findings raise emphasis to the financial impact of credential leaks, they once more fall short of offering organized technical solutions for continuous monitoring.

One of the earliest attempts to integrate automation with platform-dependent monitoring was made more recently by Basu et al. [20], who suggested automated techniques for identifying compromised credentials across messaging and darknet sites. Their analysis shows that it is feasible to systematically detect and analyze credential breaches, which is in line with our project's objectives. Their emphasis on automated pipelines, however, necessitates a large investment of resources and ongoing oversight, something might not be constantly possible in settings with inadequate infrastructure.

When combined, the evaluated literature offers insightful information about three related issues. First, a number of studies demonstrate how Telegram has developed towards a secret sector where compromised information circulates at scale, highlighting its emergence as a crucial hub for the distribution of stealer logs and credential breaches [11], [15], and [17]. Second, previous research highlights the practical effects of these breaches on people and organizations, showing how credentials that have beenstolen can be used again in later intrusions and how the monetization of stealer records has led to serious hazards in a variety of industries [12], [19]. Third, methodological difficulties in gathering, categorizing, and tracking leaking data in subterranean ecosystems are frequently mentioned in the literature. Although encrypted messaging services provide a wealth of threat intelligence, researchers point out that current solutions are either very conceptual or largely rely on automated methods that require a lot ofresources[14,16,18,20]. There arestilldefinite research gaps in spite of these efforts. First, there is limited space for human, regulated, and periodic approaches that strike a balance between viability and usefulness because the majority of existing works either function at a macro-level scale (big database insights) or at a highly advanced automated level. Second, a queryable local database system that enables stakeholders to look at particular credentials or breaches periodically is absent from most previous research. Lastly, it can be challenging for non-technical users to understand results when visualization and reporting elements are absent. By concentrating on Telegram groups that share stealer logs, putting in place a pipeline for manual data collecting and processing, and arranging the data in a standardized local database, our suggested approach immediately overcomes these drawbacks. Through the addition of querying capabilities and a visualization dashboard, the system connects the dots between useful cybersecurity tools and insights from scholarly research. Additionally, it provides a solution for systems with limited resources, where systematic monitoring is still crucial but real-time automation isn't always feasible.

## III. METHODOLOGY

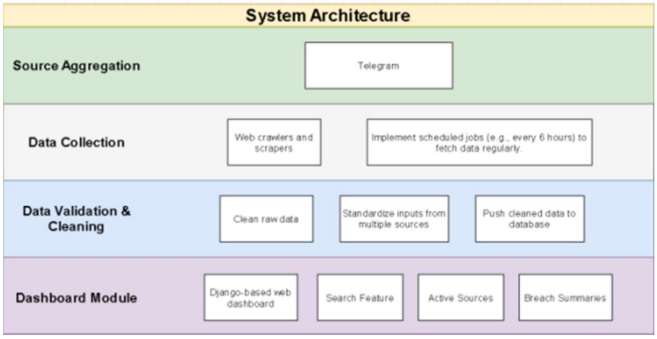



Fig.1. System Architecture

This study adopts a systematic approach to detect any personal data that can directly or indirectly identify an individual, which has been leaked in a breach in Telegram by accessing its channels. As a primary step, we monitor the data from the deep web, collect it and process it thoroughly.
Our model follows 4 steps:

### *A. Data Collection*

To accomplish this stage, we have the deep web as our primary data source. There are several Telegram groups that frequently share stealer logs. These stealer logs contain personal information such as passwords, emails, usernames, CVV numbers, card details, and numerous other compromised credentials.
Currently, the data is being collected manually by joining and monitoring the suspicious Telegram channels. This helps to avert complicated rules and regulations imposed by automated scraping. The system supports nested folders, ensuring each file is being parsed. As there will be numerous files in every folder, it will have various kinds of data in it along with junk. The Logs can be unstructured and inconsistent, thus requiring preprocessing. This acts as a challenge, while parsing and analysing the data.
Data collection is performed without any hacking or unauthorized actions. The system strictly adheres to ethical considerations, ensuring that all data acquisition processes are legitimate and respect privacy and legal boundaries. This commitment to ethical practices is fundamental to maintaining data integrity and trust.

### *B. Data Preprocessing*

The raw data in the folder may be unstructured, containing junk. This may lead to biased analysis, resulting in inaccurate output.
The system uses a Python-based parsingmodule forreading all the files and folders.
The raw data, therefore, is preprocessed. The raw data is normalized by trimming, removing the white space, converting into lowercase to maintain consistency, later standardizing the format.The redundant entries were removed by hashing, preventing duplication during analysis.
Irrelevant entries such as channel advertisements, ASCII banners, or incomplete text were discarded.
After transforming the data, key fields like passwords, emails, cvv, usernames, ip address, urls, etc are extracted from the preprocessed data, then mapped to create a structured format.

### *C. Data Validation and Cleaning*

The transformed data is analyzed to inculcate useful information and store it in structured format.
In the Data Analysis process, the system categorizes the data leaks according to fields - passwords, cvv, usernames, or any other credentials.
It identifies frequent domains, repeated usernames and clusters of similar breaches.
This helps to ease the process of query and retrieve the collected and transformed information and gather required insights. The extracted values are then inserted into accurate columns of the table schema created. The query allows searching and retrieving data by specifically searching for emails, domains, usernames. For instance, a user could input an email address and retrieve all breaches in which it appeared, along with associated credentials and source information.
Since the system is manual, new Telegram dumps are parsed every week/month. Here, Database acts as a central breach repository, which enables faster search for keywords and scalable analysis across numerous files.

| victim_id integer | domain text | username text | password text | application text |
|---|---|---|---|---|
| 5 | coursehero | 43652@bta.com.au | 4********a | Chrome Default (139.0... |
| 5 | fifa | ingeniero.daniel.grana... | M**********@ | Chrome Default (139.0... |
| 5 | axcelerate | ingeniero.daniel.grana... | M**********@ | Chrome Default (139.0... |
| 5 | lottogo | ingeniero.daniel.grana... | M**********0 | Chrome Default (139.0... |
| 5 | petcircle | ingeniero.daniel.grana... | M**********@ | Chrome Default (139.0... |
| 5 | care | ingeniero.daniel.grana... | n**********5 | Chrome Default (139.0... |
| 5 | intuto | ingeniero.daniel.grana... | m*******3 | Chrome Default (139.0... |
| 5 | footballnetwork | ingeniero.daniel.grana... | M*******3 | Chrome Default (139.0... |
| 5 | abs | 4346 3824 7336 2302 | S****************0 | Chrome Default (139.0... |
| 5 | vetshopaustralia | ingeniero.daniel.grana... | m**********0 | Chrome Default (139.0... |
| 5 | jd-sports | ingeniero.daniel.grana... | m*******3 | Chrome Default (139.0... |
| 5 | asos | ingeniero.daniel.grana... | d********5 | Chrome Default (139.0... |
| 5 | hotdoc | ingeniero.daniel.grana... | m*******3 | Chrome Default (139.0... |
| 5 | crust | ingeniero.daniel.grana... | M**********@ | Chrome Default (139.0... |
| 5 | lottosus | ingeniero.daniel.grana... | G********** | Chrome Default (139.0... |
| 5 | auspost | ingeniero.daniel.grana... | M**********0 | Chrome Default (139.0... |

Fig. 2. Processed Data Stored in a Structured Format

*D. Data Visualization*

Topresent the extractedandprocesseddata ina neat manner that would be easier to understand, the system implements a dashboard using Django.

The dashboard incorporates both search functionality and interactive charts. Users can input an email, username, or domain, and the system retrieves all associated breach entries. Each breach is displayed in a card-based format, highlighting the compromised domain, type of leak, exposed data, and source information.

This visualization layer transforms unstructured Telegram leaks into a user-friendly, insightful platform, making the findings valuable to individuals, organizations, and researchers alike.

A comprehensive breach monitoring dashboard was developed using Django, to allow not only big organizations but also individuals to know, if their data is involved in any data breach, in a comprehensive manner.

In summary, the system's methodology follows a systematic flow starting from collecting raw, breached data from suspicious Telegram channels, followed by transforming the data into useful information and creating a dataframe schema for storing the information in structured format. This structure schema is used for analysis that would retrieve the desired information and display it on the dashboard that would be easier for the user to comprehend.

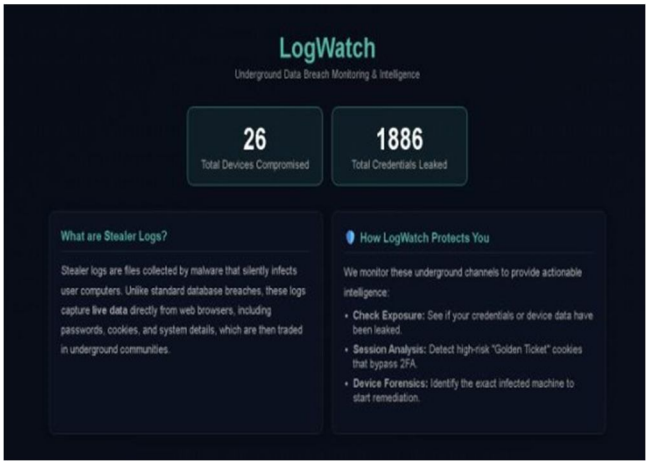



Fig. 3. Landing Page for Dashboard

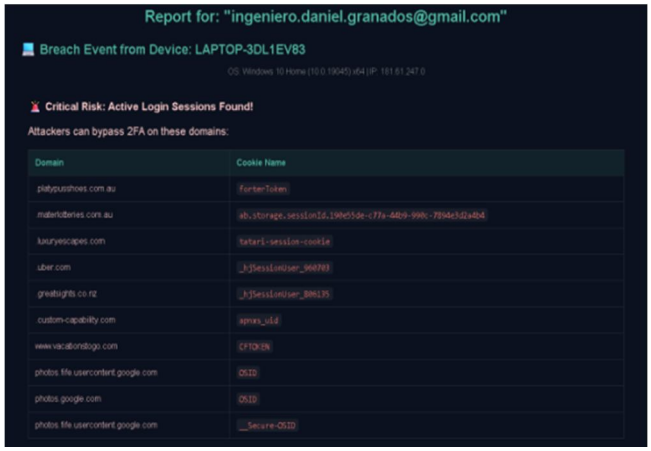



Fig. 4. Dashboard and Results

## IV. RESULT AND DISCUSSION

For collecting the breached data, we incorporated Telegram channels and processed all files. These files had intricated nested networks, which made it harder to parse every file. The files contained 75% valid breached data, along with 25 % Junk and useless data and patterns. A Python parser module helped to parse each and every file from every folder.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

TABLE I. DATA DISTRIBUTION

| *Data Type* | *% Of Total Records* |
|---|---|
| Emails | 40 |
| Passwords | 33 |
| Session Tokens | 15 |
| CVVs | 7 |
| Cookies | 1 |
| Others | 4 |

While pre-processing the data, the files included essential values like emails, passwords, CVV numbers, account numbers, bank details, session tokens, IP addresses, cookies and even phone numbers. The files also provided URLs, through which domains and suffixes were extracted. This all was then stored in a dataframe for easier retrieval and understanding.

After transforming and analysing the data from the Telegram channels, which revealed notable patterns. The insights conclude that data becomes easier to steal if the passwords are weak like '123123', 'ABC123' or if users reuse passwords for different websites. Beyond traditional credentials, a significant number of records included session tokens and cookies, indicating that attackers are increasingly leveraging account takeover techniques that bypass the need for direct password use.

As a result of System Demonstration, the dashboard gives a simple interface for users to retrieve the desireddata. The users can search for Usernames, Domains, Emails and get results. These resultsinclude a statement saying if it is breached ornot. If the statement says the user's data is breached, then the dashboard also provides the relevant data consisting of breach.

TABLE II. DATABASE RECORDS

| *URL* | *USERNAME* | *IP Address* |
|---|---|---|
| https://accounts.google.com /signin /challenge | allenxxxx@gmail.com | 141.168.xx.xx |
| http://10.0.0.2/page/quicksetup /shtml | admin | 161.10.xxx.xx |
| https://online.emetgroup.co.za /login/index.php | emxxxx1986 | 124.170.xx.xxx |
| https://auth.cricut.com /login | allenxxx@gmail.com | 103.192.xxx, xx |
| https://www.netflix.com /za/login | jacoxxxxx@gmail.com | 103.217.xx.xxx |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 14 Issue III Mar 2026- Available at www.ijraset.com*

## V. FUTURE SCOPE

Future enhancements of the proposed system can focus on improving scalability, timeliness, and analytical depth. Using morally compatible crawling and API-based technologies, one major extension entails switching from sporadic manual data collection to semi-automatic or completely automated oversight of Telegram channels. By enabling the intake of stealer records in almost real-time, such automation would shorten the time between data leaking and detection. Furthermore, machine learning-based classification models that can classify stealer logs according to data type, threat level, or targeted service can be added to the framework. Addressing multilingual, obfuscated, or improperly formatted log content which is becoming more common in underground data dumps would be made easier through the addition of natural language processing algorithms.

Increasing the system's applicability and intelligence exchange capabilities is another possible avenue. Automated alerting systems that tell people or organizations when freshly acquired data fits monitored emails, IP addresses, or usernames can improve the dashboard. This would enable preventative mitigation strategies like access audits and credential resets. Additionally, in order to create a single breach intelligence repository, the monitoring scope can be extended beyond Telegram to include paste sites, dark web forums, and other encrypted platforms. In order to provide a more thorough and coordinated response to the changing ecosystem of credential theft and data breaches, future research may also investigate secure collaboration models in which concealed insights from the framework can be communicated with cybersecurity teams, researchers, or regulatory organizations.

## VI. CONCLUSION

The paper successfully demonstrates how a systematic strategy can be utilized to investigate potential breaches of personal data that are circulating on Telegram channels.

By deploying a systematic approach of collection, preprocessing, analysis, and displaying, the developed system transforms extremely disorganized and unpredictable stealer logs into valuable and actionable information. While ensuring that ethical standards are respected and followed and thus preventing any unauthorized access or unethical hacking, the manual collection approach provides a helpful tool to monitor crucial information being discussed in secret Telegram groups (the telegram channel used here was.boxed.pw). This study highlights the rising importance of Telegram as a platform for trading stolen credentials like passwords, images, emails, cvv and the need to take proactive measures to identify, arrange, and keep an eye on such data for security and awareness reasons.

The system has a particular data preparation process. This process is critical for preventing noisy, missing, or redundant data from influencing the final outcomes. The study generates a clean and reliable dataset that can be rapidly searched and evaluated through the use of normalization, hashing, and systematic mapping of significant variables. The following study provides useful information for understanding the scope and pattern of leaks, such as identifying repeating usernames, commonly used domains, and grouping related breaches. The complete technique, when combined with the visualization dashboard, converts complex and distributed breach data into an easily accessible platform that may benefit both corporations and individual users who want to identify whether their personal information has been compromised. This is especially crucial in today's digital environment, where breaches occur often, and compromised data can spread quickly across multiple platforms.

The program is subject to certain limitations, though. Because the data gathering method is manual, the system may encounter scalability issues as the volume of Telegram dumps grows rapidly. Because of the reliance on daily or periodic updates, real-time monitoring is currently impractical and may result in new breaches going unnoticed.

Similarly, more complex visualization and connection with automated warning systems could enhance the system's usability even if Django provides a reliable interface for data presenting. Nonetheless, the study creates a strong foundation by showing how systematic management of Telegram leaks may be used to create a shared repository for credentials that have been stolen and serve as a tool for risk assessment and personal awareness. Another promising option is to extend the dashboard's capabilities to provide customized breach alerts and recommendations. For instance, if a customer's email address or associated credentials are discovered in a new dataset, they may receive immediate alerts along with useful advice on account security. Organizations may also use this technology to monitor their domains and staff login credentials so they can react to potential security issues faster.

## VII. ACKNOWLEDGMENT

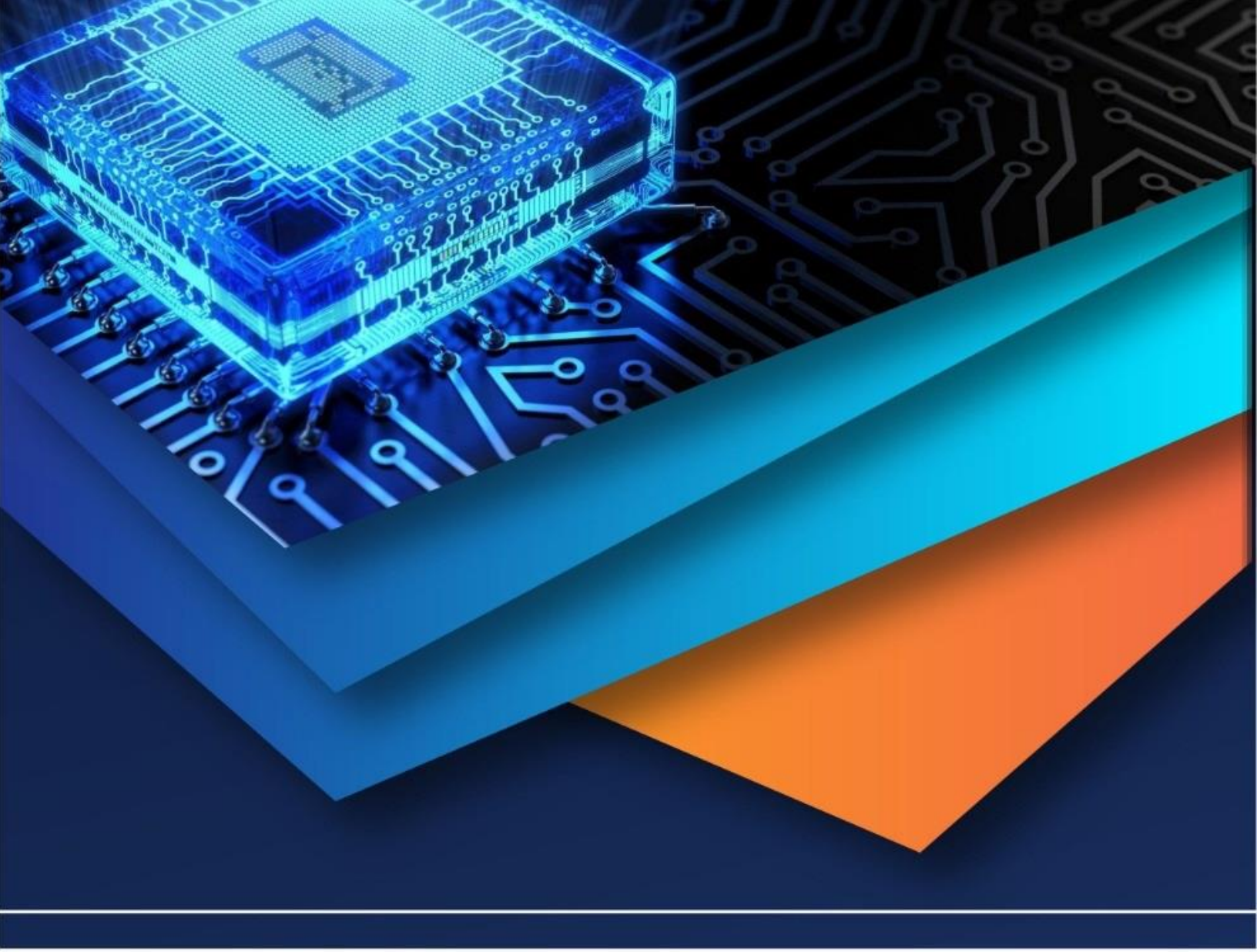
We would like to extend our sincerest appreciation to the esteemed individuals and organizations that have contributed to the successful culmination of this research endeavor. Our deepest gratitude is reserved for our distinguished academic advisor, Mr. Devendra Bodkhe, whose erudite expertise, unwavering support, and sagacious insights have been instrumental in shaping the trajectory of this research.

We acknowledge the pivotal role played by the Department of artificial intelligence & data science at Thakur College of Engineering and Technology in providing the requisite resources, infrastructure, and an intellectually stimulating environment. Additionally, we appreciate the insightful feedback and engaging discussions provided by our colleagues and peers, which have enriched our understanding, refined our methodology, and enhanced the overall quality of our research.

## REFERENCES

[1] IBM, "Cost of a Data Breach Report 2025," IBM Reports, Accessed: Sep. 15, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach
[2] A. K. Ghazi-Tehrani, "Mapping Real-World Use of the Onion Router," J. Contemp. Crim. Justice, vol. 39, no. 2, pp. 239–256, 2023. doi: 10.1177/10439862231157553.
[3] Y. Maia and M. Rubio, "Telegram's Dark Trade: Unpacking Brazil's Data Leak Surge," in Proc. SBSEG 2025, pp. 1145–1152, 2025. doi: 10.5753/sbseg.2025.9824.
[4] W. C. Lim, "Report: Telegram 'Cybercrime Ecosystem' Rivals the Dark Web, but Much Easier to Access," Swarmnetics Blog, Feb. 20, 2023. [Online]. Available: https://swarmnetics.com/blog/report-telegram-cybercrime-ecosystem-rivals -the-dark-web-but-much-easier-to-access/
[5] Have I Been Pwned,"haveibeenpwned.com. https://haveibeenpwned.com/ (accessed Sep. 15, 2025)
[6] S. Shaikh and K. Malgaonkar, "A comprehensive approach to dark web surveillance," Int. J. Eng. Res. Technol., vol. 11, no. 12, pp. 1–4, Dec. 2022. [Online]. Available: https://www.ijert.org/a-comprehensive-approach-to-dark-web-surveillance
[7] A. Dalvi and S. Bhirud, "Dark web monitoring as an emerging cybersecurity strategy for businesses," Int. J. Inf. Eng. Electron. Bus., vol. 16, no. 2, pp. 54–67, Apr. 2024. [Online]. Available: https://www.mecs-press.org/ijieeb/ijieeb-v16-n2/v16n2-5.html
[8] R. R. Gopireddy, "Dark web monitoring: Extracting and analyzing threat intelligence," Int. J. Sci. Res., vol. 9, no. 3, pp. 1693–1696, Mar. 2020. [Online]. Available: https://www.researchgate.net/publication/384008320_Dark_Web_Monito ri ng_Extracting_and_Analyzing_Threat_Intelligence
[9] E. Nunes, A. Diab, N. Shetty, D. Hoops, C. Agarwal, and P. Shakarian, "Darknet and deepnet mining for proactive cybersecurity threat intelligence," arXiv preprint, arXiv:1607.08583, Jul. 2016. [Online]. Available: https://arxiv.org/abs/1607.08583
[10] S. Sarkar, M. Almukaynizi, J. Shakarian, and P. Shakarian, "Predicting enterprise cyber incidents using social network analysis on the darkweb hacker forums," arXiv preprint, arXiv:1811.06537, Nov. 2018. [Online]. Available: https://arxiv.org/abs/1811.06537
[11] A. K. DarkGram Team, "DarkGram: A Large-Scale Analysis of Cybercriminal Activity Channels on Telegram," arXiv preprint, 2024.
[12] S. Gupta, R. Sharma, and P. Roy, "Beyond the Leak: Analyzing the Real-World Exploitation of Leaked Authentication Credentials," Sensors, vol. 25, no. 4, pp. 1123–1139, 2025. doi: 10.3390/s25041123.
[13] ZeroFox, "Introduction to Stealer Logs," ZeroFox Threat Report, 2022. [Online]. Available: https://www.zerofox.com/resources/introduction-to-stealer-logs/
[14] R. P. Kaur and T. C. Clancy, "Identifying, Collecting, and Monitoring Personally Identifiable Information From the Dark Web to the Surface Web," ResearchGate Preprint, Dec. 2020. [Online]. Available: https://www.researchgate.net/publication/347474334_Identifying_Collect ing_and_Monitoring_Personally_Identifiable_Information_From_the_Dark_Web_to_the_Surface_Web
[15] T. Almeida, L. Cruz, and R. Araujo, "Data Leak Detection on Telegram Channels: A Forensic Approach," in Proc. SBSeg 2023, pp. 511–524, Sept. 2023. [Online]. Available: https://sol.sbc.org.br/index.php/sbseg/article/view/36691/36478
[16] S. Kuznetsov, M. Ivanov, and A. Petrov, "Detecting Cybercrime Activities in Encrypted Messaging Platforms," in Lecture Notes in Computer Science (LNCS), Springer, pp. 121–135, 2023. doi: 10.1007/978-3-031-xxxx-xx_10.
[17] A. Kumar and R. Singh, "Information Leaks on Telegram Channels," Computers & Security, vol. 131, pp. 103–118, 2023. doi: 10.1016/j.cose.2023.103118.
[18] S. Kunduru, P. Mittal, and A. Kapadia, "Threat Intelligence from Messaging Platforms: Opportunities and Challenges," in Proc. ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC), pp. 45–56, Nov. 2022. doi: 10.1145/3560826.3563389.
[19] CIRCL, "Stealer Logs as a Service: Investigating the Underground Economy," CIRCL Report, 2023. [Online]. Available: https://www.circl.lu/pub/tr-79/
[20] A. Basu, N. Chatterjee, and S. Banerjee, "Automated Detection of Leaked Credentials in Darknet and Messaging Platforms," IEEE Access, vol. 12, pp. 45123–45140, 2024. doi: 10.1109/ACCESS.2024.3389123,



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY