iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** VIII **Month of publication:** August 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.46268

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 10 Issue VIII Aug 2022- Available at www.ijraset.com*

# What is Open-Source Intelligence and How it Can Prevent Frauds

Dhanush Chalicheemala[1], Dinesh Chalicheemala[2]
[1]*Information Technology, Vellore Institute of Technology*
[2]*Mechanical Engineer, Vellore Institute of Technology*

***Abstract:** This paper introduces the concept of Open Source Intelligence (OSINT) and How OSINT can prevent Frauds .The Estimated Data Consumption from 2021 to 2024 by finances online could increase from 74 zettabytes to 149 zettabytes [1] and most of this data is Publicly available. OSINT is an intelligence that is Produced by collecting, processing, analysing and correlating the information available publicly. Crimes such as fraud, illicit trade, and security are developing in the digital era of the twenty-first century, and new methods and procedures are emerging that can make them tougher to detect and investigate. OSINT investigations gather insights from open source data (OSD), revealing information on possible business partners, clients, suppliers, and workers. With the assistance of next-generation OSINT tools, corporate investigations teams and anti-fraud specialists can make the rapid and correct choices necessary to avoid reputational and financial harm.[20]*

## I. INTRODUCTION

OSINT consists of information from various sources like the internet, mass media, specialist journals and research, blogs, social media, photos, and geospatial information. Over 4.9 billion people using internet (approximately 63% of total earths population), The amount of data generated every day is enormous. This amount of data is also a great source of knowledge for governments, intelligence agencies, and commercial companies seeking a competitive advantage or keeping tabs on what's going on in the world.[3] It is difficult to organize the huge data available, into the required form by ourselves. This problem can be overcome by using the OSINT Framework.

OSINT Framework is a collection of tools that are used to make your intel and data collection tasks easier. Security researchers and penetration testers mostly utilise these Tools for digital foot printing, OSINT research, intelligence collecting, and reconnaissance. It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories. It also provides an excellent classification of all existing intel sources. OSINT Framework is classified based on different topics and goals. This can be easily seen while taking a look at the OSINT tree available through the web interface.[4]


OSINT is primarily employed in national security and business intelligence tasks, and analysts who use non-sensitive intelligence to solve classified, unclassified, or proprietary intelligence requirements across the previous intelligence disciplines would benefit from it..[5]

Intelligence agencies use OSINT to track events, equipment such as weapons systems, and people. These are the 'targets of interest' (ToIs). But hackers use OSINT to identify technical vulnerabilities as well as human targets for phishing and social engineering attacks. OSINT helps security teams unearth clues that individuals leave in the open that compromise security. Like using a vulnerability scanner to find flaws in systems, OSINT tools pick up on problem data, such as dates of birth, Social Security numbers, family members or even hobbies that could help attackers compromise an account. [6]

Open source intelligence predates the internet. Governments have long used newspapers, and later broadcasts, to track potential adversaries' military, political, or economic plans and activities. During 1930's, The British government ordered the BBC to establish a new service that would collect and analyse print journalism from around the world. The service was originally called as BBC Monitoring, but it was later renamed Digest of Foreign Broadcast.[3]

## II. OSINT ADVANTAGES AND DISADVANTAGES

### A. *OSINT Benefits*

1) OSINT data can provide insight to corporate owners and decision makers, allowing them to develop long-term strategies for a range of business objectives.[7] OSINT can help companies quickly detect when sensitive company information is discussed or published on dark web message boards or forums, helping security teams investigate breaches and learn about the vulnerability hackers may have exploited to access the information.[3]
2) Regular data collection tools and approaches may prove to be too costly for smaller or independent businesses. OSINT requires little to no financial commitment because the information is, by definition, free. OSINT offers a potentially greater return on investment and this feature is particularly relevant for organizations with a tight intelligence budget.[8]
3) It is legal to access OSINT Because the information obtained is not classified and has been widely disseminated.[8] OSINT doesn't include classified information or information derived from unknown sources. There is also no information that may be subject to proprietary restrictions, such as information obtained through sensitive or clandestine relationships.[9]
4) One of the most important advantages of intelligence is that it aids in task and time prioritisation. Because the information you collect is publicly available, you can plan how you'll use it to carry out your strategy and ensure that you're using the most up-to-date security measures.[10]
5) Users routinely exchange and update the material because it is based on public resources.[8] This particular data gathering discipline makes it possible for us to keep track of certain events and phenomena in real time. It is possible to follow migrants' routes, investigate the consequences of a terrorist attack, outburst of an epidemic, the organization of violent demonstrations and the like.[11]

### B. *OSINT Limitations*

1) OSINT contains huge collection of data, filtering away garbage data from essential information might be difficult depending on the volume of data found. Finding information is meaningless unless it is put to use in some meaningful way.[7]
2) The public information available on the Internet is inherently chaotic. This implies that the OSINT data is so diverse that it is difficult to identify, connect, and evaluate it in order to extract useful correlations and information . In this sense, in order to use unstructured information, OSINT requires processes such as data mining, Natural Language Processing (NLP), or text analytics to homogenise it.[12]
3) In addition to taking up a large amount of time, the requirement to continually monitor, search, and filter vast troves of accessible information to discover useful insights is laborious even for experienced analysts. While AI, machine learning, and other specialised technologies assist researchers in parsing information more rapidly, it is difficult for any major business to swiftly identify all crucial, time-sensitive events as they occur.[3]
4) After you have filtered out useable data, you must ensure that the information is trustworthy. Organizations and individuals may purposefully disseminate misleading information in order to deceive prospective attackers.[7]
5) The rise of OSINT raises several questions concerning privacy, respect, and personal integrity . In this regard, it should be underlined that the topic of whether OSINT is an ethical concern falls under the purview of intelligence collecting ethics. OSINT can be used by illegal organizations to keep track of different works they do.[12]

## III. WHAT DOES AN OSINT INVESTIGATOR DO?

The key to internet research is to track the digital bread crumbs that individuals leave online. Open source is defined as information that is legally available to the whole public. This website offers a wealth of free open-source resources for information study and analysis. Although the material on this website is available to anybody, it would be most useful to people in investigative jobs such as Analysts and Researchers.[13]

An OSINT investigator is responsible for obtaining, evaluating, and extracting knowledge from their discoveries. While everyone works differently and each business has its own rules for how an investigation is carried out, some frameworks are commonly followed.[14]

*A. Collecting information from open sources:*[14]

Start with the information that have with the investigator . search for all the information that an investigator can get from the his sources , information like email addresses, phone number, usernames, given names, addresses and etc.

*B. Filtering:*

Most of the findings may have irrelevant and unnecessary information for the investigation, investigator should segregate the information that is required and that is not required.

*C. Analysis of Information*

The investigator looks at the data and construct a hypothesis based on the data they observed, aiming toward an actionable insight. This can range from something simple to uncover an very elaborate schemes/plots.

*D. Gaining Insights*

At the conclusion, the investigator might offer a suggestion on what to proceed with the provided case and submit their explanation along with the pertinent evidence. It's a good idea to bring in another investigator at this point to rule out any potential bias.

## IV. OSINT IN FRAUD PREVENTION

Without efficient internet surveillance, anti-fraud, anti-money laundering, and anti-counterfeiting regulations are meaningless. It's critical for businesses that lose money due to product fraud and counterfeiting to be able to track down and prosecute the perpetrators using automated open source intelligence (OSINT) monitoring.[15]

*A. Financial Frauds*

Financial fraud is a common occurrence all around the world. It can be demonstrated by a breach of information disclosure obligations that causes reputational harm to companies and managers in the capital and labour markets, such as a drop in share prices, an increase in financing costs, and the loss of jobs for directors and executives.[16]

In certain cases, standard ways of identifying financial fraudsters have proven ineffective. Technology advancement has facilitated the growth of open-source intelligence (OSINT), which is utilised to improve information collection and processing capabilities. Financial crimes are an increasing threat, ranging from global stock market manipulation to Ponzi schemes to credit card fraud. Crooks may steal money from unsuspecting victims all around the world by using websites and email phishing schemes. Financial fraudsters frequently use information available on social media networks for their malicious goals. However, determining the nature of the fraud is difficult, and it may require the assistance of specialists. OSINT could be viewed of as a whole body check up on entities in the digital domain, rather than just basic keyword searches and creating linkages.[17]

When utilised effectively, OSINT may be used to acquire intelligence about people' or organisations' behaviour, reputation, and online activities, and then analyse them based on certain risk indicators related to financial crime. With 42% of fraudsters shown to be living beyond their means, one of the key tools that open-source intelligence checks can play is in identifying wealth mismatch as a behavioural risk.[18]

To provide an effective defence against opportunists and fraudsters, financial institutions should continue to adjust their risk assessment methods to include open source intelligence checks. Regulations are always evolving and will very certainly necessitate even more data points in the future. Using open-source data now can not only assure compliance but also potentially prevent against costly errors.[18]

*B. Insider Frauds*

Insider fraud occurs within a company and includes expenditure fraud, corruption, sabotage, and data leaking. Insider fraud at the corporate level might include skimming money from contracts, bribing or receiving bribes, false accounting, or the organised theft/embezzlement of assets and funds. Because of the various ties developed between modern organisations and their worldwide labour force and supply networks, insider threats are more prevalent than ever.

Insider fraud cases are frequently solved by finding relationships between an employee and a prospective offender. Internal data can be beneficial here, but critical linkages are frequently found in open source data.[20] Combating insider fraud begins with identifying the categories of information that may or may not be fraudulently utilised, as well as the people who have access to it.

An employee population may be vulnerable to fraud, necessitating greater awareness measures such as registration in an employee dependability programme, heightened monitoring of information access, and checks on how information is utilised. [19]

Other measures that firms may take to combat insider fraud include the construction or upgrading of important business process audits and the verification and alteration of critical data, customer financial information, and employee records. Organizations should also undertake background checks on potential employees, contractors, and subcontractors to search for any unreported criminal past or a history of financial troubles that might give a motivation for fraud.[19]

Due diligence is a vital preventative measure: organisations must work hard to understand their business partners, doing rigorous and complete background investigations. For the greatest results, these checks must include all accessible sources, which means that the use of OSD is crucial.[20]

### *C. Online Frauds*

With Internet adoption rates and sales on e-commerce sites reaching all-time highs, it's no wonder that a market teeming with counterfeit, stolen, and fraudulent items has emerged online. As internet adoption rates rise, the financial services, insurance, and industrial industries are seeing a large surge in fraud losses.

The International Chamber of Commerce (ICC), an organisation entrusted with aiding in the battle against the online sale of counterfeit products, estimates that counterfeit goods cost industrialised nations $125 billion in tax income and welfare expenditure, as well as the loss of nearly 2.5 million jobs. What's more, given the present pace of growth, the ICC anticipates the value of counterfeit goods to surpass $1.7 trillion by 2015, accounting for more than 2% of global current economic production.[15]

Infringers who trade in counterfeit products online intentionally frequently utilise false personal information or anonymous identities. An open-source inquiry might aid in determining the identities of these merchants. A test purchase is frequently used to obtain critical information (such as email addresses, payment accounts, and a return address) in addition to the facts publicly accessible online. Each piece of information is then verified using Google searches and queries on specific databases, which frequently results in the identification of the entity hosting the accounts.

Many governments make company registrations largely or totally public, allowing searches based on names, addresses, or firm registration numbers. If our investigation identifies a company as the primary entity carrying out the infringing activities, consulting these records can assist in verifying the business registration details, identifying the main actors, determining whether a company is solvent, and frequently uncovering additional registered legal entities controlled by the same directors.[21]

### *D. OSINT Future Trends*

The number of enterprises in the globe is growing, and with it, so does the danger level. The amount of open source content available has skyrocketed. The internet has grown inextricably linked to real-world risks in numerous ways. Enterprise IT security teams are increasingly being charged with undertaking OSINT operations against their own companies in order to achieve the greatest degree of operational security, aided by security analytics. [22]

Social media has grown in popularity throughout the world in recent years. Over 80% of the world's population has at least one social media account. Individuals are utilising social media accounts for more than just communication. Social media has also evolved into a medium for marketing for both individuals and corporations. Because a big amount of vital information is available in one spot, social media networks give various possibilities for online research.[23]

Availability of open-source data and rise of cyber threats are likely to drive the market demand significantly. Social media platforms accumulate data pertaining to location, community, interests, and likes for informing government agencies of any possible threats

## V. CONCLUSION

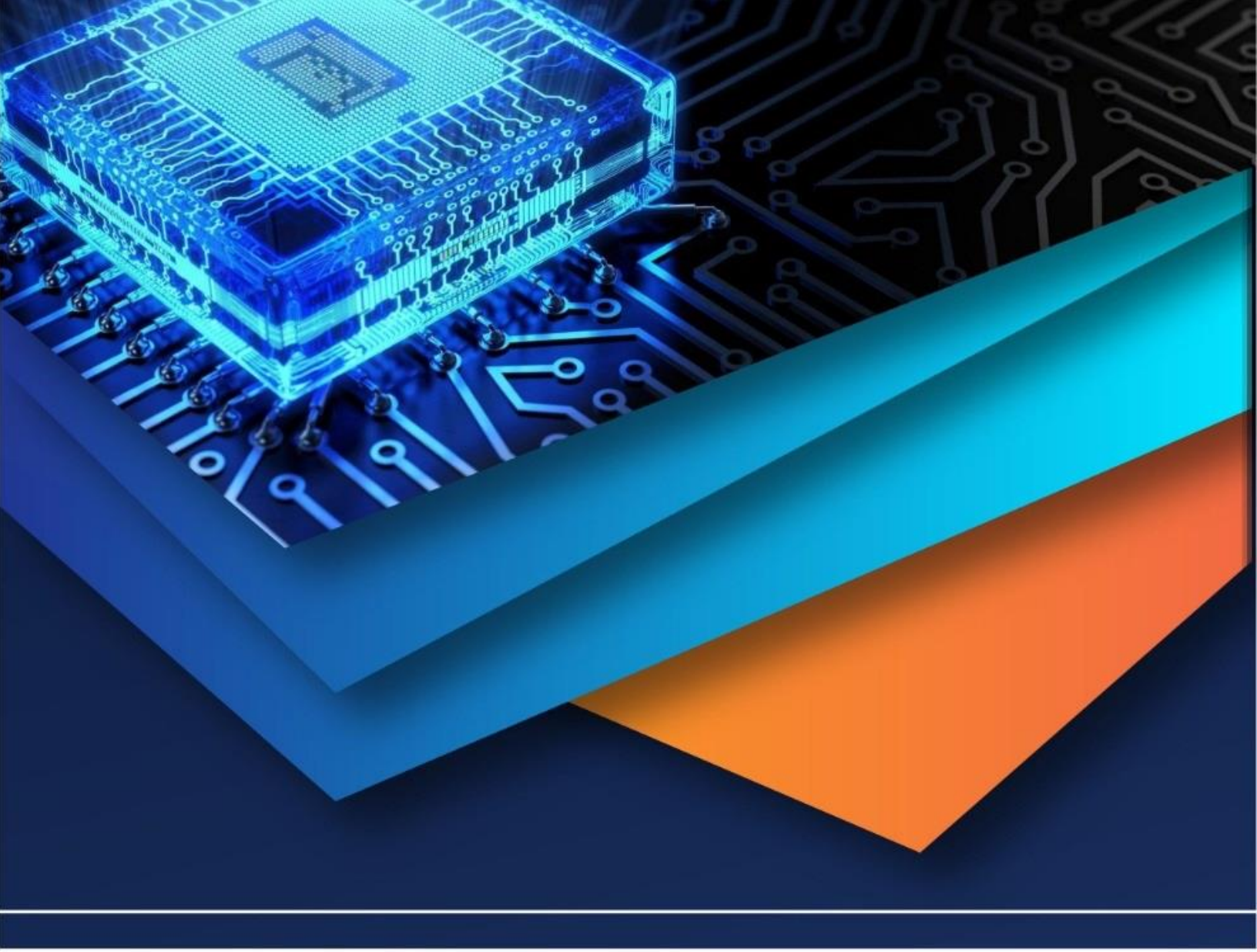
In the analyst's toolset, Open Source Intelligence is like a Swiss army knife. It's especially useful in the area of fraud prevention since hackers specialise in defeating the automatic security mechanisms that we put in place to protect them.[14]

Data is money, and as more processes throughout the world are digitised, OSINT sources are becoming increasingly wealthy. This is true even in underdeveloped countries as the global economy grows. It is up to us to create and implement techniques for making the greatest use of this OSINT data. After all, this information is widely available and open to anyone.[24]

The extraction of knowledge from public sources represents a way of resolving existing problems from a different and innovative perspective. Specifically, cybersecurity and cyber defence can be greatly benefited by the results that this type of intelligence can offer.so, innovating new osint techniques and use of osint is important to prevent Frauds in the modern world.

## REFERENCES

[1] Andre, Louie. "How-Much-Data-Is-Created-Every-Day." Financesonline.Com, https://financesonline.com/how-much-data-is-created-every-day/
[2] https://osintframework.com/
[3] "What Businesses Need to Know About OSINT in 2022 [+ Tools]." AlertMedia, www.alertmedia.com, 9 Feb. 2022, https://www.alertmedia.com/blog/open-source-intelligence/#:~:text=OSINT%20can%20help%20companies%20quickly,exploited%20to%20access%20the%20information.
[4] BORGES, ESTEBAN. "OSINT Framework: The Perfect Cybersecurity Intel Gathering Tool." Securitytrails.Com, 2 Jan. 2019, https://securitytrails.com/blog/osint-framework#:~:text=OSINT%20Framework%2C%20as%20its%20name,%2C%20intelligence%20gathering%2C%20and%20reconnaissance.
[5] "Open-Source Intelligence - Wikipedia." Open-Source Intelligence - Wikipedia, en.wikipedia.org, 1 Mar. 2016, https://en.wikipedia.org/wiki/Open-source_intelligence#cite_note-row-2022-1.
[6] Stephen Pritchard. "OSINT: What Is Open Source Intelligence and How Is It Used? | The Daily Swig." The Daily Swig | Cybersecurity News and Views, portswigger.net, 19 Nov. 2020, https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used.
[7] Mukherjee, Lumena. "Open Source Intelligence: What Is OSINT & How Does It Work?" InfoSec Insights, sectigostore.com, 17 July 2020, https://sectigostore.com/blog/open-source-intelligence-what-is-osint-how-does-it-work/.
[8] "What Is Open Source Intelligence or OSINT? Advantages & More." Cobwebs Webint Solutions, cobwebs.com, 15 Mar. 2021, https://cobwebs.com/the-advantages-of-open-source-intelligence-osint/.
[9] James Murphy . "5 Benefits of Using Open Source Intelligence - DZone Open Source." Dzone.Com, dzone.com, 2 Nov. 2020, https://dzone.com/articles/5-benefits-of-using-open-source-intelligence.
[10] Lucia Danes. "5 Pros (Advantages) of Using Open Source Intelligence (OSINT)." 5 Pros (Advantages) of Using Open Source Intelligence (OSINT), reviewedbypro.com, 9 Dec. 2021, https://reviewedbypro.com/5-pros-advantages-of-using-open-source-intelligence-osint/.
[11] Tomislav Dokman, and Tomislav Ivanjko. Open Source Intelligence (OSINT): Issues and Trends. researchgate, 0 Jan. 2020, https://doi.org/10.17234/INFUTURE.2019.23.
[12] Galindo, Javier Pastor. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. ieeexplore.ieee.org, 9 Jan. 2020, https://doi.org/10.1109/ACCESS.2020.2965257.
[13] https://www.osinttechniques.com/
[14] "Open Source Intelligence Techniques (OSINT) for Fraud Prevention - SEON." SEON, seon.io, 30 May 2022, https://seon.io/resources/guides/open-source-intelligence-techniques-osint-for-fraud-prevention/.
[15] bluemonkeydev. " Open Source Intelligence (OSINT) for Fraud Prevention and Detection – BrightPlanet." Open Source Intelligence (OSINT) for Fraud Prevention and Detection – BrightPlanet, brightplanet.com, 12 Feb. 2015, https://brightplanet.com/2015/02/12/whitepaper-open-source-intelligence-osint-fraud-prevention-detection/.
[16] Qingquan Xin, et al. "The Economic Consequences of Financial Fraud: Evidence from the Product Market in China." Taylor & Francis, www.tandfonline.com, 13 Sept. 2018, https://www.tandfonline.com/doi/full/10.1080/21697213.2018.1480005.
[17] WE_TE. "Utilizing OSINT in Combating Financial Frauds – CyberPeace Corps." Utilizing OSINT in Combating Financial Frauds – CyberPeace Corps, www.cyberpeacecorps.in, 16 Aug. 2021, https://www.cyberpeacecorps.in/utilizing-osint-in-combating-financial-frauds/.
[18] "Using Open Source Intelligence To Battle Fin Crime." Neotas, www.neotas.com, 21 Dec. 2021, https://www.neotas.com/using-open-source-intelligence-to-battle-fin-crime/.
[19] Peter Sullivan. "How Insider Fraud Can Be Detected and Avoided in the Enterprise." SearchSecurity, www.techtarget.com, 1 Sept. 2018, https://www.techtarget.com/searchsecurity/tip/How-insider-fraud-can-be-detected-and-avoided-in-the-enterprise.
[20] Brown, Charles. "OSINT in Fraud Prevention, Corporate Investigations – Blackdot Solutions." Blackdot Solutions Videris, blackdotsolutions.com, 17 Mar. 2022, https://blackdotsolutions.com/blog/fraud-prevention/.
[21] "GreyScout | Using Open-Source Intelligence for Brand Protection." GreyScout, greyscout.com, 8 June 2021, https://greyscout.com/open-source-intelligence-for-brand-protection/.
[22] "Fact.MR – Open Source Intelligence Market Forecast, Trend Analysis & Competition Tracking - Global Review 2021 to 2031." Open Source Intelligence Market Size, Share, Trends 2031, www.factmr.com, 1 July 2022, https://www.factmr.com/report/open-source-intelligence-market.
[23] "Worldwide Open-Source Intelligence Industry to 2028 - Integration of Artificial Intelligence with Open-Source Intelligence Presents Opportunities - ResearchAndMarkets.Com | Business Wire." Worldwide Open-Source Intelligence Industry to 2028 - Integration of Artificial Intelligence with Open-Source Intelligence Presents Opportunities - ResearchAndMarkets.Com | Business Wire, www.businesswire.com, 26 Jan. 2022, https://www.businesswire.com/news/home/20220126005532/en/Worldwide-Open-source-Intelligence-Industry-to-2028---Integration-of-Artificial-Intelligence-with-Open-Source-Intelligence-Presents-Opportunities---ResearchAndMarkets.com.
[24] Varga, Gergo. "OSINT for SecOps: How to Tap into Open Source Intelligence - Hashed Out by The SSL Store™." Hashed Out by The SSL Store™, www.thesslstore.com, 10 Feb. 2022, https://www.thesslstore.com/blog/osint-for-secops-how-to-tap-into-open-source-intelligence/.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY