An Integrated Big Data Model to Salvage Nigeria's Insecurity Challenges

Onoja Anthony [1*], ***Kembe Msugh Moses*** [2*], ***Bwebum C. Dang*** [3], ***Obilikwu Patrick*** [4].

[1] *Department of Data Science, Scuola Normale Superiore, Pisa, Italy;* [2,4] *Department of Mathematics and Computer Science, Benue State University, Makurdi-Nigeria;* [3] *Department of Mathematics, Faculty of Natural Sciences, University of Jos, Nigeria.*

ABSTRACT

There is no doubt about the tremendous achievement of Big Data since its inception in recent times. Developed nations like the United States, Germany, and Australia are utilizing it along with manpower skillsets in their fight against crime and recorded tremendous success. In Nigeria, the fight against insurgence and local crime has witnessed an upsurge in recent times ranging from multiple attacks recorded by the Islamic State of West Africa Province, Boko Haram, Fulani Herdsmen and Farmers' clashes, Bandits, Cyber-crimes, Kidnapping, IPOB, and other civic unrest such as the ENDSAR protest. These have overwhelmed the present security architecture which has often struggled to contain the situation and restore peace to warring factions. This study, therefore, proposed an Integrated Big Data for Security Information Sharing (IBDSIS) model that integrates datasets from databases of security agencies, non-paramilitary organizations, and Internet of Things (IoT) devices in Nigeria to form a holistic cloud-based information sharing platform. The implementation steps and strategies proposed by this study to adopt the IBDSIS modeling framework into the current national security architecture can bring together domain experts and data scientists to analyze tones of datasets pooled together using artificial intelligence, machine learning, and graphical visualization techniques to observe hidden patterns and insights for knowledge discoveries. The results of their analyses (products) will be customized into web applications and continuously update and deploy for security agencies' utilization in the fight against insecurity and external aggression. Our study expounds on related literature on common data models, big data, and applications to national security. We proposed the implementation steps and strategies for the adoption of the IBDSIS architectural modeling framework for information sharing by the relevant security agencies.

Keywords: Crime, National Security, Big Data, Data Integration, Information sharing

OPEN ACCESS

****Correspondence:*** *Anthony Onoja. Department of Data Science, Scuola Normale Superiore, Pisa, Italy.*
Email: *anthony.onoja@sns.it.*

Specialty Section:
This article was submitted to Science section of NAPAS.

Accepted: *13 April, 2022*
Published: *1 May 2022*

Citation:
Onoja A, Kembe MM, Bwebum CD, Obilikwu P. (2022). An Integrated Big Data Model to Salvage Nigeria's Insecurity Challenges. Nig Annals of Pure & Appl Sci. 5(1):125-136. DOI: 10.5281/zenodo.6891960

Publisher:
cPrint, Nig. Ltd
E-mail:
cprintpublisher@gmail.com

Access Code

http://napas.org.ng

INTRODUCTION

Ever since the emergence of Data Science as a hybridization of Statistics, Computer Science, and domain knowledge, humanity has continued to record ground-breaking discoveries ranging in fields of medical sciences, engineering, governance, and economies [15]. The field of Data Science employed the use of scientific methods, processes, algorithms, and domain knowledge to extract hidden patterns and insights from structured and unstructured data sets. Diverse skills such as mathematics, machine learning, artificial intelligence, statistics, big data, database, and optimization coupled with a deep understanding of problem formulation are integrated for meaningful insights from data [5], [9].

Big Data is mustered around thongs of concepts, technologies, and methodologies that envelop a novel technique for gathering, managing, and analyzing data-not just tabular and relational data, but also linguistic, visual, and textual data [14]. The problem with 'big data is that there is too much data being generated, too fast, and too many different sensors to manage easily [20], [11]. The unspeakable joy with Big Data is that new types of analytics and algorithms, including artificial intelligence and machine learning, can be utilized to analyze these huge messy datasets from diverse sources. Analytics from Big data has contributed to new knowledge discoveries, examination of hidden patterns, relationships, and insights that long eluded the traditional methods of statistical data analyses [15]. The applications of Big Data analytics and technologies in beefing national security and minimizing criminal activities through information sharing, storage, and analyses by relevant security agencies in Nigeria are crucial especially at these perilous times [21].

For example, there have been recent developments in applications of big data technologies in developed countries such as the United States of America, Germany, Australia, etc. which potentially offer the national security communities new capabilities to beef up data collection, collation, and information sharing to analyze for hidden trends and insights from Big Data [16], [17]. With the recent data explosion in the digital era, diverse means of gathering data range from Internet of Things (IoT) devices and social media (Twitter, Facebook, Instagram, etc.) now stream in large volume, high velocity, and veracity [14]. This makes it impossible to manage, store and obtain hidden insights from these data sets using the existing traditional methods [22].

In response to the growing breadth and depth of the 21st-century national security threats in Nigeria, relevant bodies have been charged by the Federal Government in Nigeria to enact policies that emphasized breaking down 'stovepipes' to create an effective 'information sharing and collaboration model' to assist in curbing crimes and other forms of civic unrest that has bedeviled the country [13]. One of the key challenges in implementing such an approach is the sheer volume or 'flood' of data, with the outburst of crime reported across the six geo-political zones in Nigeria, almost at the same time [18]. There is also a limited capacity of agencies and human resource experts in Nigeria to manage and analyze this exponentially growing data flood that prevents the national security community from fully exploiting its benefits [15]. Overcoming the data flood by existing security agencies in Nigeria requires the application of new technologies [11]. The national security communities in Nigeria risk being overloaded by the information it collects if it is unable to innovate in response to the big new data norm. In a developing country like Nigeria, with its population rising, and a history of diversity and religion, the need to adopt new technologies such as Big Data and Artificial intelligence is crucial as the country witnessed a geometric rise in crime rate daily [4].

The lack of effective manpower to manage the data flood, crack crime syndicate, checkmate migration from foreigners, etc. and make effective inferences from a large volume of an

accumulated dataset is a worrisome problem. For example, Nigeria has been at war with the Boko Haram Islamic insurgents for the past 10 years and recorded limited success in ending the war using the same old methods and intelligence [3]. Terrorism according to the United States experts in fighting ISIS, required engaging terrorists within and outside the battlefield [3]. On the battlefield using force such as the military while out of the field using intelligence such as Expert Data Scientists and Analysts through crime analysis, social network graphical crime analysis, Machine learning predictive models, clustering like Principal Component Analysis, and Artificial intelligence methods [16]. This study, therefore, aimed to emphasize a paradigm shift from the traditional method of information sharing and analyses to using Big Data techniques to combat crime as a threat to National Security in Nigeria.

This study stressed the need to improve the current information-sharing framework by key security agencies such as the Nigeria Police Force (NPF), Military (Army, Air Force, Navy), National Identity Management Commission (NIMC), Nigeria Security and Civil Defence Corps (NSCDC), Economic and Financial Crime Commission (EFCC), National Intelligence Agency (NIA), Department of State Security (DSS), etc., by adopting the Big Data techniques. The rest of this study is structured as follows: In Section 2 we present the related works on Big Data and national security, in Section 3 we present the Big Data systematic model components in National Security, In Section 4 we present the Proposed Integrated Big Data Model and methodological implementation framework to national security and Section 5 we Conclude the work and made recommendations.

Related work

The concept of Big data is a buzzword that encompasses modern-day data analytics framework and techniques to draw inferences from large tonnes of datasets of diverse sources, streaming in at high velocity. The interest in Big Data lies in its value, considering the rate at which the data is being generated from multiple sources [11]. At the dawn of the 21st century, user-generated content, and social media platforms such as Twitter, Facebook, and Instagram are generating more than 2.5 billion gigabytes of data daily, the big data hype is growing exponentially. Big data in this context focus on the series of analytical technologies that seek to draw insights from unstructured data that is difficult to manage by traditional approaches due to volume, velocity, variety, and veracity [9].

In modern times, the world is drastically witnessing a high rate of linkage in areas of human movement and goods, information sharing, the exponential growth and dissemination of technology, and the interconnected effects on the political, economic, and environmental lives of people. According to Babuta [4], the high level of physical and virtual interconnectedness presents a growing number of significant challenges to preventing and mitigating national and transnational security threats, while ensuring a balance between respecting individual privacy and protecting the nation from harm. The work of Chi [7]; stressed the need of adopting big data and machine-learning technologies by security agencies in nations. According to the study, the national security communities need to continuously revisit their assumptions about big data. Big-data analytics can be limited by problems of representation; information loss during data extractions and transformation, bias and discrimination; false positives and negatives; and feedback loops [7], [23]. Jin, Wah, *et al.,* [14] opined that the grand challenges of Big Data applications (namely, data complexity, computational complexity, and system complexity) posed serious setbacks to the utilization of Big Data in several organizations. Chi [7] stressed that some of the challenges to big-data analytics include overhyped expectations;

the inherent complexity of big data; the difficulty of cost-benefit analyses; data siloes and fragmentation; and the opacity of algorithms.

The work of Fidow, Hassan, *et al.,* [12] developed a novel approach that employed the use of mobile applications with big data analysis for crime reporting and prevention using aggregate data from multiple sources, the Hybrid Smart Crime Reporting App (HIVICRA). The HIVICRA is an infographic intelligent crime-reporting analysis application that incorporates crime data sourced from local police, social media, and crowdsourcing, including sentiment analysis of Twitter streams in conjunction with historical police crime datasets. An evaluation of the approach suggests that by combining sentiment analysis with smart crime reporting applications, it is possible to improve the forecasting of crime. According to Yan, Q, *et al.*, [25], many countries have opted for the use of data-driven technologies, IoT, and crime analysis to predict and handle crime patterns and logic. However, most countries underuse this technology by using conventional techniques in crime analysis. Their study further stressed that developing countries like Nigeria are yet to embrace the use of big data analytics in fighting crime but are eager and willing to adopt these techniques to minimize the rising cases of crime in the country.

In addition to the existing criminal activities, new criminal activities are taking a monstrous dimension recently in various forms all over the country and threatening the sovereignty of Nigeria. Boko Haram killings, herdsmen attack or ambush, unknown gunmen, kidnapping, smuggling, drugs, and arms trafficking due to porous borders and seaport have posed great challenges to security agencies in Nigeria. Other related cyber-crimes such as "yahoo-yahoo" or internet fraudsters, defamation of characters, fake news, etc. are geometrically rising in Nigeria [1].

According to Babuta [4], the concept of national security and today's challenges in the United States evolve around national security in levels. At the highest level, which could be considered the strategic level, nations often seek to **1)** Maintain their citizens' trust in government; **2)** Maintain their economic stability and growth; **3)** Protect their citizens' health, safety, security, and **4)** Reinforce and protect their sovereignty and position in the global community.

Though there are differences that exist among nations concerning the relative importance of these four goals, they usually can be viewed as common ground when conceptualizing national security. Berger, & Roderick [6] stated that nations usually achieve their strategic goals of national security through several objectives such as **1)** Political security, both national and international, **2)** Military security; both national and international; **3)** Protection and resilience of critical infrastructure; **4)** Border security, freedom from external coercion, and geostrategic security; **5)** Economic and commercial security; **6)** Security of the environment, natural resources, and energy.

Big Data systematic model components in National Security

Integrating information

The use of Big-data analytics technologies can potentially automate the integration of unstructured data flows from diverse sources at high speed, making them searchable and sortable [7], [8]. The use of text analytics is adopted to read physical transcripts and identify relevant textnot just keywords, but concepts, sentiments, topics, and persons [14]. Video analytics in like manner can automatically analyze the backlog of hundreds of hours of CCTV, Nigeria Army information on terrorism, threats, Police report collation across the 36 states in Nigeria, Immigration archive information obtained on foreigners, Nigeria correctional centers reports, Nigeria custom services, Federal Road safety corps, Economic and Financial Crime Commission, Independent and Corrupt practices,

mobile phones, National Identity Management Commission, Social media profiling such as Facebook, Twitter, Instagram, YouTube, drones and satellite imagery feeds and recognize and track individuals automatically. Fusion techniques such as extraction, transformation, & loading (ETL) and CDM techniques can run across the top of these analytics to fuse and standardize different data types automatically into an integrated feed of relevant information for further systematic analyses [5], [9]. Such a feed can reduce the time analysts spend collating information manually. Creating a platform for data integration is not a guarantee of data completeness, though this can create a platform to minimize crime [13] and threats to National security in Nigeria.

Standardization of Common Data Models

Common Data Models are used to enable the transformation of data from diverse observational databases into a common format with a standardized vocabulary, which can then be used to perform systematic analysis [24]. Employing the use of a standardization process improved data quality, help to increase efficiency, and facilitated cross-database comparisons to support a more systematic approach to observational research [24], & [20]. The work of Voss, Makadia,

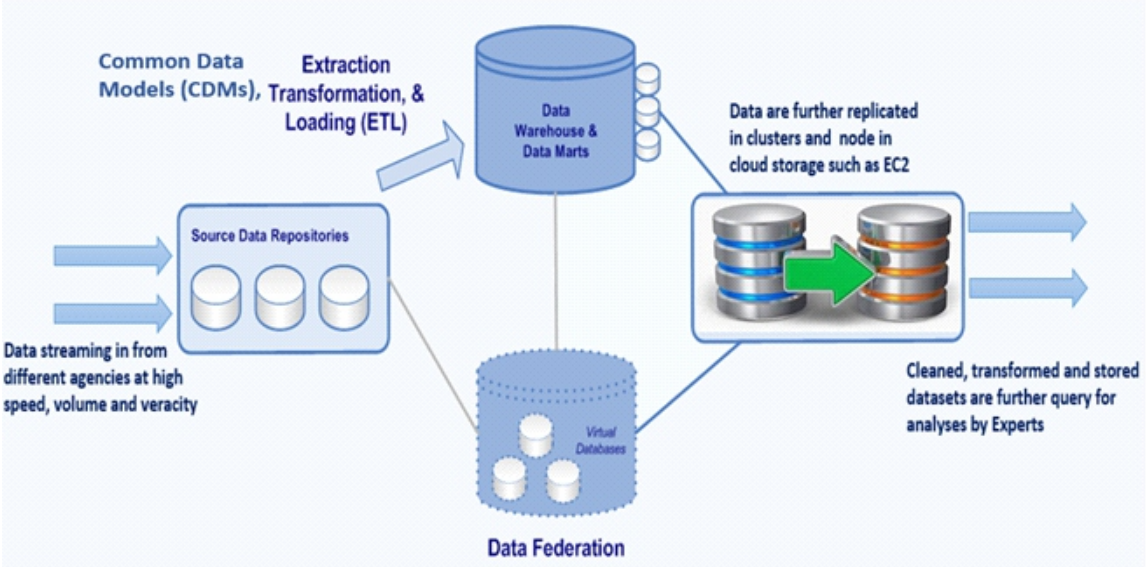

Figure 1: A cloud-based data integration platform (Extract, Transform, & Load).
Shows how datasets are integrated from different security agencies at high speed, veracity, and volume, the cleansed datasets are further stored in cloud storage such as AWS-EC2, S3, Google, Hadoop, and HDFS cluster nodes for data management, visualization, and analyses by Experts.

& *et al.*,[24] used the standardization of common data models (CDM) techniques to observational healthcare databases to standardize data structure, content (through a standard vocabulary with source code mappings), and analytics. This enables the institution under discussion to apply a network-based approach to transform the CDM which resulted in minimal information loss across all 6 databases executed in less than 2 hours. Making comparisons across diverse data sources using the

CDM approach has continued to demonstrate data quality and consistency, this can be integrated using the Big data platform for national security datasets.

Predictive analytics

Big data technologies have improved the scope and accuracy of predictive analysis in areas of crime analysis. In the private sector, predictive analytics has become commonplace in marketing [9]. Google Suggest builds "models" or "profiles" for individual users based on their search histories and other data, and then predicts or suggests auto-completion to search queries based on a corpus of past data, such as similar user profiles, past searches, and click-through patternsa predictive system that has underwritten Google's rise as a search engine giant. In national security agencies, big-data technologies can be used to build similar predictive models for threat and risk [18], [7]. Predictive analytics is not a panacea for random events full of brevity of uncertainties. It heavily relies on past data to predict future performance, extrapolating functions of best fit based on past data to determine what the future is most likely to look like. It is unlikely that it will foresee inflection points beyond the data used to construct the model [20]. Interpretable supervised predictive machine learning models such as Logistic Regression, Random Forest, and Decision trees and unsupervised approaches such as clustering and association analyses can be incorporated by experts in areas of Data Science and Statistics to infer hidden information and patterns to minimize crime from tonnes of Big Data [8].

Cloud Storage platform

Cloud storage systems consist of several storage devices connected by the network providers such as Amazon, Google, and IBM. It is typically composed of Network Attached Storage (NAS) or Storage Area Network (SAN) type of distributed storage with the feature of storage virtualization [11]. As Cloud storage is built upon commodity servers and disk drives, several cloud storage facilities are utilized to store huge tonnes of datasets collated from diverse sources. Amazon

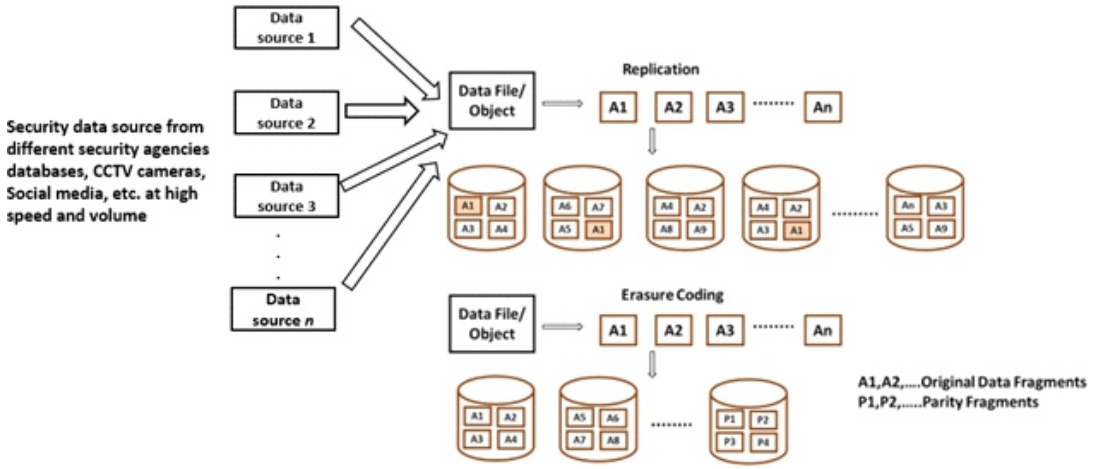

Figure 2: Transformed security datasets are replicated and erasure-coded across clusters in cloud storage facilities to avoid data loss. The data replication and erasure coding across clusters will boost data reliability, minimize memory usage that overcomes computational challenges

Web Services (AWS), S3, EC2, etc. are utilized in storing huge datasets. To avoid data failure, loss, and redundancy, data are replicated, and Erasure coding is adopted for data reliability in cloud storage [11].

Humans in the loop

Big Data when collated and stored on cloud facilities cannot be managed alone by sets of artificial intelligence and machine learning algorithms [21]. To make effective use of these tonnes of datasets been generated, there are need to form a collaborative platform by involving the skills and knowledge of the Domain Experts (security intelligence such as Army, police, etc investigative units) and Data Scientists, Statisticians, Data Engineers, Computer Scientists knowledgeable in the management of Big Dataset on Hadoop, HDFS, clusters, and nodes. These experts will generate meaningful insights from huge, diverse datasets employing data visualizations, data mining skills such as machine learning skills and artificial intelligence deep neural networks, network sciences, and textual analytics.

Hidden knowledge discovery

Analyzing a huge volume of datasets for past behavior, or data mining can result in the discovery of non-obvious relationships that can be used for predictive analysis. The manual collection, collation, and analysis of human-led mining for predictive insights have been the traditional bedrock of marketing and business intelligence approaches [18]. Modern analytics technologies can automate and accelerate the process. The increased speed and scale of analytics-driven knowledge discovery mean that algorithms can search through different security agencies' databases to discover correlations that previously escaped been detect by experts. Those correlations need to then be tested to establish causal or mechanistic links as part of a holistic theory-building process before they can be relied on for predictive modeling in certain security scenarios.

Proposed Integrated Big Data Model

This study proposed an Integrated Big Data for Security Information Sharing (IBDSIS) model that uses the CDM approach to pool and standardize datasets from different databases of security agencies and relevant organizations (public and private) charged with the mandate of handling information and services in the geographical regions of Nigeria. IoT devices such as smart mobile phones, RFIDs, wireless CCTV cameras in public places such as places of worship (Churches, Mosques, Hospitals, Schools, and Markets), Remote sensing information from satellites, GIS, and Social media platforms such as tweets from Twitter, Facebook, etc. are integrated and stored on cloud facilities such as Hadoop, AWS EC2, S3, etc. However, it is worth noting that, the citizens' data privacy rights must be taken into consideration when using the proposed IBDSIS model [25]. The services of experts from domain areas and Data Scientists are employed to manage, analyze, build interactive restful API for data visualization, and knowledge discoveries for security agencies and policymakers to utilize in the fight against the rising cases of insurgence and crime in Nigeria.

Steps to Implementation of IBDSIS Modeling Framework

This study proposed the IBDSIS model to augment the current national security architecture in Nigeria. To implement the IBDSIS modeling framework (see **Figure** 4), we illustrated using an infographic, the methodological steps to follow to fully integrate and utilize our proposed model.

To achieve the aim and objectives of this study, we proposed five methodological implementation

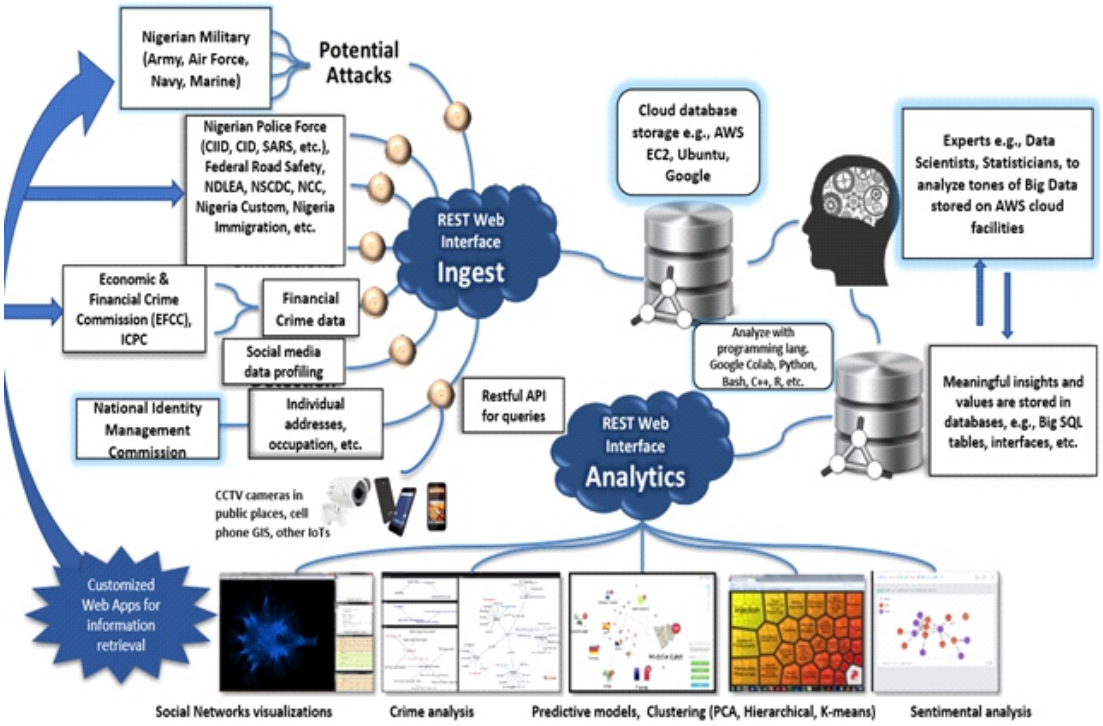

Figure 3: Proposed IBDSIS model for National Security in Nigeria

The proposed IBDSIS model will use the CDM method to standardize and integrates datasets from different databases of security agencies in Nigeria, non-paramilitary organizations, private firms, IoT devices, etc. to form a holistic platform on the cloud where domain experts and Data Scientists, Statisticians, Computer Engineers can be hired to analyze tones of data for knowledge discoveries in the fight against crime and external aggression.

strategies for integrating the IBDSIS model to augment the current national security architecture in Nigeria. **(a)** setup a data collection strategy: integration and collections of Big Data from different sources e.g., social media platforms, IoTs such as CCTV cameras, drones, RFID chips, signals, telecommunication datasets, National security agencies databases such as the Nigerian Army, Navy, Airforce, Nigerian Police force database, Economic and Financial Crime Commission (EFCC) datasets, Nigeria Immigration, National Identity Management database, Drug Law Enforcement Agencies, etc. Usually, datasets from IoTs platforms have properties such as large-scale streaming data, heterogeneity, time and space correlation, and a highly noisy unstructured dataset which can be in *HTML, CSV*, text, *JSON*, or image format. Datasets curated from databases of various security agencies are usually semi-structured and structured formats such as *CSV* using *SQL* or python query programming languages. **(b)** Data integration using ETL techniques and stored in secured cloud containers such as EC2, S3, AWS,

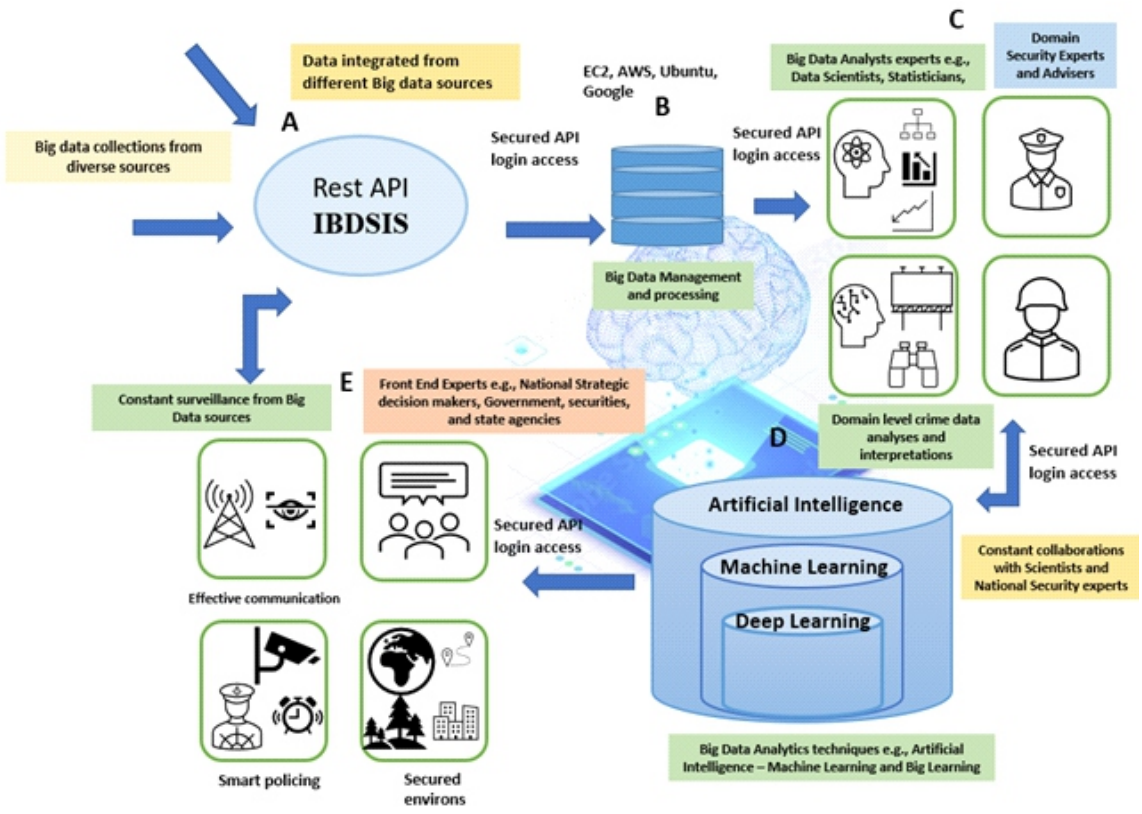

Figure 4: Proposed IBDSIS Implementation Framework for National Security in Nigeria

Google, Ubuntu, etc., which will be queried using python programming language or *SQL* by domain experts for further insights and knowledge discovery analyses; **(c)** the imploration of domain-level experts such as Data Scientists, Statisticians, Programmers, Computer Scientists, in collaboration with major security domain-level experts e.g., national security team, strategic security and policy team from state, and national level to properly ask the right questions and hypotheses, query the right dataset and implore the right analytics approaches. **(d)** here the experts (data scientists, statisticians, etc.) utilize Big Data analytical skills and techniques such as Artificial Intelligence Machine Learning, and Deep Learning methods to clean, explore and analyze big datasets of concern following threats and national security issues that seeks insights to proffer solutions. Machine Learning (ML) techniques can be supervised, unsupervised, or semi-supervised learning tasks. The supervised ML task can be further subdivided into classification or regression learning tasks. Note, that these techniques can be implemented by experts knowledgeable with cloud computing skills, infrastructure, and experience in writing lines of algorithmic codes using programming languages using Python, R, *SQL, C++*, etc. These approaches are used to analyze these large crime datasets that pose threats to national security in Nigeria and beyond. **(e)** the results of the analyses are further refined as reports, dashboards, web applications, software packages, etc., presented/training front-end users and decision-

makers to further strengthen security posts and present national security architecture in Nigeria. Artificial Intelligence and industrial *4.0* knowledge have proven to be very effective in combating crime and terrorism in developed countries, and this can be harnessed in the Nigerian context to further augment the present security architecture in Nigeria that heavily relies on traditional approaches to tackling crime.

There is an urgent need and a patriotic call to salvage the soul of Nigeria from the present security challenges that have engulfed all regions of the country. Intense collaboration between security agencies and experts in utilizing modern-day Data Analytical skills such as artificial intelligence, machine learning, statistics, mathematics, and domain knowledge may have the answers to unlocking hidden patterns from tonnes of information and the carbon digital footprint left by these culprits. Big data technology and approaches such as the proposed IBDSIS framework by this study will assist in a more efficient information sharing and profiling of targets. It is also worth noting that other innovative approaches seek an alternative to address some challenges posed by ETL techniques that this paper did not cover in-depth. Approaches such as the collocation big data model [20] can be incorporated on top of the IBDSIS proposed framework to address the issues of data loss during transformation and information sharing considering the sensitivity of security data.

CONCLUSION

In conclusion, while the new age has recorded tremendous growth in the usage of big data analytics in boosting national security architecture in developed countries, the human element and traditional approaches to tackling insecurity issues in developing countries like Nigeria have still been utilized. Considering the growing volume, velocity, and veracity of data inflow in the national security process in Nigeria, some degree of machine learning and artificial intelligence decision-making is inevitable to help prioritize crime analysis. However, automated analysis of data is not fundamentally altering, and will not fundamentally alter the need for a human being in the loop at multiple levels of national security. In recommendation, social-scientific research on big data usage in curbing insecurity in developing countries like Nigeria should focus on adapting Big Data Analytics for gathering information, storage, and sharing insights with relevant agencies. More experts in the domain of Data Science and Statistics should collaborate with security agencies to analyze and disseminate large crime datasets. Federal and State governments should build a robust national and state security architectural system that is devoid of traditional mundane methods but highly sophisticated for interactions between domain experts, Data Scientists, and machines to make them as effective as possible in tackling crime.

Future work

In the future, this study seeks to implement a prototype of the proposed IBDSIS modeling framework for a local institution/organization in Nigeria. Using the local institutional databases, CCTV cameras, RFID installations for a stipulated time frame, and social media streaming API rest dataset platforms like Twitter, and Google will be used to collect social media texts. These datasets will be dumped in a cloud infrastructural docker container for ETL transformation and analyses for relevant insights, and knowledge discoveries by experts using Machine learning techniques supervised learning tasks and unsupervised learning tasks. All codes and algorithms will be written and implemented using python programming language and SQL query languages.

Conflict of Interest Statement

No conflict of interest was declared.

Contributors

All authors agreed to be accountable for this study and made contributions through conceptualizations, drafting, and revising of the manuscript, and proofreading the final work.

REFERENCES

[1] Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. *The Electronic Library*, *26*(5), 716-725.

[2] Al Chukwuma, O., & Francis, O. (2014). Banditry and crisis of public safety in Nigeria: issues in national security strategics. *European Scientific Journal*, *10*(4).

[3] Anyadike, N. O., & Nkechi, O. (2013). Boko Haram and national security challenges in Nigeria; causes and solutions. Journal of Economics and Sustainable Development, 4(5), 12-23.

[4] Babuta, A. (2017). Big data and policing: an assessment of law enforcement requirements, expectations and priorities. Royal United Services Institute for Defence and Security Studies.

[5] Bansal, S. K. (2014, June). Towards a semantic extract-transform-load (ETL) framework for big data integration. In *2014 IEEE International Congress on Big Data* (pp. 522-529). IEEE.

[6] Berger, K. M., & Roderick, J. (2014). National and transnational security implications of big data in the life sciences. *New York, NY: American Association for the Advancement of Science*.

[7] Chi, M. Big data in national security: online resource.

[8] Chimezie, U. C., Ivo, A. S., Eziechina, M. A., & Uche Daniel, C. (2019). Database Integration In Nigeria: A Case For Improved Security And National Planning. Database, 6(11).

[9] Diouf, P. S., Boly, A., & Ndiaye, S. (2018, May). Variety of data in the ETL processes in the cloud: State of the art. In 2018 IEEE International Conference on Innovative Research and Development (ICIRD) (pp. 1-5). IEEE.

[10] Endert, A., Hossain, M. S., Ramakrishnan, N., North, C., Fiaux, P., & Andrews, C. (2014). The human is the loop: new directions for visual analytics. Journal of intelligent information systems, 43(3), 411-435.

[11] Esomonu, N. P. M., Esomonu, M. N., & Eleje, L. I. (2020). Assessment Big Data in Nigeria: Identification, Generation and Processing in the Opinion of the Experts. International Journal of Evaluation and Research in Education, 9(2), 345-351.

[12] Fidow, A., Hassan, A., Iman, M., Cheng, X., Petridis, M., & Sule, C. (2019). Suggesting a Hybrid Approach: Mobile Apps with Big Data Analysis to Report and Prevent Crimes. In *Social Media Strategy in Policing* (pp. 177-195). Springer, Cham.

[13] Folarin, S. (2021). Corruption, politics and governance in Nigeria. In Nigerian Politics (pp. 377-394). Springer, Cham.

[14] Jibril, M. L., Mohammed, I. A., & Yakubu, A. (2017). Social media analytics driven counterterrorism tool to improve intelligence gathering towards combating terrorism in Nigeria. In ideas (Vol. 107).

[15] Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and challenges of big data research. Big Data Research, 2(2), 59-64.

[16] Kim, G. H., Trimi, S., & Chung, J. H. (2014). Big-data applications in the government sector. *Communications of the ACM*, *57*(3), 78-85.

[17] Li, L., & Jiang, L. (2020, April). Research on City Public Security Administration Based on Intelligent Policing. In *2020 International Conference on Urban Engineering and*

Management Science (ICUEMS) (pp. 692-695). IEEE.

[18] Machina, A. A., & Songjiang, L. Crime Analysis and Intelligence System Model Design using Big Data. *International Journal of Computer Applications*, *975*, 8887.

[19] Nachiappan, R., Javadi, B., Calheiros, R. N., & Matawie, K. M. (2017). Cloud storage reliability for big data applications: A state of the art survey. Journal of Network and Computer Applications, 97, 35-47.

[20] Obilikwu, P., & Ogbuju, E. (2020). A data model for enhanced data comparability across multiple organizations. Journal of Big Data, 7(1), 1-25.

[21] Ogbuju, E., Taiwo, K., Ejiofor, V., & Onyesolu, M. (2018). Big data driven e-government framework in Nigeria. Bayero Journal of Pure and Applied Sciences, 11(2), 252-259.

[22] Oghi, F. E., & Unumen, J. O. (2014). Military intelligence and the challenge of national security in contemporary Nigeria. International Journal of Research in Humanities and Social Studies, 1(2), 7-13.

[23] Overhage, J. M., Ryan, P. B., Reich, C. G., Hartzema, A. G., & Stang, P. E. (2012). Validation of a common data model for active safety surveillance research. Journal of the American Medical Informatics Association, 19(1), 54-60.

[24] Voss, E. A., Makadia, R., Matcho, A., Ma, Q., Knoll, C., Schuemie, M., ... & Ryan, P. B. (2015). Feasibility and utility of applications of the common data model to multiple, disparate observational health databases. Journal of the American Medical Informatics Association, 22(3), 553-564.

[25] Voss, W. G. (2016). European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting. *The Business Lawyer*, *72*(1), 221-234.

[26] Yan, Q., Chen, W., & Poor, H. V. (2018). Big data driven wireless communications: A human-in-the-loop pushing technique for 5G systems. IEEE Wireless Communications, 25(1), 64-69.