REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Electrical And Computer Engineering

APPLYING SPSS METHODS TO ANALYZE CYBERSECURITY RISKS IN POWER SYSTEMS AND INDUSTRIAL CONTROL SYSTEMS

Ali Abubaker ABULSHOROUD

Master's Thesis

Supervisor

Asst. Prof. Dr. Muhammad ILYAS

İstanbul, 2025

APPLYING SPSS METHODS TO ANALYZE CYBERSECURITY RISKS IN POWER SYSTEMS AND INDUSTRIAL CONTROL SYSTEMS

Ali Abubaker ABULSHOROUD

Electrical and Computer Engineering Department

Master's Thesis

ALTINBAŞ UNIVERSITY

2025

The thesis titled APPLYING SPSS METHODS TO ANALYZE CYBERSECURITY RISKS IN POWER SYSTEMS AND INDUSTRIAL CONTROL SYSTEMS, prepared by ALI ABUBAKER ABULSHOROUD and submitted on 25/12/2025 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

Asst. Prof. Dr. Muhammad ILYAS

Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Muhammad ILYAS	Department of Computer Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Software Engineering, Altınbaş University	_____
Assoc. Prof. Dr. Ali HAMITOĞLU	Department of Computer Engineering, İstanbul İstinye University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Ali Abubaker ABULSHOROUD

Signature

DEDICATION

I dedicate this thesis to Asst. Prof. Dr. Muhammad İLYAS for his guidance, direction and patience to complete this work.

ABSTRACT

APPLYING SPSS METHODS TO ANALYZE CYBERSECURITY RISKS IN POWER SYSTEMS AND INDUSTRIAL CONTROL SYSTEMS

ABULSHOROUD, Ali Abubaker

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Muhammad ILYAS

Date: 12/2025

Pages: 75

Cyberattacks can significantly undermine public confidence in organizations, disrupt financial operations, and result in significant financial losses. The purpose of this research paper is to explore the relationship between ROA, efficiency in operations, and cybersecurity through descriptive and inferential statistics. The study was conducted in two rounds at various locations mainly at the significant commercial and industrial hubs of Libya. The initial phase had been conducted, where 58% of respondents were aged between 25 and 35 years, while 24% were aged below 25, and 18% were older than 35 years. During the second phase, a significantly greater proportion of participants (84.3%) were under 25 by 9%; and, correspondingly, only 6.7% of participants were over age 35. The correlation analysis showed a strong positive association between profitability, operational efficiency and cybersecurity in both periods. In the first phase, profitability was positively related to both operational efficiency ($r = 0.806$) and cybersecurity ($r = 0.657$), and all correlations were statistically significant ($p < 0.01$). Similarly, the second phase also showed strong positive correlations with profitability, operational efficiency ($r = 0.862$), and cybersecurity ($r = 0.732$), confirming the robustness of these relationships over time.

Keywords: Cybersecurity, Effectiveness, Operational, Profitability, Security.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

AD	:	Advantages
AI	:	Artificial Intelligence
APTs	:	Advanced Persistent Threats
BD	:	Big Data
BDA	:	Big Data Analytics
BI	:	business intelligence
DDoS	:	Distributed Denial of Service
EDR	:	endpoint detection and response
GDPR	:	General Data Protection Regulation
HIPAA	:	Health Insurance Portability and Accountability Act
KNN	:	K-Nearest Neighbor
MFA	:	Multi-Factor Authentication
Mgmt.	:	Management
MLP	:	Multilayer Perceptron
Orgs.	:	Organizations
ROI	:	Return On Investment
Sig.	:	Significant
STR	:	Strategic
SVM	:	Support Vector Machine
Tech	:	Technological

1. INTRODUCTION

In modern times, it is legitimate for cybersecurity to protect both company and national interests. This refers to the protection provided to digital data and basic infrastructure from various threats and vulnerabilities in cyberspace, which are supposed to be advantages (AD) of digital technologies [1]. As organizations (Orgs.) become increasingly dependent on digital operations and interconnected systems, there are more frequent and sophisticated attacks [2]. However, cybersecurity challenges are not limited to technology; they also encompass human behavior, as it is worth noting that the most significant (Sig.) risk comes from human error or negligence [3]. Security threats from insiders, especially those with privileged access to systems or exploiting previously unknown vulnerabilities, are among the most dangerous, often causing even more damage than external attackers [3]. Cybersecurity needs to be in every employee's heart and mind if its defense structure is supposed to be rigid, or else leaders on the least-off would not bother with the issue. In IT resilience, it is not so much the business itself as important services required by the society such as government, public safety, and economy [4]. Thus, at present, the national cyber security policy stands as one of the pillars of modern-day defense policies. Countries such as Turkey [5],[6], India, Singapore [7],[8], and Estonia [9],[10] have developed STR framework objects to enhance cyberspace security, While international agencies, such as ENISA (2012) [11], NATO (2012) [12], and the ITU [13] (Evre & Ciylan [14]) have a primary role to play in the relevance, agility, and robustness of the above.

Modern digital transformation (DT) works at big speed on all types of businesses, and with companies continuing to digitize their business processes-increasing dependence on networked technologies-further-more business assets is now vulnerable to complex cyber threats. These cyber predators are racing to keep up with tech challenges,fueling a fluid and treacherous security landscape [15]. In such a situation, the importance of prescriptive and proactive cyber security Management is Felt. These should range from an assessment of risks to how you would respond if an incident did occur, plus a defense-in-depth fender with multiple layers of guards[16], [17], [18].

On the other hand, Big Data (BD) has transformed the way companies work and apply STR. In reality, however, big data-as-three Vs (volume-variety-velocity [18])-are transforming a

class of software once known as Business Intelligence (BI) systems into real-time predictive Analytics engines [19], [20]. But managing big data securely is proving difficult, particularly for cities where data nearly always needs updating. Actually BI systems must be performant, but they also should ensure data security and data integrity.Therefore, it is crucial to incorporate cybersecurity awareness partially for BD and BI systems. More sophisticated attacks are ransomware, phishing as well AI-based which have an ability to expose sensitive information and the performance of the organization [21]. The conventional security methods of talk-and-block, embodied for example by the firewall, are a thing of the past: it's time to create new and innovative ways of performing security work. Compromise in any of these two domains will result in significant financial losses, reputational loss and punitive fines if [22], [23].

Furthermore, a successful cybersecurity has a relationship with organization key performances such as financial performance, business continuation and sustainability [24], [25]. Performance, which takes ROI or Profit Margins and Net Income into account, grows more dependent on the effective handling of digital risk. Productivity (operational efficiency) - simply the output/input ration: cybersecurity also has a significant weight of productivity [26].

Societally, the greater dependence on internet services for education, business, governance and entertainment requires that we be all the more attentive as a nation to cyber hygiene For example, Libya with 88% of households having internet access by early-2024 thus making it imperative to have cybersecurity/security awareness [27]. However, even in the case of minor mistakes such as falling for phishing or mishandling personal data, this might end up being disastrous [27].

1.1 AIM OF THE STUDY

Goal of study is to provide information on how prevention is successful against organizations in urban China and illustrate the call for stricter cybercrime legislation to guard our privacy and sensitive data which enables businesses in a more and more digital society.

1.2 IMPORTANCE OF THE STUDY

The progressive integration of business intelligence into the BD, in truth, has created a revolution in terms of competitiveness and activities. But Urban city institutions have the responsibility to take their own steps in order to protect that such sensitive data from potential cyber threats.

1.3 PROBLEM OF THE STUDY

The studies explore how the threats of data security affect Misurata companies when they purchase anti-cyber assault (DDOS, Phishing, and Malware etc.) solutions. What is abundantly clear is that traditional security will never be effective in mitigating these rapidly evolving risks and protecting companies against a data breach or cyber crime.

Creating holistic cybersecurity policy to manage the particular risks posed by BD in business intelligence systems may enable companies operating within Misurata to protect their data and thus become competitive in a digital environment. The analysis will also recommend cybersecurity practices to mitigate threats.

2. LITERATURE REVIEW

2.1 BIG DATA

BD's meaning includes complex data, large amounts of data, or heterogeneous members whose standard processors can hardly work on them in order to store and analyze them. What constitutes "large" depend of circumstances or person handling the dataset. It typically denotes certain measures or volumes too large to be able to address how traditional-systems can manage [29].

Wu et al. [30] provided one of the earliest definitions of BD as "a massive heterogeneity, of data originating from separate sources, distributed, decentralized and controlled in which complex relationship extraction is sought". This view welcomes the scale, variability and even the superposition of BD. Data can be from any sources, are showcased in real time and data themselves interact in complex ways that the traditional systems cannot deal with.

In order to get further insights into the pathogenesis of BD, Wu et al. [30] formulated the HACE theorem (heterogeneous, autonomous, complex and evolving data properties). This theorem states that BD is massive and heterogeneous, the studied relations are changing. That kind of complexity and scale does not serve well in traditional database Mgmt. systems designed for processing data.

Similarly, Manyika and colleagues [31] define the BD as "collections of datasets that are so large and complex that they become difficult to work with using on hand database management tools or traditional data processing applications". Put another way, what this definition really underscores is that both the size and complexity of BD frequently make older tools and technologies obsolete when it comes to Big Data, very often necessitating the creation of new systems to contend with it.

New tools and techniques have emerged for large datasets processing in BD, leading to the concept of BDA which uses specialized instruments to process, analyze and extract patterns from big heterogeneous databases. It is not like the classical methods of data manipulation, structured data and fixed queries, BDA will include machine learning, natural language processing, predictive analytics among others. Transition from its predecessor to the BD technologies represents a Sig. mismatch of the data they were developed for each systems

process. Traditional systems were prepared for structured, well-defined datasets, whereas systems designed around BD should handle data that is often scarcely structured and in real-time. This gap between the technologies available today and those that are required by the modern data environment underscores the need for an excellent BD platform that meets the diverse and growing demands of data processing. Table 2.1 gives characteristics comparing traditional data Mgmt. versus BD Mgmt. [29].

Table 2.1: Comparison of BD vs Traditional Data [29].

Traditional Data	**BD**
Here, the data is "Structured" data.	Here, the data is "Unstructured or Semi-structured " data.
The size of the data is tiny	The size is more than the traditional data size
Here, the data is Centralized.	Here, the data are distributed
It is easy to work or manipulate	It is challenging to handle the data
A typical system configuration is sufficient to process	High system configuration is required to process the data
A traditional database. The tools are enough	Special kinds of tools are required
Standard functions are enough to manipulate the data	Requires a special kind of function to manipulate the data

With this massive increase in data volumes, challenges arise in efficiently processing and handling these massive amounts of data. Moving from megabytes to gigabytes, then to terabytes, and finally to petabytes and exabytes requires unconventional research in data Mgmt. The colossal size of data being sprawled everyday needs specific solutions and technologies to handle its growing complexity as well the fast growth. The transition to BD technologies from traditional data Mgmt. systems is primarily driven by performance and processing concerns. Structured data is defined as data that is precisely organized and can be categorized into tables and rows, which is what database systems are designed for. However, a Sig. proportion of today's data is unstructured such as text documents, social media posts, images, videos, and sensor readings making processing large volumes of unstructured data a Sig. challenge, as it does not fit within the rigid structures of traditional databases. As it grows, the need for new and advanced technologies to process and analyze this type of information will increase [31].

2.1.1 The Synergy of Business Intelligence and Big Data Analytics

Today, the business world runs on massive loads of data that no previous era could match in volume and complexity; this is what one might call the BD era [32]. BD, the volume of heterogeneously large, high-speed datasets that Orgs. must handle daily, sees an immediate rise in numbers generated by digitization, the number of devices connected to the Internet, and the rapid growth of online platforms. Today, large volumes of misunderstood BD are outgrowing the volume discussion in a qualitative dimension: Transformation in organizational decision processes with business transformation in real value creation and value extraction [33] evolved. Some of the traditional data processing systems were for example designed with small, narrow and structured data in mind, that just don´t fit an increasing amount of what BD needs are nowadays. Companies are seeking to adopt new age data processing systems that bring insights from these diverse forms of data. It's what the 3Vs (Volume, Variety and Velocity) framework connotes it makes obvious how such an unprecedented scale that data comes to be generated by enterprises like yours, and processed for targetted services for your customers - there is value associated with this. The impacts of BD on the firm are broad; firms that are adept in processing or analyzing information may gain competitive advantage with identification of wider scope for opportunities both future oriented and as incremental refinements to performance today [19].

Meanwhile, BI was also expected to evolve along the direction of increasing complexity of BD. For instance, BI was past-oriented and merely descriptive of what had happened. Today, the rational BI systems of BD environments have gained more proactivity and future orientation through real-time analytics and predictive modeling efforts [34]. Further along, this evolution has indeed made BI more than just an aggregator, since it now includes features for integration, data quality management, and advanced-analytics processes [35]. Moreover, modern BI platforms allow one to use several data sources to provide a unified means of analyzing in both structured and unstructured formats in order for decision-makers to obtain a wholistic picture of the enterprise landscape when forecasting events for more STR planning.

BI can proudly claim to have watched the democratization of business unfold; this was an application once considered exclusively in the realm of IT departments, whereas now it is a concept that explodes beyond all departments within the organization, throughout the whole enterprise [36]. Rapid, self-service BI tools such as Tableau or Microsoft's Power BI have made it possible for the non-technical generalist to do their own experimentation with data and analysis. This democratization accelerates discovery, reduces reliance on IT, and establishes a shared culture of data and evidence across companies. Offering this perspective on a relatively equal footing, organizations then enjoy far more agile responses to shifts and trends within the context of a market [37].

This merging of BI with BD has also led to certain analytic tools being developed to process large amounts of data and derive any meanings. Delivering intelligence Constructed for the STR vendor, these aren't those standard reporting tools you used to use; in fact, they're more like machine leaning algorithms that take an action based on what has been learned. Analytical tools like these are critical to Orgs. seeking to derive value from their data assets [37].

Standard Reporting and Querying Tools: Although new analytics are getting everyone's attention, traditional reporting tools and SQL based querying and report generation has been central part of the BD market [37]. They are still the go-to for relational database data searching and historical reporting. These tools are used by BI platforms, such as Tableau and Power BI, to create interactive dashboards that show the trends and headline figures in the data. The huge difficulty that has in BD tools to deal is due to the high amount of different sources of data and specifically with unstructured or semi-structured data [37].

Advanced Analytics: There is a stronger motivation to use more advanced analytical methods such as Orgs. probably the latter," but find one another Get to know your first responder dates. Descriptive analytics informs a business of what has happened in the past, and diagnostic analytics burrows into the reasons why things happened as they did. As predictive analytics applies statistical and machine learning techniques to foresee the future trends and possible events, predictive models give rise to being insightful on the expected changes in the market, customer behaviour, and the corresponding impending dangers. Advanced analytics is the prediction of future trends by the prescriptive approach that gives what are the steps to take on a decision [38].

Machine Learning and Predictive Modelling: Current BD analytical tools have evolved in respect of the dominating rise of machine learning algorithms to such an extent that systems can discover patterns from data and act without explicit being programmed with algorithms [39]. They now have the capability for addressing complicated issues like nonlinear relations in the data, being particularly powerful for unstructured forms of data like text, image, or video. Both supervised learning (most certainly in classification and regression) and unsupervised learning (as clustering/correlation algorithms to allow apparatus finding patterns which were not immediately apparent) [39].

Prediction Modelling: Any scenario planning or decision making will be heavily reliant on prediction models and frameworks being established. Predictive analytics allows organisations to understand which of a range of factors are impacting the future, and predict customer needs, make better supply chain decisions, and implement data-driven marketing. This will have a more drastic impact on finance, health care and e-commerce applications where better predictions imply competitive edge[40].

BI along with BDA is a probability for larger changes, where issues, frameworks and their anticipation switch abruptly. This is a very special mix of technology that is here presented to corporation by A.B.S as one in a million opportunity to stand over the roar of huge databases from all over around, and enable an easy ground for market/consumer orientated navigation. Utilizing BI and BDA as the fusion means not only a technical transition, but is also interpreted as a strategy, encouraging the companies to do better than others in certain target market. [19]

And a look at markets the world over. Orgs. have to date been derived for the BDA and BI. At all levels it provided deep insights and made the traditional fragmentation analysis to move towards dynamic real-time monitoring. BD characteristic of high volume and variety such as it has transactional data, social interactions, web accesses, or reports from other external market resources enable companies to throttle real-time market trends processes [41].

As the result of on-the-fly market relationship tracking by BDA/BI technology, Retail Orgs. really well can also reveal; these businesses were able to track the number of units sold in real time so that no unit could ever be over-sold. These Orgs. are able to use public opinion

in social media to monitor price strategies of competitors and adjust their inventory practices based upon forecasted demand [42].

This data supports informed decisions in furtherance of the Org. have a more positive influence in shaping institution to encapsulate the changes of market only after they have occurred. This expectation serves as the foundation for marketing as business very fast players, by which it outperforms rather torpid competitors [19]. Study Consumer Psychology Even You studying and understanding the consumer is not an option, it's a requirement. BDA helps to unpack complex patterns and preferences hidden in a great bulge of data, being useful addition to BI. In the past, only rudimentary transactional information was employed to understand customer behaviour. Today, in this era of social media analytics and user generated online activity as well as consumer generated feedback, Orgs. be paid more attention to their preferences and behaviours [43].

Quick And Efficient Operation: The combination of BI with BD also enhances operational efficiency. The single one and only touchstone of this is true for any company on the face of the earth which wants to continue in a digital age. And they can justify this operation to optimize resource usage and reduce wastage on real time data processing of big volume granular data. In supply chain Mgmt. this integration could be proved very beneficial. For instance, analysing supplier performance, market demand and logistics data enable companies to have real-time visibility of the supply chain operation and thus to optimize inventory levels and lead time/shipping time while mitigating stockout /overstock risks [44]. Greater visibility saves money, and creates operational flexibility that allows a firm to be more responsive to customer demand. They can also support HR departments by optimising recruitment procedures, pinpointing talent deficiencies and/or improving workforce efficiency e.g. through analysis of employee performance data, records or engagement metrics [19].

2.1.2 Big Data in Smart Cities

The development of BD has progressed quickly in recent years, and been accompanied by challenges with respect to cybersecurity more generally, but particularly within the space of Smart Cities. BD can be characterized by 3V model; Volume, Velocity and Variety that means big data consists of large volumes of data in high velocity way with multiple

heterogeneous types. Nevertheless, traditional data processing is under threat in the presence of these types of features; therefore, addressing data storage, analysis and protection systems had become intricate [45]. Inspired by that work, Holubová et al. [46] further suggested two additional characteristics, canonical veracity and data value, where the former represents how closely of a record quality is associated with a truth or fact, and the latter refers to its worthiness on owned data items resulting in a new 5V model. Recently, new dimensions were added to capture the dynamic and ever-changing nature of BD, by introducing its validity (that is the time till the data remain valid "over time") and volatility (the time till the cyber evidence remains extra-corpus "at rest") [45], [46]. Here, the term smart cities can be considered as being extremely alarming since BD represents one of the main “pillars” on which urban governance and public services are grounded. Smart cities are living things, the organic body using technology (the IoT and sensorsito data-driven decisions on service performance, life quality for citizens and sustainability). But such a scenario would lead to the production of vast amounts of data and thus has led to concerns about privacy. No one is going to want his or her private information and privacy compromised via data breaches, cyber-attacks and unauthorized access. Meanwhile, people’s personal data related to their movement, health and daily activities is getting quickly abused for potential identities’ theft, fraud and for surveillance [47],[48].

Velocity arises when data is generated with IoT devices and sensors in Smart City– the more rapid it’s produced(te time-related processing), the more this data continues to be making the traditional security model obsolete or showing all its weakness[49]. Indeed, scale demands proportional need to implement cyber defense capabilities (for example real-time encryption algorithms, mechanisms ensuring lower data disclosure rate and techniques to anonymize data), which can be simply retrofit into what makes smart cities smart while at the same time support privacy as well as operational efficiency [50], [51], [52].

Additionally, there are socio-technical issues in the form of the regulatory and governance landscape \remove{which} also may hinder market uptake of data protection solutions. This is reinforced by Bellanova and De Goede [53] who posit that whether effective or otherwise, embedding a national or local legislative structure can be weighty in determining how any data protection discourses become framed. Certain cities are facing a weakness in data management, which is that there’s a still that “mismatch between their infrastructural

environments and required infrastructures" (DuBuisson), undermining the actual implementation of devices for protecting privacy. Furthermore, smart cities are becoming something entirely new as they confront new technologies and threats. Given this contextualisation, increasingly imbued with these concerns, data protection and privacy policies would need to be flexible so as to respond sensitively to the local society-techno-cultural configuration; also technological responses should fit into societal perspectives [54].In fact, smart city visions will strongly differ in scale, from the national and regional to the local area ls level: they are city-specific strategies defined for using ICT and data for urban development. If infrastructure-focused strategies concentrate on the material aspects of our urban life (mobility, energy and waste Mgmt.), soft infrastructure investments put the human side center stage with investments in inclusion, knowledge exchange or social innovation [55]. This fast track to development is a great opportunity for Smart Cities as well however, may be an important element that will make the differences: guaranteeing their strategy matches both – the tightening of technology and the tightening of regulation on security, inclusiveness opinion Welcome another product android. Integration of frameworks for sustainable development should also address urban challenges, overall economic social, and environmental problems [56].

Ethical and social implications of the BD challenges in Smart Cities have to be dealt with. Heavy reliance on pervasive data collection systems raises potential surveillance, privacy, and data governance issues [57]. Heavy e-gentrification due to the digital-infrastructure and data-planned cities benefits diversion is even more concrete at present. It puts today's socio-economic disparity on the edge, mostly with peripheral urban communities that are already deprived, and deepens them [59].

2.2 CYBERSECURITY

Often confused with information security, cybersecurity actually concerns itself with all material properties even transcending the scope of all information security to include asset and human protection. The human factor in the security and information areas is mostly rendered as human contribution in the process of developing security. This gets another dimension in cyber security: the human as possible target-or even blindside attacker-of a cyber-attack. The other normative dimension would be the view regarding the protection of these especially vulnerable groups such as children as the duty of society as a whole [60].

The 'cybersecurity domain is evolving from a predominantly technical issue to a global focus-it engulfs issues of national security, economics and public safety as a consequence. Already, more than fifty countries have adopted national stances on cybersecurity and cybercrime in cyberspace, reflecting an emerging appreciation of the need for secure digital infrastructure. Consider the United States, which has implemented a broad-based cyber-security strategy that is loosely based on general international co-operation and mutual response to global cyber-threats [61]. And the UK too has promised Sig. funding and has pledged to spend £650 million over four years under the National Cybersecurity Programme, to safeguard its digital environment [62].

However, the difference between cybersecurity and information security is often not taken into account, and both terms are used repeatedly without a clear definition in academic literature as well as policy papers. In its simplest form, information security deals with the Mgmt. of data and information systems in order to prevent (among other things) unauthorized access or use of data and systems while still providing access to those who are authorized to have it. Security is important, yes, but it's more about the security of particular data or organizational systems and infrastructure than it is about the inhabited ecosystem. Cybersecurity, on the other hand, is more macroscopic and considers a suite of assets across the entire digital environment to address security risks throughout cyberspace. The International Telecommunication Union specifies these as core objectives of cybersecurity (ITU-T X.1205, 2016): availability, integrity and confidentiality. Availability: systems and data must be available when needed. One either possesses the right to alter information or not; this is what integrity actually stands for. Privacy means the protection of what is sensitive from the reach of unauthorized capability. Falsified transactions may lead to either false transactions or both. Indeed, authentication and non-repudiation have emerged as the new constraints in the scope of contemporary challenges in cybersecurity-the most critical dimensions in establishing the credibility and accountability of electronic transactions and communications. The boundaries of these categories are unclear, but they should also be taken into consideration in devising responses. Cybersecurity is, in fact, a much broader concept than information security, whereas information security is Customarily viewed as mostly part of ICT (Information Communications Technology) concerning the protection of data by contrast, cybersecurity involves a compartment of problems ranging from the

security of physical infrastructure to human resources and the efficient functioning of cyberspace as such [60].

2.2.1 The Intersection of Big Data and Cybersecurity

This is the decade of coming together with BD and cybersecurity in an era of escalating complexity and attacks. DT has sprinted and especially in the current coronavirus disease 2019 (COVID-19) crisis, business-as-usual operations have swiftly transitioned online – subsequently creating even more data. Such a limitation dramatically reduces the efficacy of conventional methods to counter or detect cyber-attacks. Therefore, several researchers have attempted to enhance cyber security through the application of BDA and machine learning algorithms [64].

Hashmani et al. [63]. proposed an ensemble approach to BD security, showing that it outperformed traditional classifiers such as K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Multilayer Perceptron (MLP) [64]. Using a benchmark dataset containing 3.2 million records, distributed across major email providers, it allows for the blocking of 7,000 spam and phishing URLs per day. This focus yields particularly effective results for distinguishing between benign and malicious activity. Furthermore, the authors, who express a desire to expand their work by discovering threat actors, contribute to improved security.

Ashish Bajpai et al. [65] describe the AD of BD analysis compared to traditional cybersecurity approaches. Illustrator, like BD, can manage large volumes of data and volatile data about online work through datasets of social networks and smart devices in its functionality [65]. Lifecycle analysis of BD obscures the steps of creation, processing, and output using technologies such as Hadoop and NoSQL databases, and machine learning algorithms such as MapReduce for anomaly detection, fraud detection, and fraud prevention. Interventions are examples. This article focuses on the potential of BD analysis to overcome the limitations of traditional approaches for managing large, dynamic data sets.

In the work of Sunita Satpathy et al. [66], the potential of BD in digital forensics was emphasized, mainly arguing that single-classifier-based methods cannot handle large amounts of data in cybercrime investigations [66]. Later, it was proposed to exploit BDA to handle massive amounts of data in criminal investigations, with the introduction of Hadoop

tools, machine learning algorithms, and decision trees for rapid analysis. These works underscore the need for integration of BD to predict transparently and efficiently throughout the conduct of a digital forensic case. Faheem Ullah and Muhammad Ali Babar conduct a systematic assessment of BD cybersecurity analysts' systems to pinpoint common quality attributes and architectural styles. The authors further analyzed the limitations of legacy cyber-security tools for processing unstructured data or, rather, revealing advanced persistent threats (APTs).They presented a fusion- based digital forensics model that would need to be improved by integrating BD tools in the proposed model for better cyberthreat analysis and prevention.

Bellin et al. [68] identified different applications of BDA for cybersecurity, such as unified data representation and zero-day attack detection [68]. They presented the real-time analysis, dimension reduction, and event sampling in Cyber Security Operations scenario. The authors further studied the ways to use BD tools for efficient threat detection and prevention across heterogeneous systems.

Similarly, Jiajing Chen et al. [69] emphasized the importance of AI methods (like machine learning, deep learning and statistical inference) in cybersecurity analysis [69]. They proposed a next-generation firewall design which includes AI algorithm with automatic intrusion and malware detection. They also show how AI can shrink the design of algorithm, hence minimizing the human effort needed to find cyber threats. Ledong et al. [70] reviewed the issues related to implementing cyber security in advanced manufacturing systems, with a focus on Internet of Things and cloud integration [70]. They explored system weaknesses, such as software accessibility and physical security problems and suggested cloud-based solutions.

The cybersecurity also change the logic level and apply BD to monitoring, response (detection) and prevention is being applied. Timurlui and Jackson [71] targeted the BD applications for automated analysis in support of Orgs. detect threat in a timely fashion and as a result, lower the frequency of security breaches [71], they particularly concentrated on log monitoring and data compression techniques for attack prevention, showing a Sig. reduction in security breaches as a result of implementing BD solutions.

Roberto et al. [72] studied the application of BDA in automated cybersecurity decision-making and proposed a four-step research methodology that included data ingestion, correlation, anomaly detection, and automated threat detection [72]. They demonstrated how integrating BD into cybersecurity processes improves threat identification and reduces response times. Their work formed the primary basis for the development of subsequent automated security systems.

By combining analytics and centralized models, Mitic et al. [73] delved deeper into some of the concepts of cyberattack prediction, detection, and prevention [73]. They recommended Apache Hadoop and machine learning algorithms for the analysis of bulk datasets to determine patterns and create reports for strengthening countermeasures.

Roopa Goje and Dadi Ramesh [74] suggested the amalgamation of different models such as online constant examination and event processing models like Esper and Hadoop for real-time cyber threat detection and prevention [74]. Through the use of these models, their collaborative detection system improved threat identification that could be later expanded to incorporate more complex attack scenarios.

2.2.2 Comparative Analysis of Big Data on Cyber Security

This section presents a comparative analysis of BD analysis on cybersecurity, as shown in Table 2.2

Table 2.2: Comparative Analysis of Big data Analysis on Cybersecurity.

No	Title of Work	Authors	Description
1	An Ensemble approach to Big Data Security (Cyber Security)	[75]	An ensemble approach for BD Security was used, and it was shown to be most accurate compared with single classifiers
2	BDA in Cyber Security	[76]	The author recommended using BD. Analytics instead of the Traditional Approach due to a massive amount of data that is changing from time to time, and also due to the sensitive nature of the data
3	BD Computing Application in Digital Forensics Investigation and Cyber Security	[77]	The author has also discussed the usage of tools in Digital Forensics, and also designed Forensic Investigation model
4	Tactics for BD Cybersecurity Analytics Systems: A Review	[67]	Authors have proposed a new technology to overcome the limitations in traditional cyber security tools by means of BD Cyber Security Analytics Systems
5	BDA for Cyber Security	[68]	The author has imparted the importance of BDA in Cyber Security to handle unified data representation, zero-day attack detection, and data sharing across the risk detecting systems, real-time analysis, sampling, and dimensionality reduction, system constrained data processing and time series analysis for anomaly detection
	AI-Driven Cyber Security Analytics and Privacy Protection	[69]	The author has proposed a next-generation firewall that includes an automatic intrusion detection system, encrypted traffic classification, malicious software detection, and so on, using the applications used by AI-Driven cyber security
	BDA and Cybersecurity for Advanced Manufacturing	[70]	The author has proposed a Cloud-Based Design and Manufacturing (CBDM) to work on the cyber secure platforms.
	BD and Cyber Security: Contemporary Issues	[73]	The author has proposed an infrastructure combining a complex, analytical, and centralized model with high-speed ingestion, to identify the change in pattern and to generate a report to improve the security in cyber systems
	Designing a Collaborative Detection System for Detecting Threats to Cyber Security in BD	[74]	The author has collaborated on five models, such as Esper, Hadoop, Agilis, Storm, and Spark, for security threat identification.
	Data and Deep Models Applied to Cyber Security Data Analysis	[78]	The author has developed a new technology, such as BD Platform (BDP) and Lexical Link Analysis (LLA).

The frequency and sophistication of cyber-attacks have escalated significantly, driven by the rapid advancement of digital technologies. Malware, viruses and such other cyber threats are getting more sophisticated which has shown the increase in their level of difficulty to detect

and control. In contrast to this, BDA is being considered as a new promising tech solution for improving cyber security. By analyzing large volumes of data in real-time from multiple sources including network and system logs, BD improves the speed and accuracy of threat identification [64]. As much as modern cybersecurity can be transformational, this is what BDA offers with signature improvements as far as threat detection, prevention, and response are concerned. Nevertheless, successful execution of social engineering must be preceded by resolving the pressing technical and ethical challenges [64].

2.2.3 Cybersecurity Threats in Business Intelligence Systems

Cybersecurity attacks increasingly face organizations installing BI applications to tackle BD. These systems are meant to serve better decision-making with insights derived from vast and complex datasets, which makes them an attractive target to cyber criminals. BI systems are likely honey pots for hackers due to the diverse information they manage- from customers to intellectual property. Research shows that organizations implementing BI platforms are battling strong cybersecurity threats, including data breach, malware attack, insider threat, and APTs [79]. Each of these threats carries its risk with the potential to severely halt the business and expose sensitive data.

The ramifications of these cybersecurity attacks pose heavy effects on BI systems, and in some instances, the damages can be catastrophic. When data is breached, possibilities for damage control- embarrassment and otherwise- arising from sensitive customer records or financial details or your proprietary trade secrets could prevent culprits from inflicting harm, both in the short term and permanently. The real costs of data breaches are incalculable: from here onwards, lost revenues and damage control funds and for marketing better. Organizations can incur colossal fines, especially those subjected to laws that enforce strict data protection regulations, such as healthcare, finance, and e-commerce. GDPR, on one hand, applies in the EU, while on the other hand, HIPAA imposes hefty penalties on organizations that fail to safeguard personal information adequately in the US [80]. These regulations, also a common thread, with an added cautionary note-whoever compromises the business intelligence (BI) systems and organization is liable under the compliance issues of data protection regulations. And, on top of that, a BI environment under attack from malware and APTs has far-reaching consequences. The APTs could go unnoticed for a much longer duration while compromising the integrity of the business intelligence systems. Such attacks

are typically discovered later in the kill chain, when counteracting such threats becomes very difficult. These types of APT also pose a serious risk from an organizational perspective in terms of competitive positioning and general operational security, as not only do they represent direct data loss, but also expose business processes and system services put under the stress of threat when integrity of business intelligence (BI) is put under question [81].

Insider Threats can generally be classified into two: malicious and unintentional. Those employees with a smidgen of access who are inadvertently linked to data with an external situation pose a severe threat to a BI solution through their ability to potentially harm an organization, either purposefully or by accident. After very few moments contemplating a wealth of sensitive information flowing in business intelligence systems, establishing strong access protocols and training for all employees (for that matter, audits as well) becomes clearly evident. One erroneous action, for example, a false positive, or an ill-timed credential leak can morph into widespread cyber attack [82]

With all these threats troubling the mind, any Organization should put serious attention into a more proactive approach to protecting against business intelligence systems. Strong and proven encryption protocols, multifactor authentication for all users, and constant active monitoring to detect suspicious activity in real-time and respond appropriately should all be part of a solid strategy. On an organizational level, an incident response plan should be drawn up that ensures swift reaction to any breach or attack. Regular auditing and revising of BI software system should be done the same way as it does for other training for staff of every enterprise that needs to be in place for defense. If effective, these two modes of prevention will keep vulnerabilities from being exploited and decrease the probability of a successful attack [79].

2.2.3.1 The evolving landscape of cybersecurity threats

Cybersecurity has both threats and counteractive measures which seem event metamorphosing rapidly. As we all know, technology progresses, and so does the technique and the tools used by the cybercriminals; thus, vigilance becomes crucial for Organizations. The figures in the following are indicative of holistic evaluation on escalation of threats including enterprise cybersecurity [83].

Rising amounts of cyberspace attacks: Cyber- attacks are now a near continuous threat where a new hacker attacks every 39 seconds [84]. Historically, the first trend of alarm is polymorphic malware that keeps changing its code in deployment to escape detection;95 percent: of orgs. since 2019 are in there. All these repetitive changes should make it more and more complicated for time-based defense to rely on that these things would catch them off-guard [85]. About 30 million new estimated malware attempts were thought to grow until 2018, and this growth did not relieve much in terms of frequency and sophistication of attacks [84]. The re-infection is again disappointing at a steady rate of 50% of attacked devices. About 93% of these companies reported at least one serious cyberattack, thus making Spain the country most affected in 2018 [80]. [86].

The techniques in cyber-attacks are advancing: Newer techniques now entail cryptocurrency mining and abuse of encrypted channels-phasing old tactics like ransom ware. Due to its 400% increase last year, cryptojacking stands on the fast track, where a hacker uses an unwitting victim's computer to mine coins like Monero and Bitcoin. With this kind of attack, criminals have higher returns but less risk than a traditional ransomware attack and would find it easier to perform [87]. A recent example is Smominru botnet, which has affected over 500,000 Windows machines that could mine Monero with revenue of 3.6 million USD [85].

On the other hand, supply chains projects suffered massive assaults at 78 percent with regard to the year 2018-as given to the fact that the interconnected systems are truly vulnerable. These attacks are initiated on a weaker partner to penetrate bigger systems via trusted channel [88]. Malicious Attack Vectors: Well-known attack vectors still exist against business houses. Approximately 63 percent of the breaches involve vulnerable passwords and usernames, thus placing emphasis on securing authentication [89]. Malicious documents made up Word, PowerPoint, and Excel files made up 38 percent of total dangerous attachments worldwide; next came compressed archives (. zip and. jar) and PDF files, respectively [90].

Internet and online shopping do these businesses, indeed making them more susceptible to attacks. So if anything it's the smaller ones that feel more threatened by online sales risks – the majority of whom which have malware implanted to their websites in some way. We are seeing this as an artifact of the greater threat surface that businesses now have it is no longer only digital infrastructure but customer-to-business interactions [88]. Cloud Security

Troubles: Cloud computing is now essential to conducting business, but it's not without putting businesses in the line of fire. 91% of those using the cloud, for example, reported that their applications have been compromised in some manner; 82% said they do not know what security pro-cesses protect them and are placing responsibility with the provider. These are apparent for necessity practice to companies even for clear and Strick security models in containing the cloud environments not exposing confidential information [91].

What's Next for Cyber Crime: Trends indicate the cybercrime industry will continue to adapt, experimenting with new strategies and avenues of attack. Another newcomer, the fileless attack, which evades detection by running directly in memory rather than files, gained Sig. momentum in 2018. Given that fileless attacks accounted for 77% of successful cyberattacks, the situation is expected to worsen as attacks become more sophisticated in the future [92].

On the contrary, developments have brought new threats, despite the decline in attacks using financial Trojans.. Zeus, Emotet, and other financial malware evolve and still pose some Sig. threats to financial transactions and sensitive data [84]. With the increasing use of open-source tools for malware development, it is now easier for both amateur and professional hackers to launch sophisticated attacks [85]. As shown in Table 2.3

Table 2.3: The Most Popular Attacks of the Years 2014, 2015, 2016, 2017, and 2018 [87],[92],[94],[95],[96],[97].

Threat	**Place by year**				
	2014	2015	2016	2017	2018
Malware	1	1	1	1	1
Web-based attacks	2	2	2	2	2
Web-app attacks	3	3	3	3	3
Botnet	4	4	5	8	7
DoS атака	5	5	16	6	5
SPAM	6	9	7	16	6
Phishing	7	8	6	4	4
Exploit kits	8	16	11	14	--
Data Breaches	9	11	12	11	8
Physical attack	10	6	10	10	10
Insider threat	11	7	9	9	9
Information Leakage	12	13	14	13	11
Identity theft	13	12	13	12	12
Cyber Espionage	14	15	15	15	15
Ransomware	15	14	8	7	14
Rootkits	16	10	4	5	16
Crypto jacking	-	-	-	-	13

The ENISA Threat Landscape Report [92]. periodically analyzes the dynamism of cybersecurity threats, highlighting the dominant and Sig. threats to Orgs. in 2018. Among these, cryptojacking attacks emerged as a Sig. threat for the first time, while exploit kits, which were among the top four threats in 2012 and 2013, disappeared from the list. This shift reflects a general shift in cyberattack tactics, with cybercriminals increasingly turning to financial motives such as cryptojacking and ransomware against individuals [92].

Between 2014 and 2017, the cyberthreat classification underwent only minor changes, with relatively little change in the ordering of threat categories. Notably, mobile threats included malware, web attacks, and web application attacks. These were the primary threat types, while the rest were secondary. However, this may be changing, as reports indicate that the impact of insider threats and cyber espionage, which recently gained prominence as categories in 2014, have received Sig. attention as a result of increasing threats by insider and state-sponsored adversaries [96]. Categorization in these factors is defined against a range of elements associated with how often they occur and of the impact and relationships to other cyber threats [84].

This is knowledge that will matter to Orgs. to invest in their network security solutions first.prompt. Cyber threats are clearly more than merely Technology problems; they are more psycho-social than technical. Threat origins have strong ties with human behavior and motives. The cyber-attack underwriters are the cybercriminals, insiders and terrorist groups. Most of them operate in secret, under cover identities, while attacking the softest systems. But attackers often just don't bother (NewSky Security reports). This implies that being aware of the nature of threat actor can aide in coming up counter measures against them [92].

Moreover, the particular attack vectors that allow or initiate an attack are so that one can advance the claim of a single warning actor. To manage the spread of threats and respond to incidents, we must first understand the vectors. The ENISA Threat Landscape Report [92] lists some typical attack vectors such as browser hijacking, malicious e-mails, app stores for mobile devices and USB devices. By these vectors, malware installation or the installation of malicious payloads, hence opening a way for unauthorized access by the attackers into the system. It is time that organizations start to do wide-ranging risk mitigation with STR considerations in an environment of increasing sophistication of cyber threats. Ransomware and cryptojacking are two of the most significant types of malware in the last few years.

WannaCry and NotPetya are ransomware that encrypted user data and tried to demand a ransom to unlock it. Irrespective of the fact that the motive could be financial, some measure of sabotage is carried out by exploiting, for example, known vulnerabilities (such as EternalBlue [82]). Cryptojacking, meanwhile, is a subtle threat that leeches users' computing power to mine for cryptocurrencies. Another new issue now is that of the increasing phishing threat. According to the ENISA Threat Landscape Report 2018,95% of Malware and two-thirds of Data breaches in Organisations come from successful Phishing attacks. These attacks prey on human instinct and take advantage of trust and curiosity to collect sensitive data like logins and, in some cases, even bank account numbers. Enterprises ought, therefore, to consider staff training with respect to being able to recognize phishing attacks and improved email filtering performance as well as the availability of MFA [83].

Similarly, the emergence of Internet of Things presents difficulties in terms of cyber security associated with botnets. These types of activities in some context might include botnet attacks, such as the well-known 2017 malware Mirai attack that launched a large scale DDoS through vulnerable- IoT devices which enforced enhancing security frameworks for IoT-based contexts [98]. These connected devices, as part of the Internet of Things, represent a particular kind of threat because they can be compromised and used to amplify an attack, although without many security prescription. Thus, an Org. ensure that all such devices are properly protected and actively watched over[84].

Organizations must be vigilant on new Threats that have come about constantly to stay ahead of the game. Enterprises must combine old-world security solutions (firewalls and anti-malware apps) with new-generation EDR views of actual time monitoring & attack management. Of course, mostly important to lock down the cloud-hosting infrastructure because that is also what most of Organizations are tending towards these days. So it is crucial to incorporate this perspective with threat intelligence on cloud security knowledge and have continuous monitoring and updating for defending against attacks. In other words, the understanding about cyber-threats: what a threat is composed of; why threat actors threaten and how they attack are really vital to make cyber-defenses against these threats. This kind of insight is what will let a great organizer become an effective defender. Feasting upon this constantly-evolving threat landscape are (yep) Orgs. have to fine-tune security

posture to counter these threats and put in place appropriate defenses, be they technology or staff discipline, that will mitigate the exposure [84].

The threat agents concept is relevant when examining elements of cyber-attack(s). These individuals or organizations are armed with resources and motives to constitute, carry out and induce threats against digital systems and networks. Threat agents are usually divided into three main classes: Cyber Criminals, Company Insiders, and Terrorist Organizations. Cyber Criminals are the most common threats corresponding to monetary gain. Some of them use highly sophisticated means to commit their evil deeds, for instance, data theft or ransomware deployment. Yet, company insiders may even outplay by far as they have been provided legit resources inside the organizations then can exploit for their benefits or sabotage the company itself. In the end, there are terrorist organizations that have now made the cyberspace the new front of their warfare for worldwide influence and are trying to destroy national or foreign infrastructure for a given ideology or policy [99].

Immensely varied in interests, the attackers have one thing in common; the tools and techniques that they apply can be tracked by security professionals for making predictions regarding their next move. For example, studies indicate that cybercriminals extensively share attack tools and infrastructure with state actors or internal personnel, except that their motivations result in subtle variants in usage. That understanding is helpful because it feeds the prediction of attack patterns and hence leads to developing countermeasures. Attack vectors are the ways and methods of execution the malicious attackers used in launching attacks. It explains how an adversary would enter into a system or network by exploiting security vulnerabilities on either a device, a software, or human behavior. It becomes very important for Orgs. to know the surfaces on which attack can take place, so that would help them in understanding the workflow of an adversary, which may turn out to be beneficial in incident response and prevention [83].

Common attack surfaces include hostile attacks against web browsers, phishing emails, threats from mobile application stores, and malicious USB devices, all of which carry their problems for detection and mitigation. Web-based attacks can be conditions in which hackers compromise weaknesses in browsers or their plug-ins to send phishing emails that trick users into giving information or following malicious links. Nowadays, a mobile store application concept is gaining immense popularity. Attacks use malware disguised as legit

applications and can result in serious data leakages and full system compromises. USB Drives are perceived as vectors because plugging one into a machine can allow for injecting malware. Knowing the threat types and attack vectors would assist the Org. in the dynamic threatscape through having a more tightly integrated, defensive capability to try to leverage. Security awareness training; advanced effective defenses; and well tested incident response are all that stands in between you and these attackers. By remaining vigilant to these threats and taking a proactive stance, Org. can reduce the likelihood of falling victim to a cyber-attack [83].

2.3 BIG DATA AND BUSINESS INTELLIGENCE (BI) IN URBAN CITIES

Industry infections soon raced from the plowed field simplicity of olden time life to nightmares industrial swarms in countless throngs. Steam engines continued to target barriers that had previously divided cities in social and geographical terms: the city was henceforward a megacity outflowing along the ridges. Urban life in the late 1800s was redefined yet again by electricity and telecommunications that reduced geographical distance while shaping both a new environment for acquaintance and one (he believed) that had preserved many facets of face-to-face[111].

All technologies converge onto such communication crossed geographical distance(s)[112] and were designed to set networks from distance100 This type of technology, like the Internet would bypass at each barrier in forming social ties [100] [115]

Efforts to apply computer technology and personal digital devices were incredibly effective in reconfiguring the way cities operate in the post-World War II decades. This Tech evolution means cities can now collect vast quantities of data from all sorts of places, harvesting the ground for what we have since dubbed “smart cities”. Therefore, the urban systems are more and more handled with the real-time processed big data based-AI to dynamically achieve the optimization in traffic management, energy consumption, public security, environmental surveillance or other applications. This paradigm is based on BD, involving unstructured, semi-structured and structured information found in different sources. There are five critical dimensions of BD, referred to as the “5 Vs” that include volume, velocity value variety and veracity. Volume describes the variety of data available from urban-scale sources that is gathered within various city activities, such as social media

posts, data collected by sensors like traffic and environmental conditions. Velocity also refers to the speed at which data is generated and processed—information is streamed continuously, even now, from smartphones, sensors and cameras for example. Value is the result associated to the data in how easily it can have been used for decision-making, including anything from better flow according traffic software up to prediction needs in our infrastructure. There is a large variety of data, including text, image, audio and video data that have to be analyzed differently for insightful results. Valid means the extent to which a method measures that what it purports (accuracy); confirm, that is, to relate and demonstrate correspondence between all method data enabling results to be interpreted (reliability); correct – validate: securing needful (actionable) information [99]

Urban problems, such as traffic congestion, housing shortages, flooding, and environmentally related natural disasters, have been exacerbated by new technological advancements and rapid urban growth and density. These problems have intensified the challenges of urban infrastructure and governance in developing regions, including China. A new model of urban management would be required, not factoring in the three dimensions of these challenges: physical space, social space, and cyberspace [101]

So technically, reimagining urban planning is a game-changer: it is no longer just about thinking in terms of physical space and social interactions, but also about putting in cyberspace, which encompasses the flows of data over the internet and other digital infrastructures. In this situation, smart cities are a way to deal with the problems of fast urbanization. These urban areas apply various technologies (IoT, cloud computing and AI) to observe and control the functions of cities. Based on urban BD, cities could promote public service delivery, infrastructural development and support sustainable urban systems. As Guoji Li (2015), academician of the Chinese Academy of Engineering, appropriately referred to it – "Urban BD could possibly make a role contribution like what honey bees do for agriculture when they cause crop productivity by pollination; technology caused urban system effective function as supported by BD" [102].

Urban BD, as opposed to general BD, represents information produced by the physical and social systems of a city. Urban BD covers both dynamic and static information of various types (urban facilities, transportation, public service and individuals) from diversified sources. The data obtained can be applied to an array of tools, such as resource allocation

management, urban planning and decision making. Crucially, it incorporates the visibility of what cities do in fact, using academia to arm decision-makers with a more science-based and data-driven approach towards city Mgmt. [103].

Urban BD has its own particular characteristics besides the common five Vs, such as hierarchy, integrity and correlation. Traffic, etc. have data types on city to share the cross-cutting analysis of info on urban matters and hence provide some explorations about aspects of the city [103]. These characteristics call for further processing and analysis. One solution to the challenges of urban BD defines how data are extracted. As a result of that the first stage of this extraction process consists in gathering huge amounts of data into an unspecialized "datahold",where after some kind of cleaning and pre-processing job over these dirty data to identify it's not-normal behaviour, (e.g. initial cleaning for their analysis). And, statistical / machine learning methods such as linear regression, random forests and artificial neural networks are later employed on this processed data. The resulting understanding is visualized and interpreted to guide next steps in urban planning and policy [104]. Applications of BD in urban development are increasingly being introduced in the cities to leverage innovation. The network of smart cities is comprised from a combination of sensors, devices and informational systems that collect work in real time to observe the functions on urban20. Nowadays AI and other emerging technologies are already in place to structure city systems in order to be efficient, sustainable, and resilient. BD can help a city to address some critical urban challenges, such as traffic jam,pollution and energy consumption, with the aim of improving life quality for residence Facilities Public service delivery Buildings [101].

Meanwhile, smart-city applications are increasingly framed in the light of IoT devices and back-end cloud communication networks for BD integration and application such as that in transportation, health care or public safety. For example, in the transport domain, BD may reduce traffic congestion by monitoring real time trends and adapting signals accordingly. In the health domain, BD might be utilized for predicting outbreaks and providing enhanced healthcare using analysis of health-related records in association with environmental factors [101].

Urban BD is more and more applied to the analysis and solution of actual problems occurring in the cities. This information covers the full range of urban activities — from plumbing

and commute times to public health and shopping — and contains real-time snapshots of how cities function across sectors. Thus, it is very important for the building of a smart city, urban sustainability and responsive governance. In order to efficiently process and utilize such a large dataset, it must be classified in accordance with the data source as well as urban Mgmt. Aims. Urban BD is a versatile and complex resource which can be categorized into various categories according to the source, utilized methods of processing and potential use. These categories serve as data structure for urban planners, businesses, politicians, and inhabitants to find empowering subsets of the status quo and transitional states toward safer streets more easily (see 2.4).

Table 2.4: Cases and User Groups for Urban Big Data Of Five Types.

Type	Example	User group
Sensor data on urban infra-structure and moving objects	Internet of Things; sensor system for managing environments, water, traffic, fuel gas, and buildings; mobile phone; monitoring camera	Public and private urban operation and Mgmt. Orgs.-zation, independent information & communication technology (ICT) development personnel, engineering science researchers
User data on society and human	Participatory sensing system, social media, network use, global positioning system (GPS), and online social network	Private enterprises, customer-centered public Orgs., independent developers, data science, and urban social science researche
Governmental administration data	Public administration data on transactions, taxes, and revenues, payment and registration; basic public data on population, traf-fic, lands, housing, and geography; confidential microdata on personal employment, medical treatment, welfare, and education	Public data: innovators, hackers, and researchers Confidential data: governmental data institutions, urban social scientists who are committed to research on economic and so-cials, public health, and medicine researchers
Customer and transaction record data	Storage card and business records; fleet Mgmt. system; customer data; data on public utilities and financial institutions; product purchase and service agreement	Private enterprises, public institutions, and independent developers, and data science and urban social science researchers
Arts and humanities data	Text, image, audio, video, language data, artistic, and material culture, digital object, and other media	Urban designers: historical, artistic, architectural, and digital humanities Orgs.; community Orgs.; data sci-entists and developers; and private Orgs.

The importance of urban BD in shaping and building cities is growing very significantly. The rise of smart cities creates the requirement to structure and interpret the heterogeneous data flow within city life. BD in the city is regarded as a distinctive information spectrum formed by various types of sources, such as physical systems, economic events and social activities. A lot of this information is big, messy and semi-structured and its use must be done in an organized manner. Urban BD is often codified into multiple systems, which accentuate the various levels of urban life and governance [106].

"urban supply-side functions" as one example of a framework for classifying urban BD. Urban administrative systems based on these frameworks collect urban data created by public departments, infrastructure Mgmt., and service delivery systems. The key utility of these data is that it can give us an idea about the way cities and hence city services (for they are mainly provided for select parts of cities) are spread within those. In this context, data can be of categories such as public transport services, health care service and educational system. Our goal is to develop organizational innovations that convert data into information governance structures, which will in turn improve resource allocation and service delivery [107]. Urban demand, on the other hand, is for BD urban municipal services; residents and businesses are potential stakeholders in these services but also non-profits and one level of government. The service preferences, service usage, satisfaction with the services of the city in general is captured in data from these queries. Cities, as a result, can learn the concrete needs regarding application service systems from urban BD users [106].

2.3.1 Applications of Urban Big Data in Urban Development

A recent BD trend in urban indicates a notable shift for city wonders and construction, leads to opportunities for fine-grained understanding of the urban systems. But who said that inquiring about the functioning of a city and its transformations33 must consist only of monstrous investigations?Similarly, It also opens up possibilities for enhancing a city's competitiveness at the international level within a rapidly changing information society [109]. In the DT era, BD has become an STR resource for cities to mine underutilized sources information and alternative mechanisms of economic growth and development [110].

For any city facing such an environmental challenge, the extent of new opportunities that becoming BD at scale, depth and breadth would open up would be increasingly a function

of its ability to harness it. Well organized data resources could lead to massive social and economic benefits of the CI systems in urban crescents, increasing the efficiency of services systems and raising the living standards for its cohabitants. BD could illuminate trends in these urban sectors (e.g., transport, habitat, education and health), improving urban planning efficacy, public service delivery and resource exploitation [111]. In addition, the capabilities facilitated by BD encourage sharing, integration and joint use of the factors of production which results in innovations on the way firms and government address urban challenges [110].

Big Data has been shown to be crucial in enabling urban resources management, and also for the initiation of an economic transformation with new business frameworks and development nodes [110]. For example, BD can to help the cities to enlarge new type of business models as well as flow factors of production (i.e., capital, labor and technology). Accordingly, it aims to maximise core values by building on strength in cities' economies and developing a sustainable system that can embrace change [112]. This shift is not merely confined to the private sector but also involves governments. However, BIG Data has the potential to contribute significantly to governance for data-driven policy making rather than prolonged interests of the people[113].

What is more, through the use of BD, also governments can expose such relationships that would normally remain hidden during classical analyses. These ostensibly unrelated data sets would be tied together in a BhD presentation of urban planning and governance as something far more dynamic and in-the-moment. Sorting the decisions' with heavy socio-economic environmental implications [114]. " Thus, BD is very relevant to the diagnostic for urban development; hence, policies are supported through qualitative and quantitative analysis that go straight into significant developments in government's administrative abilities to face multifaceted social issues as well [111].

Secondly, BD could contribute to Urban Studies by enrich the knowledge of urban models and processes of urbanisation into a positive direction. By interacting with both the structured and unstructured data they have access to, cities can perhaps enter this world more dynamically: better managing their resources in ways that people become used to underpinning a more effective engagement of urban populations. This participatory governance is instrumental for urban policies to be more inclusive and better adapted to the

reality of different people in different situations. BD promotes the encounter and understanding of urban life, and rational planning as far as cities can be planned but also an advanced reasoning on policies for a sustainable urban development [113], [33]. Finally, BD as a part of urban governance enables more intelligent and efficient dispatching of cities that are capable to adapt to the challenges posed by the 21st century and catch opportunities presented by the 21st century [113], [33].

2.3.2 Role of Business Intelligence in Decision-Making in Urban Environments

Urban contexts are simply not an option when it comes to BI for environmental management decisions. With such a tool, organizations can develop better infrastructure to compete in bus/public transport services that are smart and sustainable while further specific benefit objectives that are likely to differentiate them from competitors. Big data thus helps track and reduce environmental harm and also helps achieve sustainability goals. It has become important to integrate business intelligence within an organizational environmental management system to minimize environmental impact, optimize resource use, and comply with environmental laws [114].

Business Intelligence Business intelligence (BI) is a term for technologies and practices in the collection, integration, analysis, and presentation of STR-related data to end users [115]. BI is a fundamental domain for environmental Mgmt., that activities according to massive and sometimes automatically collected information (such as energy consumption, waste generation, CO2 emissions as well other important environment metrics business companies need). BI leverage data - but applied to what? (analytics, this element)/what for?Data used in such models are not representative of data seen by the model when it was deployed as described here The how/why behind business intelligenceFailed attempt to let business "make sense" out of Big Data / BI and make production-readyHappens to be about Like every major technology trend (such as AI or big data) there's some ambiguity on who Business Intelligence exactly Orgs apply advanced analytics like predictive modelling and machine learning to discover valuable insights from troves of their Big Data. Orgs. environmental performance [116].

BI improves environmental Mgmt., with complete information system and real time identification of problems. BI sorgt durch Echtzeitüberwachung und kontinuierliche Bewertung fü:r proaktives Vorgehen bei einzelnen Umweltrisiken, wie z.B. einem Unfallschadens im Betrieb oder Rohstoffknappheit. It would have been far easier to enforce the immediate cessation of environmental damage, and that full compliance with the most recent regulatory initiatives [117]. It allows the development of data-informed sustainability policies for a company, that can project ambitiously how much any business should measure its progress by extrapolate over them available in literature KPIs and benchmarks [114].

The benefits of artificial intelligence (AI) include: addressing biodiversity, engaging stakeholders, improving transparency, enhancing governance, managing risks, and monitoring performance. AI is also applied in studying the implications of these responses. In a reciprocal manner, when environmental responsibility is affirmed, it creates mutual accountability between organizations and relevant stakeholders regarding environmentally related behaviour. Furthermore, transparent communication about environmental performance fosters trust among leading companies, particularly with their investors, the community, and regulators. This builds a positive reputation and contributes to global competitiveness [117]. Indeed, people are becoming more aware of how companies can support their environment. This enables multinational corporations to develop global agendas at a time when companies with strong corporate social responsibility are under increasing pressure [118].

Sustainability is not simply about sharing business profits. An acquired advantage rests on the fact that these activities are presently deemed compulsory for a business hoping to balance environmental conservation with its' pocket. At present, companies are forced to deal with environmental challenges such as climate change, the depletion of resources and pollution – which many of them have a Sig. threat not only to an already threatened world but also to future businesses[118]. With the addition of Business Intelligence, companies are able to log every type of waste that is emitted into the environment then comparing by using different age equipment or technology, finally when making a purchase their priority is how the new tool aids in becoming sustainable. Such dual attention to sustainability and profitability ends up helping operations, while at the same time creating new opportunities for companies that innovate, since they can now take advantage of market openings due to

the increased demand for green products [115]. sustainability in business operations as a growing regulatory or legal liability the imposition of metaphorical environmental cuffs and ankle-snappers. With the civil code and legal norms released by the government, problems like taxes on carbon emissions and sustainable reporting are gaining importance; as a consequence, there is more demand for efficient and rigorous enforcement of this legislation. Here, companies are forced to utilise BI for their own benefit in order to comply with the environmental legislations [116].

Businesses for their part now have the instrument in BI to optimally apply insight to all Environmental standards from modern to nascent into the future. The integration of BI into environmental Mgmt. frameworks will be a Sig supplementary task. shift from the conventional qualitative intuition to a systematic, data-driven one. For long time, environmental Mgmt/ has been concentrated on manual data collection tools and subjective judgments that have delayed a company's ability to monitor its environmental performance and based decisions (Negro & Mesia, 2020). When applied, BI had transformed this land by presenting timely information, that is considerate choice-making and gradually achieve truly efficient and responsible practice of environmental stewardship [117].

BI has been recognized as an indispensable instrument for making Mgmt. of the environment more efficient in the dynamically evolving urban areas. One important reason for combining the BI system with Mgmt is that we can keep the real-time data on pm environmental condition, and analyze them. Sensors, IoT devices and remote monitoring can help make Orgs more efficient. to track various environmental indicators, such as air and water quality, energy use, waste generation and carbon emissions [119].

Today, business intelligence (BI) tools can integrate, refine, and apply company data, providing valuable insights for those working within an organization to measure environmental performance and identify opportunities for improvement.

Predictions and modeling are used to assess environmental impacts. These analyses help predict energy consumption, resource requirements, and environmental concerns. Companies can also be proactive by anticipating their risks and opportunities and predicting the environmental impact of positive behaviors in terms of sustainability, based on historical data. Enhanced BI-based functionalities can also be leveraged to improve transparency and

accountability in environmental reporting. BI provides real-time, synchronized control and accurate reporting on centralized systems to ensure compliance with industry requirements and best practices [37]. Furthermore, BI solutions create interactive dashboards and reports to present real-time environmental performance data to stakeholders. Internally and externally, regulators, as well as investors and customers, have access to information about a company's sustainability efforts its success stories. In the corporate environment, integrating business intelligence (BI) leads to a learning organization and more fact-based decision-making. Environmental data is becoming globally accessible to decision-makers at every level of the organization, both now and in the future, fostering a culture of transparency in decision-making. BI tools facilitate better interdepartmental collaboration, enabling teams from different functions (such as operations, compliance, and finance) to work together toward shared environmental goals. This collaborative environment not only enhances sustainability efforts but also improves resource efficiency across the board [120].

However, perhaps most importantly aside from its actual role in environmental management BI's ability to uncover environmental threats and opportunities. By leveraging data from multiple sources, from field sensors and organizational databases to internal monitoring systems, BI can help reveal an organization's full environmental footprint. Through retargeting, organizations can use predictive modeling and advanced analytics within BI systems to understand climate change risks, resource scarcity, and other environmental challenges [120]. For example, multivariate analysis and big data volatility analysis powered by business intelligence tools can predict the negative consequences of severe weather events, enabling organizations to take steps to mitigate these risks. Predictive analytics can also be used to help identify environmental assets (such as energy optimization and production process improvement) as a step toward both sustainability and profitability [120].

Optimal resource utilization is also a key objective of business intelligence. Resource utilization metrics, including energy and water consumption, as well as raw material consumption, are tracked and interpreted using business intelligence tools that identify a key area of focus. For example, by linking consumption to energy production, business intelligence systems can alert users when a resource is being wasted (such as a delay in consumer production or inefficient use of saved energy). We are here to guide these people, so we invest heavily in foresight to empower operations to control those operations to

maximize their efficiency and value across all their resources. You can also use predictive analytics within a business intelligence tool to forecast future resource utilization based on market trends, weather changes, and demand fluctuations. This, in turn, reinforces the importance of accurate performance forecasting for proactive resource planning to avoid waste, thereby saving money and reducing environmental burden[116]

Business intelligence (BI) tools are also crucial for monitoring and reporting on environmental assessments. These programs can provide information from various sources, offering a more comprehensive view of a company's environmental performance. Leveraging advanced data visualization capabilities, BI tools present complex, multidimensional datasets and their interpretations in an easily understandable narrative format on screen, making it easier for stakeholders to comprehend environmental data and take action.[121] Thanks to their adaptability through predictive modeling and real-time monitoring, AI systems can be efficiently managed for environmental monitoring. The ability of BI tools to analyse data will enable the organisation to monitor the environment and identify any aberrations from the natural environmental norm, and take corrective action on an instantaneous basis. In addition, these BI systems will be an essential tool to achieve full environmental reporting automation so that the reports needed for compliance with regulations can be calculated correctly and on time [121].

Tech development for smart cities grows directly with the velocity of BI systems adoption. Smart cities promise to enhance urban Mgmt, and the quality life of their citizens. This is an extraordinary time where the importance of this decision making is extreme as it demands some immediate and reliable transmission of factual information. With the widespread use of business intelligence projects in urban areas, smart cities have a greater tendency to pursue better quality of life for their citizens. The point is that with energy consumption, traffic and waste Mgmt. The key author of the term business intelligence was Dresner [122] who became evident one thing – its role does not come down merely to improving decision making processes Turing effectiveness up just any middle or large company but also to optimising working efficiency when it comes of both public and private sectors.

The major elements of business intelligence system are data warehouses, which regularly refreshing and storing the data by applying the ETL (Extract, Transform, Load) process. ETL jobs should work to ensure data is good and usable for decision makers. So long as

data has been well-cleaned and structured according to a specific format, it can be visualised using advanced visualisation utilities (for instance, in the form of pivot tables, charts or dashboards), where raw data can then be turned into decision insights and packed around natural idioms which do not require too technical knowledge on the part of clients [123].

So that the economies of cities and corporate leaders would have even more knowledge for making rational decisions at better times. It is however quite clear that capabilities of BI systems are for sure a main feature had by successful Orgs including smart cities based upon the history. The sig for accessibility of fully integrated and condensed data with BI has been facilitated Responsiveness sig. to policymakers, because it allows them to spend more resources and time on development of STR interventions instead of examination of data [124]. Combine this together, and even more becomes possible, as ERP systems that retrieve information quickly and are cost-effective to maintain are beneficial to a business. A good example of this can be seen with Kraft Foods, who implemented SAP Business Objects BI 4.0 in 2012. The company stated that through BI-software, staff could more easily retrieve all the information within the ERP-system and companies using for example EK-budget The reports became a turning point of their own higher education institution and in this way facilitate that students remain departments [125]. But as the success and business benefits of BI systems become increasingly well-known, those applications are likely to function less as a means for pulling data –- and be more about the future: in advanced predictive analytics and decision making. For instance, Oracle Business Intelligence (BI) software has several more sophisticated applications that analyze and simulate historical and real-time data. This would enable firms to anticipate the future developments and take an action (Yılmaz, 2010). In the area of financial reporting and risk analysis, banks, for instance, can use BI systems to ease data analysis procedures, report in compliance with regulations and improve (operational) efficiency [126].

What is more, are not in any need of services to inject Business Intelligence into organizational systems. Foremost among the barriers are inherent visualization limitations, as well issues with integration of diverse data sources into a cohesive, accessible, and interpretable format [127]. It is this situation that led to the establishment of Business Intelligence Competency Centres (BICCs) for Orgs. with regard to all phases of the business intelligence implementation as well as appropriate application of business data [123].

BI and the banking sector BI has gained prominence in banks for supporting decision-making, with the application of BI concepts to economically enhance financial reportability, risk Mgmt., efficiency analysis etc. For instance, financial institutions acquire Sig. benefit of using the system from the perspective of being able to maintain continuous reporting on a financial level and understanding the operation s through use of Oracle BI 11g [128]. The users can put on analysis request customer accounts and loan, being through a periodic statement of income; improving the date banks financial institutions [128].

The business intelligence system in business Mgmt. and the urban environment works on the way to the most favorable development considering pure efficiency and strategy engine data-driven activities. The ability to process the data acquired from multiple sources into actionable information at speed, gives a competitive advantage in changeable and tough business climate. Through the example of Kraft Foods and numerous such companies, it has been proved that BI adds to enhanced decision-making not only in different verticals but also leads to a leaner organization with better end results [129]. Yet in Smart cities, BIs efforts enable urban areas to not only play in the Tech world but also offers sustainable solutions (to citizens as well, as stake-holders) [128].

2.4 THE EMERGENCE OF SMART CITIES AND THEIR RELIANCE ON BUSINESS INTELLIGENCE (BI) SYSTEMS

In fact, STR planning is the backbone of all Org. Not to mention with the advent of smart cities, STR planning has become essential in harsh climate and dynamic urban scenario. Which, of course, mean that businesses will need a well-formulated BI system for good decision-making. Such systems are most suitable when coupled to a data warehouse and refreshed as part of a series of ETL processes with the result of creating high-quality, accurate and available information.

This, of course, means the need for a well-structured BI system to achieve good decision making in business. Such systems normally work well when coupled with data warehouse systems refreshed with a number of ETL processes in order to create clean, accurate, immediately accessible information. With its real-time structure, data is constantly integrated to enable rapid executive decisions, under the control of decision-makers, and efficiently managed in a challenging environment [130].

Competition in the business world has intensified significantly with technological advancements, increasing the complexity of smart cities. Adopting new technologies has become a necessary, though not the only, requirement for success in this complex environment. Indeed, business intelligence has become an effective tool, facilitating appropriate decision-making and generating actionable, ready-to-use intelligence through intermediaries from diverse data sources. Large BI applications have integrated every possible or imaginable combination of data, making it easy to create rectangle, bar, and pie charts, with countless other possibilities. Besides this, BI is a common denomination for cluster engagement supported by various decision mechanisms throughout every layer of society [131] .

Decision-making becomes quicker, and anyone can leverage visual analytics to ease it down to their fourth and fifth layers of interpretative mindset capabilities. Based on numerous studies, most firms have struggled to effectively utilize organizational data in their decision-making processes. The only competitive scenario today is mainly rooted in the explosion of data being generated in all industrial sectors, with one enterprise representing the others in positions of continuous growth. Business Intelligence can also enhance the impact across multiple data repositories, thereby positively affecting the organization's robustness. In this sense, BI is a significantly powerful, cheap, easy-to-handle, and expandable practice for satisfying the needs of the organization in most fields, especially where data destruction is evident and hard to interpret [124].

In the past, when top Mgmt. was overwhelmed with vast amounts of information, it was of little use to them, as the information was beyond their understanding. Decision-Support Systems were established to facilitate trade-offs, summarizing and circulating data into formats that support more layered decision-making activities. The flip side of this relationship with these systems is a Sig. flaw: they suffer from problems including low visualizability, poor usability and weak adoptability (not to mention lack of integration) thus allowing multiple paths for designing more complex BISs [132].

2.4.1 Business Intelligence and Its Impact on Decision-Making

BI systems would have been able to deliver value in every sector, and one of their ADs is the ability to present data visually so as to make sense for non-IT experts i.e., no specialist

IT knowledge would be required; another benefit could be processing through mullions of data virtually at blink of eye, bespeaking faster decisions. This rapidity spares decision-makers dealing with strategies the overhead of processing data. Another advantage of BI systems is they reduce the complexity in operating with key performance indicators (KPI) [129], leading to more effective reporting and analysis. Process of optimization in terms of financial analysis, risk Mgmt., efficiency analysis etc. Forms the basis for professional business intelligence systems for the purposes of financial reporting and accounting. 1 03 A Unified And Auditable Presentation of Financial Information The structure built by the Oracle Business Intelligence11g results in fast creation of reports with a single presentation for easy reporting, one of business intelligence benefits banking. This further forwards to banks the ability offer consolidated balance sheets, audit details and risk analysis for regulatory and operational needs [133].

Given the changes in banking space, BI system enabled enhanced reporting and increased effectiveness of operations. Enabled in banking, but not is Sig. Oracle Bus Intel 11g – How much data do we actually need? AD was used as part of the process for reviewing customer accounts and thereby determining the financial prospects of loans. Currently, banking institutions face the challenge of having disparate software systems--for example accounting, asset management, etc.-operating on the market. An interfaced BI systems allowed to just go in and correct the data discrepancy. This single solution enables the reconciliation between accounting account total amounts and voucher numbers, allowing for a simple form of bank transactions' reconciliations not leading to any disclosure of errors [128].

The BI applications enable the banks for analyzing their P & L on periodic basis, assessing the financial position and detecting differences observed in account balances through the reports generated by them. These skills were critical for isolating the types of misallocated vouchers from which we could then tighten up change in banking systems and processes. In this sense, through automation, BI applications identify common mistakes in banking thus helping in improving robustness and integrity of the financials as well as operational efficiency [128].

2.5 THE IMPORTANCE OF SECURING BIG DATA IN URBAN AREAS

Ensuring sustainability of BD inside the modern Orgs., and therein within the urban context, has become a delicate matter, more so as cutting edge technologies that are data driven are increasingly being adopted. Big data (BD) is the term used to describe large complex sets of data (structured or unstructured) which cannot be processed by traditional methods. Using BD technologies, Orgs. can produce, acquire, process, analyze and visualize big data to extract insights to support decision-making systems as well as diagnostic and prediction tasks [134].

As the amount of data grows and with the complexity involved in its Mgmt., storage, processing and security is getting more difficult in urban environments, as one can consider for instance that there are a multitude of intelligent devices and miscellaneous kind of critical facilities present to add to the exposure level of those pieces of data for an attack. One of the problematics in the realm of BD governance is its governance. In such context, the source data of quality will eventually be kept up-to-date for ML applications and decision-making, without disregarding legal and ethical practices. BD governance is the system of policies, processes, and tools used to ensure that data is handled in a responsible and secure way in accordance with defined standards or regulations [134].

Additionally, as urban Orgs. more and more depend on BD to improve organizational efficiency and public service quality, it is even more obvious for such a framework to be secure. Sure, Data Governance is what takes away from the chances of a security breach in mismanagement, an abuse of value even though none present themselves in a very good light for valuable Big Data. Implementing BDA becomes a highly dicey exercise for urban organizations because it involves a lot of risk in the areas of security and privacy, and undoubtedly, cybersecurity would be the first of such challenges. The surface area through which a cyber-criminal can launch probes has grown tremendously-from a multitude of devices-networked into systems-for convenience and exploitation. Power grids, health-care systems, and financial networks are typically affected by these breaches-and there cannot be sidestep effected without covering massive disruption According to one estimate that the number of connected devices from which cyber-attacks originate are likely to reach 20.8 billion worldwide this year; it means an increase of threats-from loss of data at the finger stroke to mayor directed hacker attacks [135].

This, however compounds the effect of no stringent enforcement in BD governance frameworks to direct when where data should be stored, transmitted or accessed by nonauthorized parties. Orgs. will thus deploy a holistic BD governance framework capturing security and privacy considerations across all dimensions of data Mgmt.. Its alignment of people, processes, technologies and rules ensures that Orgs. optimise the value of BD as an STR asset, securing, preserving data integrity and regulatory compliance. The system should balance between information storage and transfer in order to achieve best utilization of BD for decision-making while maintaining security [136]. As such, the model should be inspired by the Evaluation and Direct Monitoring (EDM) cycle instead of a linear input-output process in that governance intervention is an ongoing process [137].

In BD governance, a particularly influential area is that concerned with cybersecurity, especially focused on network intrusion detection systems NIDS). Today, with the cybersecurity threat landscape becoming even more sophisticated, Orgs. Now have to BDA in anticipation and preempt attacking activity. Sophisticated analytical data sets provide security operators with a near live monitoring of traffic flow characteristics and have relatively rapid response times for abnormal flows which could indicate potential intruder either external or internal [138].

This utility will be important for getting a more secure database-collect-retain-analyze for sec data in Orgs. securing data and mitigating the impacts of malicious cyber activity2. urban orgs. face various challenges to tap into the potential of BDA without sacrificing its security and privacy too much on the outsourced data. You need infrastructure and especially the required computing resources in a scale that extends beyond what smaller Orgs can deliver. with limited capabilities[134].

What makes this worse is that we also have to follow extra data protection rules; depending on where in the world we ship (for example GDPR, CCPA). Consequently, data governance frameworks must compromise to allow flexible scaling using performance while at least meeting the privacy and security requirements [134].

Operating BD in any 21st-century Org., particularly when it is sited urbanely entails the most comprehensive considerations on all dimensions that consist of both hard power actions and softer data governance frameworks. Data will be safely stored, processed and used by

the institution, so they can process as much BD as they would like to without worrying that it might get a large fine because of data leaks or unlawful use of its data. Such BD applications will be even more needed in the future as data governance frameworks become pervasive () and use of those databases proliferates -especially in urban domains–, exampled by health, private finance and governments. The next stage of this will be a research push to see how else BD systems can be scaled, protected, and secured in such an increasingly inter-connected world [134].

3. MATERIAL AND METHODS

3.1 TYPE OF STUDY

The study was designed in a descriptive cross-sectional manner.

3.2 PLACE AND TIME OF STUDY

This study was conducted in two phases.

The first phase: In the Urban Cities Company. It is situated on the Mediterranean Sea between Tripoli and Sirte; it serves as the nation's commercial port and has maintained a strong commercial reputation for several centuries [28].

The second phase: The Misrata Free Zone Company is located in the heart of the coastal city of Misrata, on the Mediterranean Sea, where major trade routes converge between North and South and between Europe and Africa. That STR site provides investors with convenient access to regional and world markets at a minimal cost. The Misrata Free Zone incorporates Libya's most high-profile commercial port, which represents around 60% of the country's non-oil trade. The zone provides a perfect place for both local and foreign investors as all taxes, customs duties and other imposts on commerce are not payable in this zone [139].

The Libyan Iron and Steel Company is one of the largest industrial companies in Libya. It spans an area of 1,200 hectares in Misrata, 210 kilometers east of Tripoli. The company's design production capacity is 1,700,000 tons of liquid steel per year, using a direct reduction process for iron pellets using local natural gas [140].

Major companies, including the Libyan Iron and Steel Company and Al-Naseem Food Industries Company, were established there. The simple random sampling method, which is one of the probability sampling methods, was used to select the sample. G-power analysis was used in calculating the sample [19],[22],

3.3 STUDY SAMPLE

Figure 3.1 illustrates the sample size assessment using G-Power analysis, and Figure 3.2 illustrates the G-Power diagram. The sample size was set at 50 employees in the first phase, and 134 in the second phase. Google Forms submitted the data electronically.

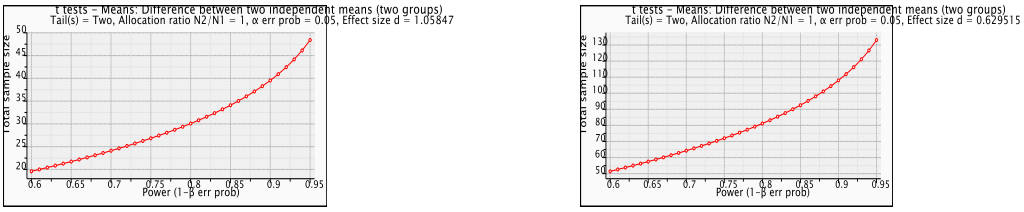
Using a theoretical value of 1.96, a 95% confidence interval, and a sampling error of 0.05, the sample size was calculated with p = 0.5, q = 0.5, and d = 0.05, assuming α = 0.05; based on the calculation results [141].

N represents the universe, n denotes the application frequency, p denotes the frequency of the event under study, and q denotes the frequency of non-occurrence of the event under study. t: the theoretical value obtained from the t-table at a specified degree of freedom and error level; d: the required ± standard deviation corresponding to the occurrence of the event.

$$n = \frac{Nt^2\,pq}{d^2(N-1)+t^2pq} \tag{3.1}$$

(a): The first phase (b): The second phase

Figure 3.1: Sample Size Assessment Utilising G-Power Analysis (A) The First Phase, (B) The Second Phase



(a): The first phase (b): The second phase

Figure 3.2: G-power Plot (A) The First Phase, (B) The Second Phase.

3.4 DATA COLLECTION INSTRUMENTS

The survey consists of three to five questions: age, sex, and education. The second half contains Spillan and Parnell (2006)[142] Profitability Scale. by Egerson et al. [143]. This scale contains 4 items, and the Cronbach alpha value is 0.853.

(3) "Realizing ROI Goals" by De Weerd-Nederhof et al. [144], developed by Egerson et al. [143], which consists of five items (Cronbach's alpha = 0.83).

The fourth part measured cyber security using the Information Security Culture Scale of Flores and Ekstedt [145]. and then developed by Egerson et al. [143], including 7 items such as "My work colleagues alert me about risky emails, downloading viruses or using weak passwords", which indicated a Cronbach's alpha was 0.89. All of the constructs were measured using a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree).

4. RESULTS AND DISCUSSION

The data were processed in SPSS (version 26.0; Statistical Package for the Social Sciences) with a significance level of 0.05. Descriptive statistics including frequency, percent, mean and standard deviation were applied. The internal (measurement) model was also in common predominance, in the analysis of external loadings, construct validity, reliability and R-squared.

4.1 DESCRIPTIVE ANALYSIS OF DEMOGRAPHIC DATA

A descriptive analysis was first performed to see demographic profiles of the subjects before any inferential analysis. The purpose was to have an account of age, gender and education level of the sample. The distribution of these variables provides context for the study results and can be used to evaluate the representativeness of the sample. Details are provided in Table 4.1 below.

Table 4.1: Socio-Demographic Data.

Items		**The first phase**		**The second phase**	
		n	**%**	**n**	**%**
Age	Less than 25	12	24,0	12	9,0
	Between 25 and 35	29	58,0	113	84,3
	From 35 and over	9	18,0	9	6,7
Gender	Male	23	46,0	77	57,5
	Female	27	54,0	57	42,5
Education level	Secondary school	28	56,0	88	65,7
	Diplom/ high diploma degree	14	28,0	38	28,4
	Bachelor's degree	5	10,0	5	3,7
	Master degree	3	6,0	3	2,2

In Table 4.1, 58% of the study sample were between 25-35years old, 54% were female, and 56% were high school graduates in the first phase. Also, 84.3% between 55 and 35 years old, 57.5 were male, and 54.7% had a secondary school in second phase

4.2 FACTOR AND RELIABILITY ANALYSIS

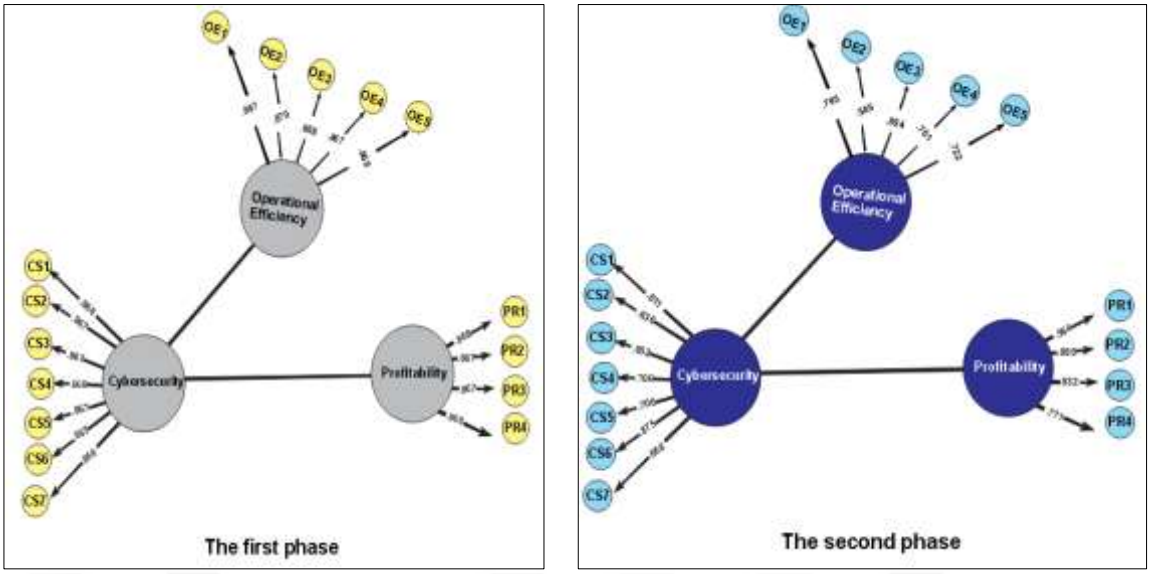
A principal components analysis was conducted to validate the classification of questionnaire items into the expected categories. The results confirmed the validity of the

scale's structure, providing a solid basis for further interpretation. A summary of the exploratory factor analysis is presented in Table 2.4 below.

Table 4.2: Reliability and Convergent Validity.

Construct	Indicator	The first phase		The second phase		AVE	Decision
		Composite Reliability	Cronbach's Alpha if Item Deleted	Composite Reliability	Composite Reliability		
Profitability	PR1	0,852	,868	0.853	0.564	0.854	Accepted
	PR2		,867		0.885		
	PR3		,867		0.832		
	PR4		,868		0.771		
Operation efficiency	OE1	,848	,867	0.869	0.795	0.575	Accepted
	OE2		,870		0.585		
	OE3		,868		0.894		
	OE4		,867		0.761		
	OE5		,868		0.722		
Cybersecurity	CS1	,845	,868	0.924	0.811	0.597	Accepted
	CS2		,867		0.636		
	CS3		,867		0.652		
	CS4		,868		0.788		
	CS5		,867		0.706		
	CS6		,869		0.875		
	CS7		,869		0.868		

In Table 2, Cronbach's alpha test coefficient was 0.852. The operation efficiency was .848, and finally, it was .845, reflecting the acceptability of reliability and the internal consistency, convergent and divergent validity of the measurement.



(a)The first phase (b)The second phase

Figure 4.1: Study Model.

4.3 CORRELATION ANALYSIS

Table 4.3: Relationship between Profitability, Operations Efficiency, And Cybersecurity First Phase.

Correlations				
		1	2	3
1. Profitability	r	1	,806**	,657**
	Sig.		,000	,000
2. Operation efficiency	r	,806**	1	,774**
	Sig.	,000		,000
3. Cybersecurity	r	,657**	,774**	1
	Sig.	,000	,000	

**. Correlation is Sig. at the 0.01 level (2-tailed).

In Table 4.3, there is a positive relationship between profitability, operation efficiency, and cybersecurity $p<0.05$

Table 4.4: Relationship between Profitability, Operations Efficiency, And Cybersecurity, Second Phase.

Correlations				
		1	2	3
1. Profitability	r	1	,862**	,732**
	Sig.		,000	,000
2. Operation efficiency	r	,862**	1	,815**
	Sig.	,000		,000
3. Cybersecurity	r	,732**	,815**	1
	Sig.	,000	,000	
**. Correlation is Sig. at the 0.01 level (2-tailed).				

In Table 4.4, there is a positive relationship between profitability, operation efficiency, and cybersecurity $p<0.05$

4.4 REGRESSION ANALYSIS

Table 4.5: Relationship between Profitability and Cybersecurity According to Linear Regression, First Phase .

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Bound	
							Lower	Upper
1	(Constant)	1,747	,343		5,09	,000	1,05	2,43
	Operation Efficiency	,086	,029	,530	2,99	,004	,02	,143
		-,041	,018	-,412	-2,32	,024	-,07	-,006
R^2= ,164 F= 4. 604 p=0.015								
a. Dependent Variable: profitability scale								

In Table 4.5. The results of the linear regression analysis showed that the variables are profitability and Cybersecurity. ($F = 4.604$; $p = 0.015$) which means that they are statistically Sig., and the R^2 value was found to be 164. Thus, all the independent variables in the model explain 16.4% of the variance in Cybersecurity. In addition, the R^2 shows the generalizability of the model. This means that if the model were generated from the universe instead of the sample, it could explain 16.4% of the total variance.

Table 4.6: Relationship between Profitability and Cybersecurity According to Linear Regression, Second Phase.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	-,233	,734		-,317	,752	-1,686	1,220
	Total Operation Efficiency	,793	,041	,862	19,565	,000	,713	,873
R^2= ,862F= 382,98 p=0.000								
a. Dependent Variable: Total profitability								

In Table 4.6, the relationship between profitability and cybersecurity. According to the linear regression (second stage), overall operational efficiency plays a Sig. and strong role in influencing profitability. In the context of your study on cybersecurity, this suggests that as companies implement better operational efficiency strategies (including stronger cybersecurity protocols), their profitability is likely to improve. The high R^2 value (0.862) indicates that operational efficiency (potentially influenced by cybersecurity measures) explains a Sig. portion of profitability. Therefore, investing in cybersecurity measures, which often enhance operational efficiency, is critical for improving profitability in business intelligence systems, especially in urban cities where BD is prevalent. $P<0.05$ and confidence intervals confirm the robustness of these results, indicating that the relationship between operational efficiency (cybersecurity) and profitability is strong and reliable.

Table 4.7: Relationship between Operation Efficiency and Cybersecurity First Phase.

Model 1		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Bound	
							Lower	Upper
1	(Constant)	2,124	,390		5,44	,000	1,339	2,909
	Operation efficiency	-,007	,034	-,048	-,209	,836	-,076	,061
	Cybersecurity	-,003	,023	-,027	-,116	,909	-,049	,043
R^2= ,005 F= ,118 p=,889								

In Table 4.7, the results of the linear regression analysis where the variables are profitability and Cybersecurity. (F = ,118; p = 0.889) which means that they are not statistically Sig., and the R^2 value was found to be .005. Thus, all the independent variables in the model explain 11.8% of the variance in Cybersecurity. In addition, the R^2 shows the generalizability of the model. This means that if the model were generated from the universe rather than the sample, it could explain 11.8% of the total variance.

Table 4.8: Relationship between Operation Efficiency and Cybersecurity Second Phase.

Model		Unstandardized Coefficients		Standardized Coefficients	t	sig.	95,0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	,711	1,446		,491	,624	-2,150	3,572
	Total Operation Efficiency	1,291	,080	,815	16,177	,000	1,133	1,449
R^2= ,665F= 261,68 p=0.000								
a. Dependent Variable: Cybersecurity								

In Table 4.8, Operational efficiency has a strong and positive impact on cybersecurity. As companies improve their operational processes, particularly with regard to cybersecurity measures, they improve their overall cybersecurity framework. The model has a high statistical significance (with an R^2 coefficient of 0.665), indicating that operational efficiency is a key factor in determining the level of cybersecurity in organizations. This is especially applicable to your research on using cybersecurity techniques in business intelligence systems.

Overall, the effective ops of the firms studied benefit from cyber security. This correspond to Egerson et al. [143] who reported that generally, cyber security significantly improves the productivity of Nigerian ATM banks. Robust cybersecurity safeguards banks against disabling cyberattacks and this aids continued stability (Victory et al., 2022) [146]. “It is also about increasing the effectiveness of the financial system, preventing disruptions and slowdowns thus ensuring transactional regularity and availability of services” [147]. It is demonstrated that cybersecurity influences positively the profitability of firms in the sample. This result corresponds to the study by Egerson et al., 2024 [143], which suggest

that significance but positive impact on cyber security was also found. profitability of Nigerian depository banks. Effective cybersecurity regulations reduce the costs of future data breach and fraud; they can mitigate losses on financial should there be Ojeka et al., [148]. Efficient cybersecurity systems protect investments in finances, thereby creating a conducive environment for a sustainable profit-making and long-lasting business [143].

.

5. CONCLUSION

As indicated in this research, cybersecurity measures will quickly take center stage for Libyan businesses to improve their operational profits and performance. These inferences might extend in agreement with the theory of dynamic capabilities in that it would be naive for Libyan firms to simply look up and assess the security situation-incrementing and decrementing threats- from which clear strategic directions would be defined. To avoid operational and financial downtimes, as well as to minimize long-term adverse impact on profits and survival of impacted entities, the highlight is on the importance of solid cybersecurity strategies that would be in place according to the findings.

Based on findings from the study, operational efficiency (which cybersecurity measures are part of) is a Sig. as a critical and impelling factor for better business profit ratio and cyber security in urban BI systems. The statistics find a positive correlation and stat Sig. results in the various phases of the study.

Demographic details: Ages ranged from 25 to 35 years old (58%), slightly more women than men participated (54%) and the group was mostly composed of subjects with a secondary educational level (56%). This distribution of demographics has implications for the context of the sample, but not for the results of statistical testing.

Factor analysis: The Cronbach's alpha value and the composite reliability value of the measurement model were larger than acceptable threshold, which indicated that the reliability and validity of measurement model was good. This suggested reliability and consistency of the measurement devices.

Profitability: The coefficients of operational efficiency and cybersecurity are positively significant, the coefficients being ~ 0.45 - 0.50 each, meaning that if you increase one of them then it most likely will impact on both elements positive or vice versa. This association was stable under the two phases of the study (Phase One and Two). During both phases, profitability was positively associated with operational efficiency and cyber-defensibility. Operational performance demonstrated the most significant correlation with profitability, which is a testament to the fact that best-in-class operations (cyber included) drive financial success.

The first-stage regression model revealed that SEA was significant (R^2 of 0.164) illustrating that operational concerns such as cyber security explained 16.4% of the entire variation profitability. The second-stage regression model; however, showed even higher predictive capabilities with R2 of 0.862 thus implying that efficiency (as well as effective cybersecurity) is potentially explaining up to 86.2% in variance across the firms' profitability. This is yet another demonstration that operational changes (like cybersecurity enhancements) can truly impact the bottom line. First stage deviation: In contrast, Operational Efficiency was not statistically Significant with respect to Cybersecurity in the first stage (R^2=0.005, p=0.889) which means that consequence of cybersecurity is influenced by variables other than operational efficiency. However, this was addressed in the subsequent stage where Operational Efficiency has been found to positively and significantly influence Cybersecurity (R^2 = 0.665), suggesting that its improvement through effective cybersecurity strategies will help in securing business data and systems.

5.1 RECOMMENDATIONS

Investment in operation efficiency and cybersecurity: Both operational efficiencies and cybersecurity represents the profit and safe operating conditions for Cyber Security; hence investment in process efficiencies of factories including cyber-security, must be prioritized by city -based firms possessing BD ecosystems. They are, therefore, obliged to reinforce their cybersecurity against any and all new threats -especially Business Intelligence systems.

Higher Western Earnings Stem From Protecting More Data in Depth: Its conclusions note that higher returns are driven by investments and strict operations around cybersecurity. Accordingly, businesses should consider cybersecurity as something more than just a technical requirement to protect assets but rather an essential driver of holistic business success. We need to check and rebalance our cybersecurity policies regularly.

Ongoing Education and Training: More than half (56%) of the participants had graduated high school, and business entities must maintain educative programs that serve to develop the knowledge and use of cyber by tech-literate as well as lay workers who hamper action plans' effectiveness.

Future Research Opportunities of Technologies: The scope for other future research could be undertaken to investigate the interplay among operational effectiveness, cybersecurity and productivity in various contexts (i.e. industry and country). Further, new technologies can also influence how business outcomes evolve in a more digital world, when it comes to operational efficiency and cyber security.

Model Improvement: While there was already a widely noted expectation before that operational excellence and cybersecurity (Phase 2) had a high correlation this was not so true for one specific relation in Phase 1, i.e. profit only. This inconsistency must be verified by future research findings and the measurement model need to be adjusted in order to qualify prediction level.

REFERENCES

[1] O. Tsaruk and M. Korniiets, "Hybrid nature of modern threats for cybersecurity and information security," Smart Cities and Regional Development (SCRD) Journal, vol. 4, no. 1, pp. 57-78, 2020.

[2] S. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," Computers & Security, vol. 61, pp. 169-183, 2016.

[3] J. Mills, S. M. F. Stuban, and J. Dever, "Predict insider threats using human behaviors," IEEE Engineering Management Review, vol. 45, no. 1, pp. 39-48, 2017.

[4] L. Kovacs, "National cybersecurity strategy framework," Academic and Applied Research in Military and Public Management Science, vol. 18, no. 2, 2019.

[5] Ministry of Transport, Maritime Affairs and Communications, "National Cyber Security Strategy and 2013–2014 Action Plan," 2013. [Online]. Available: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

[6] Ministry of Transport, Maritime Affairs and Communications, "2016–2019 National Cyber Security Strategy," 2016. [Online]. Available: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/2016-2019guvenlik.pdf

[7] Cyber Security Agency of Singapore, "Singapore's Cybersecurity Strategy," 2016. [Online]. Available: https://www.csa.gov.sg/TipsResource/publications/2016/SingaporeCybersecurity-Strategy

[8] Cyber Security Agency of Singapore, "Singapore's Safer Cyberspace Masterplan," 2020. [Online]. Available: https://www.csa.gov.sg/TipsResource/publications/2020/safer-cyberspacemasterplan

[9] Republic of Estonia, "Cybersecurity Strategy," 2019. [Online]. Available: https://www.mkm.ee/media/703/download

[10] Republic of Estonia, "Cybersecurity Strategy in Estonia," 2021. [Online]. Available: https://www.ria.ee/media/1494/download

[11] The European Union Agency for Cybersecurity (ENISA), "National cyber security strategies practical guide on development and execution," 2012. [Online]. Available: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

[12] NATO Cooperative Cyber Defence Centre of Excellence, "National cyber security framework manual," 2012. [Online]. Available: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[13] International Telecommunication Union (ITU), "Guide to developing a national cybersecurity strategy," 2018. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-CYB_GUIDE.01-2018-PDF-E.pdf

[14] Ö. Evre and B. Ciylan, "Measurement of the cybersecurity strategy effectiveness with a scorecard based on risk analysis," GU Journal of Science, Part C, vol. 11, no. 4, pp. 1116–1130, 2023.

[15] J. M. Borky and T. H. Bradley, "Protecting information with cybersecurity," International Journal of Cybersecurity, vol. 19, no. 3, pp. 130–145, 2019.

[16] Y. Diogenes and E. Ozkaya, Cybersecurity—Attack and Defense Strategies. Birmingham, UK: Packt Publishing, 2019.

[17] F. Özsungur, "Business management and strategy in cybersecurity for digital transformation," in Handbook of Research on Advancing Cybersecurity for Digital Transformation, IGI Global, 2021, pp. 144–162.

[18] S. A. Wymer, "The impact of digital transformation on business intelligence," J. Bus. Intell. Res., vol. 3, no. 1, pp. 10-25, 2018.

[19] A. Adewusi, O. Olorunsogo, and O. F. Asuzu, "Business intelligence in the era of big data: A review," Computer Science & IT Research Journal, vol. 5, no. 2, pp. 415–431, 2024.

[20] E. M. Kala, "The impact of cyber security on business," Open Journal of Safety Science and Technology, vol. 13, no. 2, pp. 51–65, 2023.

[21] C. Dioha, N. A. Mohammed, and J. O. Joshua, "Effect of firm characteristics on profitability," Journal of Accounting, Finance and Auditing Studies, vol. 4, no. 2, pp. 14–31, 2018.

[22] R. Akintoye, I. A. Odusanya, and O. G. Yinusa, "Cybersecurity and financial innovation in Nigerian banks," Universal Journal of Accounting and Finance, vol. 10, no. 3, pp. 643–652, 2022.

[23] I. A. Odusanya, O. G. Yinusa, and B. M. Ilo, "Determinants of firm profitability," Journal of Economics and Business, vol. 68, no. 1, pp. 43–58, 2018.

[24] K. Khalil et al., "Impact of cyber security cost on financial performance," Humanities and Social Sciences Reviews, vol. 9, no. 2, pp. 691–703, 2021.

[25] A. Sardi et al., "Big data and performance measurement research," Measuring Business Excellence, vol. 27, no. 4, pp. 531–548, 2023.

[26] W. K. Too and M. Mutuku, "Effects of cybersecurity on public sector performance," Review of Journal of International Business and Management, vol. 4, no. 1, p. 471, 2023.

[27] R. Masoud et al., "Cybersecurity awareness in Libyan universities," Scientific Journal of College of Education, vol. 4, no. 2, pp. 225–238, 2025.

[28] S. A. Ojeka, E. Ben-Caleb, and I. Ekpe, "Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness," International Review of Management and Marketing, vol. 7, no. 2, pp. 340–346, 2017.

[29] P. K. Rajendran, A. Asbern, K. M. Kumar, R. Manoharan, and A. Rajendra, "Implementation and analysis of MapReduce on biomedical big data," Indian Journal of Science and Technology, vol. 9, no. 31, pp. 1-6, 2016.

[30] X. Wu, X. Zhu, G. Q. Wu, and W. Ding, "Data mining with big data," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97-107, 2014.

[31] J. Manyika et al., "Big data: The next frontier for innovation, competition, and productivity," McKinsey Global Institute, Rep. 1-137, 2011.

[32] A. Adadi, "A survey on data-efficient algorithms in big data era," Journal of Big Data, vol. 8, no. 1, p. 24, 2021.

[33] R. Kitchin, The Data Revolution: A Critical Analysis of Big Data, Open Data and Data Infrastructures. London, UK: SAGE Publications, 2021.

[34] A. A. Gad-Elrab, "Modern business intelligence: Big data analytics and artificial intelligence for creating the data-driven value," in E-Business - Higher Education and Intelligence Applications, vol. 135, 2021.

[35] R. Suša et al., "Data integration and quality management in business intelligence systems," International Journal of Data Management, vol. 35, no. 2, pp. 44-60, 2020.

[36] B. Zohuri and M. Moghaddam, "From business intelligence to artificial intelligence," Journal of Material Sciences & Manufacturing Research, vol. 3, 2020.

[37] J. Ranjan and C. Foropon, "Big data analytics in building the competitive intelligence of organizations," International Journal of Information Management, vol. 56, p. 102231, 2021.

[38] T. Dubuc, F. Stahl, and E. B. Roesch, "Mapping the big data landscape: Technologies, platforms and paradigms for real-time analytics of data streams," IEEE Access, vol. 9, pp. 15351-15374, 2020.

[39] H. Chien, K. Hori, and O. Saito, "Urban commons in the techno-economic paradigm shift: An information and communication technology-enabled climate-resilient solutions review," Environment and Planning B: Urban Analytics and City Science, vol. 49, no. 5, pp. 1389–1405, 2022.

[40] S. K. Sahoo and S. S. Goswami, "A comprehensive review of multiple criteria decision-making (MCDM) methods: advancements, applications, and future directions," Decision Making Advances, vol. 1, no. 1, pp. 25-48, 2023.

[41] Y. Talaoui, M. Kohtamäki, M. Ranta, and S. Paroutis, "Recovering the divide: A review of the big data analytics—strategy relationship," Long Range Planning, p. 102290, 2023.

[42] J. Yang, P. Xiu, L. Sun, L. Ying, and B. Muthu, "Social media data analytics for business decision making system to competitive analysis," Information Processing & Management, vol. 59, no. 1, p. 102751, 2022.

[43] R. Varadarajan, "Customer information resources advantage, marketing strategy and business performance: A market resources-based view," Industrial Marketing Management, vol. 89, pp. 89-97, 2020.

[44] M. A. R. Saldana, "Exploring the strategies of decision-makers to improve business decisions using business intelligence and analytics tools," Ph.D. dissertation, Colorado Technical University, 2021.

[45] M. Favaretto, E. De Clercq, C. O. Schneble, and B. S. Elger, "What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade," PLoS ONE, vol. 15, no. 2, p. e0228987, 2020.

[46] M. Lnenicka, P. Hervert, and O. Horak, "Understanding big data and data protection measures in smart city strategies: An analysis of 28 cities," Urban Governance, vol. 4, no. 4, pp. 255–273, 2024.

[47] M. T. Braun, G. Kuljanin, and R. P. DeShon, "Special considerations for the acquisition and wrangling of big data," Organizational Research Methods, vol. 21, no. 3, pp. 653-677, 2018.

[48] A. A. Hussein, "Fifty-six big data V's characteristics and proposed strategies to overcome security and privacy challenges (BD2)," Journal of Information Security, vol. 11, no. 4, pp. 304-328, 2020.

[49] L. Sun, H. Zhang, and C. Fang, "Data security governance in the era of big data: Status, challenges, and prospects," Data Science and Management, vol. 2, pp. 41-44, 2021.

[50] A. J. Bokolo, "Data driven approaches for smart city planning and design: A case scenario on urban data management," Digital Policy, Regulation and Governance, vol. 25, no. 4, pp. 351-367, 2023.

[51] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," Information Systems Frontiers, vol. 24, pp. 393-414, 2022.

[52] A. R. Javed et al., "Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects," Cities, vol. 129, p. 103794, 2022.

[53] R. Bellanova and M. De Goede, "The algorithmic regulation of security: An infrastructural perspective," Regulation & Governance, vol. 16, no. 1, pp. 102-118, 2022.

[54] S. P. Williams, C. A. Hardy, and J. A. Holgate, "Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective," Electronic Markets, vol. 23, pp. 341-354, 2013.

[55] M. Angelidou, "Smart city policies: A spatial approach," Cities, vol. 41, pp. S3-S11, 2014.

[56] A. Sharifi, Z. Allam, S. E. Bibri, and A. R. Khavarian-Garmsir, "Smart cities and sustainable development goals (SDGs): A systematic literature review of co-benefits and trade-offs," Cities, vol. 146, p. 104659, 2024.

[57] M. Ziosi, B. Hewitt, P. Juneja, M. Taddeo, and L. Floridi, "Smart cities: Reviewing the debate about their ethical implications," AI & Society, vol. 39, pp. 1185-1200, 2024.

[58] B. Middha and I. McShane, "E-gentrification: Digital community engagement, urban change and digital rights to the city," in Citizen Participation in the Information Society: Comparing Participatory Channels in Urban Development. Cham: Springer International Publishing, 2022, pp. 141-165.

[59] V. Mykhnenko, "Smart shrinkage solutions? The future of present-day urban regeneration on the inner peripheries of Europe," Applied Geography, vol. 157, p. 103018, 2023.

[60] R. Von Solms and J. Van Niekerk, "From information security to cyber security," Computers & Security, vol. 38, pp. 97-102, 2013.

[61] The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," Washington, DC, USA, 2011.

[62] Minister for the Cabinet Office and Paymaster General, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world," UK Government, 2011.

[63] M. A. Hashmani, S. M. Jameel, A. M. Ibrahim, M. Zaffar, and K. Raza, "An ensemble approach to Big Data security (Cyber security)," International Journal of Advanced Computer Science and Applications, vol. 9, no. 9, 2018.

[64] S. Lavanya, K. Mythili, and S. Kannimuthu, "An integration of big data analytics and cyber security-A panoramic survey," International Journal of Advanced Research in Engineering and Technology, vol. 11, no. 9, pp. 747-754, 2020.

[65] A. Bajpai, D. Dayanand, and A. Arya, "Big Data Analytics in Cyber Security," International Journal of Computer Sciences and Engineering, vol. 6, no. 7, pp. 496-500, 2018.

[66] S. Satpathy, C. Mallick, and S. K. Pradhan, "Big Data Computing Application in Digital Forensics Investigation and Cyber Security," International Journal of Computer Science and Mobile Applications, vol. 6, no. 3, pp. 1-8, 2018.

[67] F. Ullah and M. A. Babar, "Architectural tactics for big data cybersecurity analytics systems: A review," Journal of Systems and Software, vol. 151, pp. 81-118, 2019.

[68] P. Angin, B. Bhargava, and R. Ranchal, "Big Data Analytics for Cyber Security," in Proc. 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019, pp. 0365-0371.

[69] J. Chen, C. Su, and Z. Yan, "AI-Driven Cyber Security Analytics and Privacy Protection," in Proc. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019, pp. 392-396.

[70] L. Wang and C. A. Alexander, "Big Data Analytics and Cyber security for Advanced Manufacturing," Industrial and Systems Engineering, vol. 1, no. 1, 2016.

[71] H. Teymourlouei and L. Jackson, "How Big Data Can Improve Cyber Security," in Proc. Int. Conf. Advances in Big Data Analytics, 2018, pp. 84-88.

[72] R. O. Andrade, N. Ontaneda, A. Silva, and L. Tello-Oquendo, "Application of Big Data Analytic in Cybersecurity," in Proc. 2019 Int. Conf. on Advances on Applied Cognitive Computing (ACC), 2019, pp. 47-52.

[73] D. Mitić, M. Jovanović, and N. Biga, "Big Data and Cyber Security: Contemporary Issues," in Proc. 9th Int. Conf. Business Information Security (BISEC), 2017, pp. 1-6.

[74] G. Roopa and D. Ramesh, "Designing a Collaborative Detection System for Detecting the Threats to Cyber Security in Big Data," Indian Journal of Public Health Research and Development, vol. 9, no. 11, pp. 1600-1605, 2018.

[75] M. Hashmani et al., "An ensemble approach to big data security (Cyber security)," International Journal of Advanced Computer Science and Applications, vol. 9, no. 9, pp. 197-203, 2018.

[76] A. Bajpai, A. Dayanand, and A. Arya, "Big Data Analytics in Cyber Security," International Journal of Computer Sciences and Engineering, vol. 6, no. 7, pp. 2347-2693, 2018.

[77] S. Satpathy, C. Mallick, and S. K. Pradhan, "Big Data Computing Application in Digital Forensics Investigation and Cyber Security," in Proc. National Conference on "The Things Services and Applications of Internet of Things", 2018, pp. 129-136.

[78] Y. Zhao et al., "Data and Deep Models Applied to Cyber Security Data Analysis," in Proc. AAAI Fall Symposium: Artificial Intelligence for Law Enforcement (ALEC), 2018.

[79] J. Harry and L. Michael, "Cybersecurity in business intelligence systems: Safeguarding big data for profitability and growth," Cybersecurity, vol. 13, no. 1, pp. 45-63, 2024.

[80] T. Moore, "The role of regulatory frameworks in cybersecurity for business intelligence systems," Journal of Digital Security, vol. 8, no. 2, pp. 67-80, 2020.

[81] R. Hassan and A. Muhammad, "The evolving landscape of cybersecurity in business intelligence systems," International Journal of Information Security, vol. 29, no. 3, pp. 154-168, 2021.

[82] Kaspersky, "Insider threats in business intelligence systems: How to mitigate risk," 2020. [Online]. Available: https://www.kaspersky.com/blog/insider-threats-bis/

[83] G. Roopa and D. Ramesh, "Designing a Collaborative Detection System for Detecting the Threats to the Cyber Security in Big Data," 2018.

[84] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, and G. Pavlova, "A survey of artificial intelligence for enhancing information security," International Journal of Development Research, vol. 7, no. 11, pp. 16866-16872, 2017.

[85] Webroot, "Webroot Threat Report 2019," 2019. [Online]. Available: https://www-cdn.webroot.com/9315/5113/6179/2019_Webroot_Threat_Report_US_Online.pdf

[86] Imperva, "Cyber Threats Forecast 2019," 2019.

[87] Kaspersky, "Kaspersky Security Bulletin: Threat Predictions For 2019," 2019. [Online]. Available: https://www.kaspersky.com/blog/threat-predictions-2019

[88] Symantec, "Internet Security Threat Report, Volume 24," 2019. [Online]. Available: https://docs.broadcom.com/doc/istr-24-executive-summary-en

[89] Microsoft, "Microsoft Security Intelligence Report, Volume 26," 2019. [Online]. Available: https://www.microsoft.com/en-us/wdsi/threats

[90] Cisco, "Cisco IOS XE Software Arbitrary File Upload Vulnerability," 2019. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20190327-afu.html

[91] Oracle and KPMG, "Oracle and KPMG Cloud Threat Report 2019," 2019. [Online]. Available: https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf

[92] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape Report 2018," 2018. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[93] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape Report 2014," 2014. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2014

[94] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape Report 2015," 2015. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2015

[95] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape Report 2016," 2016. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

[96] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape Report 2017," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[97] Positive Technologies, "The Criminal Cyberservices Market 2018," 2018. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/criminal-cyberservices-market/

[98] Akamai, "State of the Internet / Security: Credential Stuffing Attacks," vol. 4, no. 4, 2018. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-vol-4.pdf

[99] IBM X-Force, "IBM X-Force Threat Intelligence Index 2019," 2019. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence

[100] D. Broitman et al., "Urbanization and Big Data: A New Era of Smart Cities," Journal of Urban Studies, 2025.

[101] G. Li, Y. Yao, and Z. Shao, "Big Data in Smart City," Geomatica Informatica Science, vol. 39, no. 6, pp. 631–640, 2014.

[102] V. O. K. Li, J. C. K. Lam, Y. Han, and K. Chow, "A Big Data and Artificial Intelligence Framework for Smart and Personalized Air Pollution Monitoring and Health Management in Hong Kong," Environmental Science & Policy, vol. 124, pp. 441–450, 2021.

[103] T. H. Davenport and D. J. Patil, "Data Scientist: The Sexiest Job of the 21st Century," Harvard Business Review, vol. 90, no. 10, pp. 70-76, 2012.

[104] W. Pietsch, "Big Data: The New Science of Complexity," in Proc. 6th Munich-Sydney-Tilburg Conference on Models and Decisions, Munich, Germany, 2013.

[105] P. Thakuriah, N. Tilahun, and M. Zellner, "Big data and urban informatics: innovations and challenges to urban planning and knowledge discovery," in Proc. Workshop on Big Data and Urban Informatics, Chicago, IL, USA, 2014.

[106] Y. Pan, Y. Tian, X. Liu, D. Gu, and G. Hua, "Urban big data and the development of city intelligence," Engineering, vol. 2, no. 2, pp. 171-178, 2016.

[107] X. Zhang and Y. Liu, "Big Data in Urban Management: A Review of Applications and Opportunities," Journal of Urban Technology, vol. 27, no. 3, pp. 1–15, 2020.

[108] M. Foth, J. H. Choi, and C. Satchell, "Urban informatics," in Proc. ACM 2011 Conference on Computer Supported Cooperative Work (CSCW'11), Hangzhou, China, 2011.

[109] R. Kitchin, "The real-time city? Big data and smart urbanism," GeoJournal, vol. 79, no. 1, pp. 1-14, 2014.

[110] B. Lepri, F. Antonelli, F. Pianesi, and A. Pentland, "Making big data work: Smart, sustainable, and safe cities," EPJ Data Science, vol. 4, p. 16, 2015.

[111] L. Taylor and C. Richter, "Big data and urban governance," in Geographies of Urban Governance. Cham: Springer, 2015, pp. 175–191.

[112] J. Bays and L. Callanan, "Urban informatics can help cities run more efficiently," McKinsey on Society, 2012.

[113] M. Batty, "Urban informatics and big data: A report to the ESRC cities expert group," 2013.

[114] A. R. Negro and R. Mesia, "The Business Intelligence and its influence on decision making," Journal of Applied Business and Economics, vol. 22, no. 2, pp. 112-125, 2020.

[115] S. I. Kehinde et al., "Evolution and innovation of hedge fund strategies: a systematic review of literature and framework for future research," Acta Informatica Malaysia, vol. 7, no. 1, pp. 01-06, 2023.

[116] A. B. Mohammed, M. Al-Okaily, D. Qasim, and M. K. Al-Majali, "Towards an understanding of business intelligence and analytics usage: evidence from the banking industry," International Journal of Information Management Data Insights, vol. 4, no. 1, p. 100215, 2024.

[117] H. Awawdeh, H. Abulaila, A. Alshanty, and A. Alzoubi, "Digital entrepreneurship and its impact on digital supply chains: The mediating role of business intelligence applications," International Journal of Data and Network Science, vol. 6, no. 1, pp. 233-242, 2022.

[118] R. Maritz and A. Du Toit, "The practice turn within strategy: Competitive intelligence as integrating practice," South African Journal of Economic and Management Sciences, vol. 21, no. 1, pp. 1-14, 2018.

[119] H. Tahmasebifard, "The role of competitive intelligence and its sub-types on achieving market performance," Cogent Business & Management, vol. 5, no. 1, p. 1540073, 2018.

[120] S. Ahmad, S. Miskon, R. Alabdan, and I. Tlili, "Towards sustainable textile and apparel industry: Exploring the role of business intelligence systems in the era of industry 4.0," Sustainability, vol. 12, no. 7, p. 2632, 2020.

[121] N. Nithya and R. Kiruthika, "Impact of Business Intelligence Adoption on performance of banks: a conceptual framework," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 2, pp. 3139-3150, 2021.

[122] H. Dresner, "The evolution of business intelligence," Gartner Group, 1989.

[123] G. J. Miller, D. Bräutigam, and S. V. Gerlach, Business Intelligence Competency Centers. Hoboken, NJ, USA: John Wiley & Sons, 2006.

[124] H. Ateş, "Karar vermede iş zekasının önemi tekstil sektöründe bir araştırma," M.S. thesis, Dokuz Eylul University, 2008.

[125] P. Hannon, "Case study: Kraft Foods," SAP Insider, 2015.

[126] M. Gibson, D. Arnott, and I. Jagielska, "Evaluating the intangible benefits of business intelligence: Review & research agenda," in Proc. 2004 IFIP International Conference on Decision Support Systems (DSS), 2004, pp. 295-305.

[127] J. Reinschmidt and A. Francoise, IBM Business Intelligence Certification Guide. IBM Press, 2000.

[128] S. Biroğul and H. B. Gültekin, "Importance of business intelligence solution on decision-making process of companies," International Journal of Applied Mathematics, Electronics and Computers, vol. 4, pp. 86-89, 2016.

[129] S. Crider, "SAP Business Intelligence: Kraft Foods' Recipe for Successful BI Implementation," SAP Insider, 2015.

[130] A. Cardenas, P. K. Manadhata, and S. P. Rajan, "Big data analytics for security," IEEE Security & Privacy Magazine, vol. 11, no. 6, pp. 74-76, 2013.

[131] Z. Jourdan, R. K. Rainer, and T. E. Marshall, "Business intelligence: An analysis of the literature," Information Systems Management, vol. 25, no. 2, pp. 121-131, 2008.

[132] A. S. Yılmaz, "Esnek raporlama aracı ve iş zekası uygulamaları ile bütünleştirilmesi," M.S. thesis, Ege University, 2010.

[133] M. Gibson, D. Arnott, and I. Jagielska, "Evaluating the intangible benefits of business intelligence: Review & research agenda," in Proc. 2004 IFIP International Conference on Decision Support Systems (DSS), 2004, pp. 295-305.

[134] G. Yang, M. Yang, S. Salam, and J. Zeng, "Research on Protecting Information Security Based on the Method of Hierarchical Classification in the Era of Big Data," Journal of Cybersecurity, vol. 1, no. 1, pp. 19-28, 2019.

[135] Gartner, "20.8 Billion Connected Things Will Be in Use By 2020," 2015. [Online]. Available: https://www.gartner.com/newsroom/id/3165317/

[136] V. Morabito, Big Data and Analytics: Strategic and Organizational Impacts. Cham: Springer, 2015.

[137] A. Calder, ISO/IEC 38500: The IT Governance Standard. Ely, UK: IT Governance Ltd, 2008.

[138] J. Li, Y. Qu, F. Chao, H. P. H. Shum, E. S. L. Ho, and L. Yang, Machine Learning Algorithms for Network Intrusion Detection. Cham: Springer, 2019.

[139] Misurata Freezone. "About Us." *Misurata Freezone*. https://www.mfzly.com/en/ (accessed Oct. 1, 2025).

[140] Libyan Iron and Steel Company. "About Us." *Libyan Iron and Steel Company*. [URL not accessible] (accessed Oct. 1, 2025).

[141] D. Robbins, Understanding Research Methods. Boca Raton, FL, USA: CRC Press, 2009.

[142] J. Spillan and J. Parnell, "Marketing resources and firm performance Among SMEs," European Management Journal, vol. 24, no. 2–3, pp. 236–245, 2006.

[143] J. I. Egerson, M. Williams, A. Aribigbola, M. Okafor, and A. Olaleye, "Cybersecurity strategies for protecting big data in business intelligence systems: Implication for operational efficiency and profitability," World Journal of Advanced Research and Reviews, vol. 23, no. 2, pp. 916–924, 2024.

[144] P. C. De Weerd-Nederhof, K. Visscher, J. Altena, and O. A. M. Fisscher, "Operational effectiveness and strategic flexibility: Scales for performance assessment of new product development systems," International Journal of Technology Management, vol. 44, no. 3–4, pp. 354–372, 2008.

[145] W. R. Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," Computers & Security, vol. 59, pp. 26–44, 2016.

[146] C. O. Victory, E. Promise, and C. N. Mike, "Impact of cyber-security on fraud prevention in Nigerian commercial banks," Jurnal Akuntansi, Keuangan, dan Manajemen, vol. 4, no. 1, pp. 15–27, 2022. doi: 10.35912/jakman.v4i1.1527

[147] A. F. Anoke, J. Igwebuike, C. A. Ogugua, and V. Odumuato, "Cyber security and business sustainability of quoted insurance firms in Nigeria," Journal of Research in Business and Management, vol. 9, no. 12, pp. 16–22, 2021.

[148] S. A. Ojeka, E. Ben-Caleb, and E.-O. I. Ekpe, "Cyber security in the Nigerian banking sector: An appraisal of audit committee effectiveness," International Review of Management and Marketing, vol. 7, no. 2, pp. 340–346, 2017. [Online]. Available: https://www.econjournals.com/index.php/irmm/article/view/4124