E-ISSN: 2997-9382

SemantJournals

American Journal of Technology Advancement

https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Balancing Data Accessibility and Security in Cloud-Based Business Intelligence Systems

Sanjida Akrer Sarna

Master of Science in Business Analytics, Trine University, USA

Md Imran Khan

Master of Science in information studies, Trine University, USA

Md Rakibuzzaman

Officer at Department of Banking Inspection, Bangladesh Bank, Dhaka, Bangladesh

Annotation

In the modern data-driven business world, Business Intelligence (BI) systems in cloud-management environments facilitate real-time decision making, scalable intelligence, and multi-user sharing of data. BI Cloud-based systems have transformed data business through scalable on demand access to analytics and decision-support tools. Organizational agility by democratizing data access in departments, yet pose a huge risk in terms of data security, data privacy and regulatory compliance. With rising business use of cloud BI platforms, the competing needs of maximum data access and highly secure systems are becoming an essential issue. This study examines this balance by examining real world security breach episodes with the Security Breach dataset that contains rich records of 173 security breaches in several firms and industries. The paper focuses on types of breach, points of origination of data, participation of third-party business associates and magnitude of compromised information. It is worth noting that the most common breaches identified effortlessly deal with breaches on network servers and portable gadgets and that external business associates make up a large percentage of these breaches. This paper shows via pattern recognition and descriptive analytics how simple cloud-based BI attacks with access controls failing, inadequately encrypted information and the absence of constant observation endangers the cloud-based BI setting through a typical variety of errors and mishaps. It also points out the trade-offs that organizations must make including empowering self-service analytics or ensuring stringent access-restrictions. The analysis provides a model that incorporates Zero Trust Architecture, Role and Attribute-Based Access Control, encryption standards and third-party control, to assist companies secure their Business Intelligence infrastructure in a way that is non-detrimental to the valid information flow. This study gives practical guidance to IT executives, security architectures, and data governance experts who want to ensure a fine balance between accessibility and security in cloud BI systems. The results stress the role of a multi-tier, policy-based solution to safeguard sensitive business information and keep the benefits of real-time cloud analytics.

Keywords: Business intelligence on the Cloud, Data Accessibility, Information Security, Security Breaches, Access Control Mechanisms and Zero Trust Framework.

1. Introduction

1.1 Background of Cloud-based BI Systems

In the digital transformation age, the field of Business Intelligence (BI) systems has evolved to offer cloud-based solutions that provide modern businesses with the ability to extract real-time insights to act on the huge amounts of available data. These products come as Microsoft Power BI, Tableau Online, and Google Looker, and use the cloud to provide analytics and reporting features virtually, exploiting cloud variations in terms of their scale, flexibility, and efficiency [1]. Cloud-based BI enables users to access dashboards, reports, and datasets through any device connected to the home network, which is not the case of a traditional on-premises BI tool that means that working in a remote and distributed environment is not an obstacle to making data-based decisions and empowering the remote working team. Increased usage of these platforms in businesses is attributed to lower cost of infrastructure maintenance, rapid deployment, and integration of various data sources at the same platform. Cloud BI systems provide collaboration and self-service analytics, so non-technical users will be able to analyze data on their own and find new insights without requesting any IT departments [2]. These BI platforms have APIs and connectors to a wide range of cloud services, ERP systems and databases and can process and visualize both structured and unstructured data to support strategic business initiatives including forecasting, customer segmentation, and operational efficiency analysis. But the more the data accessed using cloud BI in terms of volume and type of data, the more the complexities that accompany it on its handling and safety. Data governance, identity management, role-based access, and third-party integrations are some of the things that take another significant role in the security of sensitive information. Although the agility and innovation potential of cloud-based BI systems are not refuted, the fact that such systems are highly cloud-dependent in a certain sense creates a new set of dangers, the active fight with which organizations should engage [3]. Consequently, organizations need to consider the architecture on which the BI environment is laid down, flow of data, access policies and relevant security procedures, to make the appropriate tradeoffs of usability and security of the data.

1.2 Data Accessibility and Security Significance

The accessibility and the security of data are two inherent cornerstones of any successful cloud-based BI environment and balancing the two can make or break the ability of the enterprise to continue operating, securing the data [4]. On the one hand, data availability is the key requirement to empower decision-makers, cross-functional collaboration, and a data-driven culture of innovation. The ability to easily and swiftly distribute data to their firms that is relevant to the employees working across different departments in a firm will make employees quick to respond to the market trends, thereby optimizing the internal operations of a firm and enhancing the experiences of the customers [5]. Real-time access to analyses enables organizations to take action on insight fast, and compete in a rapidly changing environment. Conversely, more accessibility also inevitably leads to more serious consequences, such as the possibility of unauthorized entry into the system, information disclosure, and non-compliance with regulations, multi-tenant cloud systems [6]. Weakly set authorizations, absence of encryption, weak identity and access control may leave organizations to cyberattacks, malicious insiders or inadvertent data leakage. With the increasingly strict laws to regulate data including GDPR, HIPAA, and CCPA, among others, the risks of noncompliance with securing the available information are even higher as they might lead to lawsuits and a ruined reputation. Consequently, organizations need to adopt a two-pronged

approach that can only grant access to data to the authorized users but keeps the performance and usability. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), multi-factor authentication (MFA), and end-to-end encryption, are technologies that can be used in secure cloud BI without handicapping the end-user experience. It is not only a matter of technical task but rather a matter of governance and culture to find the right balance between accessibility and security, as it involves consistency across IT, compliance, and business functions. The result of such a balance between resources is an increase of trust, accountability, and resilience, in short major attributes of a mature data-driven enterprise in a cloud-first world.

1.3 Problem Statement

With the implementation of cloud-based Business Intelligence systems becoming more prominent in organizations to achieve intuitiveness in accessing and analyzing data it becomes increasingly more difficult to safeguard data achieving regulatory compliance. The same features that are so appealing to cloud BI platforms, ubiquitous access, multiple system integration, sharing real-time data are also the ones that create a security layer that should be taken care of, lest it results in extremely damaging data leaks [6]. Most enterprises have a hard time applying security systems to guard their data without limiting the efficiency of users. Thus, this study will explore potential strategies that companies can use to successfully achieve balancing data availability and protection in the cloud computing BI settings, referencing actual data breach attacks.

1.4 Research Objectives

This study is expected to accomplish the following to offer potent, countable guidelines in dealing with the issue of accessibility-security tradeoff in cloud BI systems:

- To analyze the main characteristics of cloud-based Business Intelligence systems which encourage data availability within organizations.
- To determine typical data security threats and type of breaches to cloud BI systems based on empirical information.
- To examine the correlation between third- party access and security weakness in BI platforms [7].
- In order to assess the current access control and encryption practices used in clouds BI.
- To suggest a structure which will help organizations to protect their BI data without affecting its accessibility.
- In order to propose optimal practices and technological treatments to avoid the risks of data breaches and perform BI operations with high levels.

1.5 Research Questions

These questions of this study are followed by the mention below:

1. What strategies are established to assist organizations in striking a balance between the necessity to render data to a wide audience and the necessity to ensure data security in cloud-based BI environments?
2. Which kind of security breaches are most popular within a cloud BI environment and what are the causes of those breaches?
3. What structures and technologies can protect the organizations access without verifying the functionality of the BI systems?

1.6 Significance of the Study

The proposed study is important as it considers a vital problem in the business community of contemporary data-driven business: the process of coping with the trade-offs that are inherent to the Business Intelligence systems stored in the cloud with concerns to accessibility and security [8]. As businesses attempt to transform into more agile and customer-focused entities, they are turning, to an ever-larger extent, toward BI platforms to discover the value of large amounts of data. the adoption of cloud computing, in addition to providing superior access and affordability, opens sensitive organizational information to the ever-changed cyber threats, misconfiguration, and regulatory risks. Gathering knowledge on the ways in which breaches are made through the real-world experience, being aware of the vulnerabilities of BI systems allow organizations to make sound decisions concerning their data governance strategies [9]. Using the database of the Security Breach dataset, this paper provides evidence-based analysis of real-life cases that can act as a source of advice to enhance the security architecture. The framework and recommendations suggested should assist businesses in ensuring a healthy security posture but at the same time, take full advantage of real-time, cloud analytics [10]. This study brings benefits to academic literature by closing the gap between the technical implementation and organizational practice thus providing a comprehensive point of view on the accessibility-security dilemma. Its results are useful to IT leaders, and security professionals, compliance officers and business analysts that are involved with deploying cloud BI tools, or managing cloud BI tools in a secure and compliant manner.

2. Literature Review

The Business Intelligence (BI) systems on the cloud base of business organizations have transformed the way organizations gather, analyze, and access information to make decisions. As much as they can enhance data access and responsiveness of operations, these platforms also pose various security risks [11]. The paper on cloud BI in this literature review investigates central themes of cloud BI regarding architecture, advantages, its security weaknesses, regulatory oversights, access control measures, and vulnerabilities [12]. The focus is made to comprehend the interrelation between security and accessibility in clouds. It defines the framework to evaluate how the organizations can protect BI systems without jeopardizing its data utility by recognizing common patterns of technology and practice.

2.1 Cloud-based business intelligence systems

Cloud-based Business Intelligence (BI) systems are computer systems installed in cloud architecture that allows business to collect, examine, and visualize data of all kinds of sources. As opposed to on-premises BI systems, cloud BI systems provide elasticity, reduce the cost of operation, and are more accessible [13]. They enable people to access real-time data in different locations, departments in different devices hence they are best suited in organizations that have geocentric workforces. Companies can easily incorporate databases, cloud applications, APIs and spreadsheets through minimum set up and maintenance to make actionable insights. Most of these platforms usually implement sophisticated features like data modeling, integration of machine learning, predictive analytics, and natural language query [14]. With the adoption of digitalization within organizations, cloud BI has been critical when it comes to informed decision-making, operational efficiency, and planning. The use of third-party servers and access via the internet, however, creates an issue of data governance, vendor lockup, and availability. The increasing embrace of self-service BI, in which business people directly access and process data themselves, adds yet more pressure on the necessity of effective access control measures. Collaboration with shared dashboards, report publishing and embedded analytics, which enhance agility, is also possible with modern BI systems, albeit with a reduced level of data exposure protection [15]. With the increased volume, speed and diversity of the business data, the cloud BI systems are playing a vital role in squeezing business intelligence out of raw data. Their reliance on cloud

services presents the need for the clearly defined frameworks of security, access control, and compliance so that the data is not misused or lost [16]. It is important to know the working mechanism of these systems and the weak points so that they can be implemented.

2.2 Accessibility of data and business productivity

BI systems facilitate access to data in cloud environments, which is critical in improving the business performance and responsiveness to strategy. Employees are also able to make quick and more informed decisions when the corresponding data is easily accessible to them and this enhances speed, productivity, and innovation [17]. The cloud-based business intelligence systems are accessible by using the browser, mobile applications, and real-time streaming to give the user access to real-time analytics wherever they are. Such access is especially important in the modern decentralized and partially distributed working environment where it would be inconvenient to wait on a decision-making process [18]. Self-service analytics, Self-service analytics can also benefit greatly from high data accessibility, as it allows the more casual users to browse data on their own, with less demand of IT teams and a faster rate of insight creation. But with more open and decentralized access brings more risks along themselves. Uncontrolled access to sensitive data sets may provide basis towards violation of compliance, leakages to intruders or misuse within the organization [19]. Although accessibility increases operational flexibility, it requires a close governance and technology oversight to guarantee that information is utilized in the right method [20]. Companies need to find an equilibrium between the user-friendly access and the concept of data minimization and the least privilege. Effective data accessibility generates cross-functional teamwork, minimizes decision windows, and dependence on historic reports. In addition, it will enable businesses to determine the tendency of the market, find the areas of operational inefficiencies, and serve customers with better custom experiences. However, when no proper security measures are put in place, the same ease of access translates to breaches and legal costs to the organizations [21]. Thus, the business efficiency on accessibility of data is realized with a careful design of technological systems data management policies so that the value is offered without any secrecy or in compliance.

2.3 Security Issues of the Clouds

Cloud computing businesses have certain security concerns that are quite pertinent to organizations using the BI systems. Data exposure because of a misconfigured cloud storage opened databases, poorly secured APIs, etc. is one of the leading concerns. Contrary to the conventional on-premise systems, the cloud brings with it multi-tenancy; that is, various organizations can share the same physical resources. This expands the threat of cross-tenants attack or data loss [22]. Also, any decentralized service like that of the clouds makes it the case where a vast amount of data is constantly in motion, being moved between and between systems, accessed through remote users and integrated with third-party services and this alone makes a variety of attack vectors. The other risk is that of insider threats which can occur when either the employees or contractors are given too many rights of access where they do not have control. Besides, most of the cloud based BI structures have complex data pipelines which would cut across environments and in this manner; it is hard to apply centralized security measures [23]. Hybrid and multi-sourced cloud environments are more complex and add the complexity of federated identities to Identity and Access Management (IAM). The other technical demands are the need to maintain secure APIs connection, orchestration of encryption keys and incorporation of threat detectors which keep abreast of the dynamism of cloud workloads [24]. Weak password management, sharing of data by mistake, are other human factors that contribute to vulnerability. Further, shared responsibility model in cloud computing where cloud provider takes responsibility of security that involves infrastructure security whereas data and access security is concerned with the customer organization requires the organizations to be proactive in knowledge and completion of responsibility. The lack of doing this may lead to breaches, loss of data and even reputation

[25]. Therefore, although the cloud environment increases scalability and performance, it requires highly specified security practices that have to be active on a continuous basis.

2.4 Regulating Frameworks (GDPR, HIPAA, SOC 2, and so on)

Regulatory frameworks are the legal and operational matters that are used to provide confidentiality of data, integrity, and availability of information on cloud based BI. General Data Protection Regulation (GDPR) is an arrangement that has presented strict guidelines on data protection to organizations that process personal data belonging to EU citizenry with focus placed on user compliance, data reduction, and data breach stand. Failure to comply will attract hefty financial fines [26]. The Health Insurance Portability and Accountability Act (HIPAA) on the other hand requires healthcare information security such as encryption, audit use of such, and physical protection. SOC 2 (System and Organization Controls) is an optional compliance model where technology and cloud computing companies mostly use it to prove they have controls over the way data is managed, privacy and availability [27]. All these regulations impose upon organizations the need to establish elaborate data control policies, implement risk evaluation impacts, and be accountable to the way data is accessed, shared, and stored. These compliance requirements are even more complicated in cloud BI systems for several reasons summing up to multiple third-party service providers and distributed data architecture. To cite one example, entities should make sure that the security standards about data processors and hosting providers are met and the entities have access logs to ensure the security of access. These frameworks may require encryption at rest and in transit, role-based access controls and secure authentication implementation [28]. It must also be in control of data ownership within an organization, despite the data being stored in third party cloud systems. These regulatory requirements are not only very important when it comes to legal compliance, but they are also very important in winning customer confidence and eliminating the financial and reputational cost of data breaches.

2.5 RBAC, ABAC and ZTA Access Control Models

Models of access control play an important role in determining the capability within the cloud-based BI systems of providing the data to the persons who should have right of access to it [29]. The most common system applied is the Role-Based Access Control (RBAC), which gives access rights to a user contingent on the job identification. This makes management easier and that users will only have access to the information they require in their duties [30]. The attribute-based access control (ABAC) is quite dynamic and situational oriented where access is granted according to a set of attributes including the role of the user, place, time of access and device used. ABAC is much more granular and flexible, a property that is Priority 1 in diverse user environments that employ remote access. RBAC and ABAC can co-exist in contemporary systems of BI to find a middle ground of the usability and position of security. Zero Trust Architecture (ZTA) is more integral and underpins the assumption that no user or system, both inside and outside, can be considered trustworthy by default. It needs persistent authentication, monitoring in real-time and extreme access authentication prior to accessing any data or system. To a cloud BI solution ZTA takes care of the specialized behavior and risk-based restrictions that are applied to even authenticated users. These models of access controls, in implementing them, guarantee non-unnecessary exposure of sensitive data, reduced insider threat, and regulatory compliance [31]. Accountability is also improved by use of effective access control that allows us to trace user activities on the audit logs. When done correctly and in place, these models can play the role of reducing the attack surface substantially and securing business-relevant information against its misuse. They are inarguably crucial avenues in reconciling security aspects with operational requirements in cloud BI contexts.

2.6 Real -World Incidents and Threat Landscape

The constantly changing environment of threats associated with cloud computing and usage of Business Intelligence platforms presents dangerous implications to companies [33]. The common forms of threats are phishing, credential stealing, Distributed Denial of Service (DDoS) attack, ransomware, and insider threats. With their behavior of using several integrations, remote access, and the deployment of APIs, Cloud-based BI systems are about as tempting to malicious actors. Practical cases have demonstrated that even big businesses could be driven to data breaches when cloud storage is misconfigured and cannot be properly encrypted or is accessed by third parties without control [34]. Circumstances like strained databases, stolen credentials, and privilege escalations demonstrate that there are vulnerabilities with each layer in a cloud construction. Most breaches are found after months of unauthorized traffic meaning that there exists a flaw in the real-time monitoring and alerting systems. The incidents that occur whenever vendors or other business partners serve as trojan horses complicate the security position of companies with shared cloud infrastructure even more. The ability of a single point of failure in a BI dashboard, connector, or dataset to enable attacks on millions of records has been widely established through high profile attacks [35]. These cases do not only lead to loss of money but also loss of faith of the population and responsibility of the regulations. In the cloud BI systems, the dynamic silo and distributed data properties necessitate the organizations to be alert all the time and be able to adapt fast. Indeed, in real-life case studies, a significant portion of the breaches was preventable with the implementation of stronger access controls, encryption standards and acceptance of governance policies. Such tendencies are driving why organizations should have proactive, multiple line defenses, beyond the perimeter-based security paradigms. It is important to understand the threat landscape to come up with resilient cloud BI architectures that are highly accessible and secure.

2.7 Research Gaps

The gap in research that directly focuses on the dual problem of both accessibility and security to data in cloud-based Business Intelligence systems is apparent despite the increased studies that are conducted regarding cloud security and Business Intelligence systems. The current literature available is more of technical nature of cloud security and/or the usability and its functionality of BI tools and is hardly containing the combination of the two elements in one comprehensive model [36]. The databases on the topic are prescriptive or conceptual most of the time, without being empirically tested on actual data breaches or case study. The issue here is that it presents a knowledge gap relative to the performance of these theoretical models when applied in real-life scenarios of compromise. There is another unexplored question about the third-party service providers and vendors, their impact on increasing or reducing the cloud BI risks, because more people resort to outside platforms to store their data, process it, and visualize it. Also, whereas access control models such as RBAC, ABAC, ZTA are described well, the ways to implement them and associated trade-offs in terms of the BI-specific settings are poorly understood [37]. Regulatory models are changing fast yet little is known on the practical implementation use of compliance mechanisms in multi cloud and hybrid business intelligence systems. Human factors, which include training, company culture, and enforcing internal policy, are given too little attention in terms of important aspects that affect the effectiveness of security in BI conditions. It is important to correct these research gaps to implement practical solutions where technical, organizational, and regulatory decisions can be consistent without interfering with the analytical capabilities of cloud based BI solutions.

2.8 Empirical Study

Integrating Business Intelligence with Cloud Computing: State of the Art and Fundamental Concepts (2021) by Hind El Ghalbzouri and Jaber El Bouhdidi is an empirical study that gives an explanatory approach to perceive how cloud computing extends scaling, cost-effectiveness, and flexibility of Business Intelligence systems. The authors review the present situation of cloud BI

focusing on its capacity to support large quantities of data and promote speed of deployment at the same time touching on the major security and availability issues which must be considered by organizations. Based on a comparative analysis of the scenarios of implementation, the study provides the advantages, risks, and technical issues of migrating BI to the cloud [1]. It supports the need of balancing performance and security frameworks and models, which are quite relevant to the objectives of this research. This paper contributes its own premise which consists in the premise that cloud BI is an attractive but complicated solution that needs careful integration approaches a good empirical source of information on the nature of difficulties and desirable approaches to design in cloud BI settings.

The article Cloud-Based Management Information Systems: Opportunities and Challenges for Small and Medium Enterprises (SMEs) authored by Shohanur Rahman and Mohammad Zobair Hossain (2024) reports a mixed-method study performed to estimate the value of SMEs in using cloud-based MIS. Based on the study of 200 SMEs, researchers found out that the use of cloud technologies has statistically improved operational efficiency (40 percent), cost reduction (35 percent) and user satisfaction (30 percent). The regression analysis also displayed the robust predictive connections between the cloud adoption and performance measures [2]. 40 percent of the respondents have reported the issue of data security as a bigger concern and 35 percent have observed the challenges of system integration, which naturally complies with the issues of cloud-based BI environments. Although this observation is based only on 5 respondents, it strengthens the statement that there must be a tradeoff between accessibility and security in the practical situation, especially when tightening security limits, the capabilities of a resource-constrained organization such as SMEs. This argument is based on empirical evidence as the cloud platforms can be helpful but they need to be carefully controlled to eliminate security threats and maintain data integrity.

The article Data-Driven Threat Analysis of Mohammed K. S. Alwaheidi and Shareeful Islam (2022) brings forward the d-TM approach to cloud-based infrastructures. The paper gives an emphasis on the fact that the security of cloud environments is complicated because of the diversity of data types and data location at the stage of its life cycle: storage, processing, and transmittance [3]. The d-TM model allows a systematic identification of the attack surfaces by integrating the threat analysis within management, control, and business abstraction levels. The demonstration in form of empirical use-case suggested by the study showed that there were four major threats to attack data in transit and at processing, which makes cloud-based Business Intelligence systems vulnerable to such threats and should remedy them. The results are valuable in indicating that it is crucial to prioritize data-level threats and ensure that multilayered defenses built across technical and organizational aspects are implemented. It is useful to note that the present paper provides strong arguments in line with the assumption that secure cloud BI systems should be based on more than just mere traditional mechanisms and should embrace data-centric, proactive threat modeling to ensure the safety of system resources and the continuity of the business.

In the article, CLOUD load balancing for storing the internet of things using deep load balancer with enhanced security, the authors study the possibility of applying DLB to balance cloud loads, especially in data-intensive IoT scenarios (K. Dhana Sree Devi et al., 2023). This suggested DLB model enhances the idea of indiscriminate load balancing by adopting normalization, optimization of resources and predictive load analysis of deep learning. Response Time, Makespan, Associated Overhead and Migration Time are key metrics which were used to benchmark DLB with the traditional methods of TA, ESCE, TA+ESCE. The outcomes depicted better results on scalability, cost effectiveness, and above all security which is vital to the cloud-based Business Intelligence systems [4]. Through incorporation of smart balancing algorithms, the paper outlines the crucial need to balance the need of making data available and minimizing security risks. It is an empirical

indication of the usefulness of intelligent automation and resilient models on delivering secure and high-performance data accessibility within cloud systems.

In S. Boopathi (2024) chapter titled Balancing Innovation and Security in the Cloud: Navigating the Risks and Rewards of the Digital Age, the author examines how cloud computing is both a source of opportunity and a source of serious threat in terms of security. The researchers give a multi-dimensional perception of cloud service and deployment models, risk analysis behaviour, and obligations to comply. It highlights the challenge experienced by organizations in matching their data protection strategies with the rapidly increasing rate of digital transformation brought about using clouds [5]. The chapter will offer accessible understanding based on both real-life examples and the discussion of new technologies, including the recent applications of AI, machine learning, and Zero Trust-models, suggesting how to navigate the competing values of cloud/innovation and security/regulatory needs. The input of this paper directly supports the essence of this study, which is the balance between accessibility and security of data in Business Intelligence architectures based on cloud organizations, as it proposes an approach that allows evaluating the implementation of the clouds in an organization, given the new challenges of digital security.

3. Methodology

This study utilizes a quantification case and data-conscious approach to study a sophisticated equilibrium of the availability and security of data in cloud-enhanced Business Intelligence (BI) systems. The paper evaluates observed security incidents data in the real world to identify trends, attack vectors and contextual threats, which would apply to cloud BI. The methodology would involve subsequent steps of data sourcing, cleaning, categorization, and visualization with the help of Python and Tableau. The stages are crucial in coming up with relevant visual constitution and insights consistent with the objectives of the study. This aims to give evidence-based findings that would lead to the informative, but also secure and accessible to practices in the contemporary deployment and governance of cloud BI systems.

3.1 Source and Selection of Data

The main data set in this research is called the Security Breach Facing Digital Threats: Data Security in the Digital Era, which is obtained out of a publicly available data library. The set of data records includes numerous data breach incidents that occurred over different time frames in different fields of the United States, such as healthcare, finance, and technology. The attributes in it would include type of breach such as theft, hacking, loss of device), date of breach, number of people affected, means of attack, and location or system through which the breach was made such as network servers, desktops, mobile devices [38]. This data is directly applicable in the study of security threats of cloud BI systems owing to the rich records of actual events that relate to digital assets, access vulnerabilities and breach of endpoints, a situation that is prevalent in BI systems. The fact that these fields are rather structured, the availability of unstructured summary makes the source rich both in quantitative and contextual analysis. This makes the dataset diverse in incident type and industry, which in turn supports the simulation of the depth of the real-world BI infrastructures. The presence of geographic and time data allows getting a longitudinal and regional overview of the evolution of breaches [39]. This dataset is comprehensive and relevant and can therefore be adopted as a good empirical basis for this research on the balance of data security and accessibility.

3.2 Data Preprocessing

To achieve the analytics validity and data quality, the data in the dataset underwent processing with Python and Tableau. First, record data with null, inconsistency, or irrelevant data were dropped or contextually imputed. Free fields that included the date like, Date of Breach, Breach Start, Breach End, and Date Posted or Update were standardized to be expressed in similar

datetime format so that a correct analysis of the temporal trends would be possible. Categorical data were normalized though unsafe naming on the same data fields by correcting inconsistent naming conventions and converging breach type. Some of the numerical fields such as determinations like Individuals Affected were checked to be accurate and inconsistency rectified where there were cases of repetitive responses and inconsistencies. derived variables were added to support further analysis [40]. A field was calculated as a difference between breach start and end dates, named as Breach Duration. The scores of the Breach Severity were deduced with figures depending on the number of individuals that have been influenced. The cleaned data would then be brought into Tableau where it would be formatted to be presented and be broken out statistically. Data comparisons by year, state and type of breach and the location of the data were made available by application of filters and parameters. This preprocessing stage guaranteed the further analyses were based on the stable coherent database and allowed to receive exact information on the risks of breaches related to BI.

3.3 Techniques and tools of Analysis

This study used the hybrid visual analytics and pattern recognition capabilities to understand the data breach trends applicable to the cloud based BI systems. The major instrument of data visualization was tableau because it was a powerful instrument in dynamic filtering, trend mapping, and geographic plotting [41]. Python was also used to carry out supporting analyses in order to validate data and provide exploratory statistics. Some of the visualizations that are generated entail line graphs (about breach trends over time), bar graphs (about breach types and breach methods), heatmaps (about breach locations), and ranked lists (about data location vulnerabilities). Such tools allowed studying the effects of breaches regarding their magnitude, time reference, place, and modality. Critical reviews were then made of each of these charts and main ideas obtained:

- ***Temporal Analysis:*** Years in which the volume of breaches or its severity was the greatest.
- ***Geographic Distribution:*** Identifying the states that breach and matching them with the areas with high BI adoption rates.
- ***Method/Type Analysis:*** Improving the ability to create awareness about the most dangerous or most common types of breach methodologies.
- ***Endpoint Vulnerability:*** Evaluation of the severity of breach exploiting the physical or logical place of the data.

The analytical methodology enabled a multiple insight into the intersection of accessibility and security of real-life events. Complex relationships are better conveyed using visual techniques, and help evidence-based recommendations to be made on the design and governance of a BI system.

3.4 Ethical Considerations

The ethical integrity of the research was taken care of very well as the research was done with only accessible and available secondary, anonymized, and public information. All personal and sensitive information on the dataset used are not present, including personally identifiable information (PII), the proprietary names of organizations not registered in the public record and sensitive personal records [42]. The data considered in the research is licensed under open terms and thus is to be utilized in education and analysis. This study is not aimed at criticizing or externalizing certain organizations but to extrapolate macro trends and draw practical outcomes in terms of cloud BI system resilience improvement efforts. Efforts were not made to reveal the data anonymity or cross-checking breach incident with other sources. In addition, ethics of data science has been adhered to in all the tools used in the analysis and the findings have been reported in a clear manner without bias. The data of this study is public; therefore, it did not face the need to be

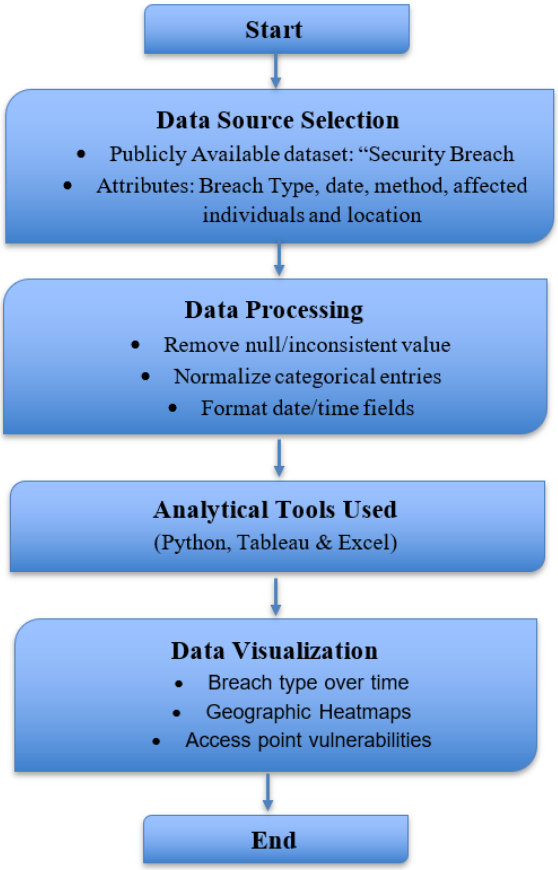
approved ethically [43]. Yet, there has been caution to ensure that breach-related information has not been harmed and misrepresented or misused during the study.

3.5 Limitations to the research

Although many interesting pieces of information can be derived by using the dataset, its limitations should also be mentioned. It is not every breach event that is reported in the open making some events in small private-based organizations to underrepresented the actual cases. The dataset too fails to make the distinction between cloud specific and on-premise states, and cloud BI relevance would need to be inferentially constructed [44]. Further, there are other areas where there is no standardization in the classification category, even though normalization is done during preprocessing. The scope of periods is also narrowed by the scope of the data. Such limitations do not disqualify the findings but as a limitation in generalizations. These are considerations that should be made when interpreting the options of the study.

3.6 Overview of Methodology Framework

Methodology Flowchart



The visual flow representation of the structured methodology employed in this research denoted as "Balancing Data Accessibility and Security in Cloud-Based Business Intelligence Systems" is as shown below. The framework explains the linear and logic process of realizing the research objectives using a quantitative and data-driven basis. The methodology will start with Data Source Selection, where publicly available data with the title Security Breach is taken into consideration because of broad coverage of the types of breaches, breach methods, breach location, and the impact of breaches over a long period of time. This dataset presents actual security incidents encountered in real life as they are of relevance to an organization in the public and the private sector which are surroundings in which systems which are based on clouds of BI get to be applied. After obtaining the dataset, preprocessing of data was done by using Python and Tableau to

normalize and clean the data. This covered the treatment of nulls, normalization of categorical names such as breach type and state, time-based fields like breach start and end times and dates [45]. This step played a major role in making the data analysis-ready and congruent. The third step, Tools Utilized in Analysis, was based in Python, data preparation, and Tableau, visualization. Such instruments facilitated the effective search of patterns, trends, and anomalies. The interactive dashboards and visual maps developed by Tableau were qualified to reflect the dense information about the breaches by means of a comprehensible presentation that people could comprehend. The Data Visualization stage was the process of developing several figures that demonstrate the trends in breaches according to the years, locations, type of breach, methods, and access points. Based on these visual outputs, there were grounds to interpret the extent and degree of the security issues within the cloud BI systems. Finally, such visual analyses gave rise to Interpretive Insights. These facts were directly used in: finding weak points in security architecture, regional susceptibilities, and suggesting the implementation of governance strategies that could succeed in balancing data access and protection. The flowchart reflects the structured process that can be repeated and used in this empirical research.

4. Result

This study displays the analytical results of the viewing and analyzing of the dataset concerning data breaches, with an emphasis on their impact on cloud-based Business Intelligence (BI) systems [46]. The findings examine some major trends in the chronology of breaches, geographical locations, breach categories, breach means and places of affected data. Both figures offer essential clues on the magnitude and the extent of threats that affect the availability and security of data. Such visual considerations form a basis upon which one can interpret the dilemma which organizations experience in determining how to ensure open access to vital data whilst maintaining a high degree of cybersecurity.

4.1 Affected Individual Based Breach Trends Analysis

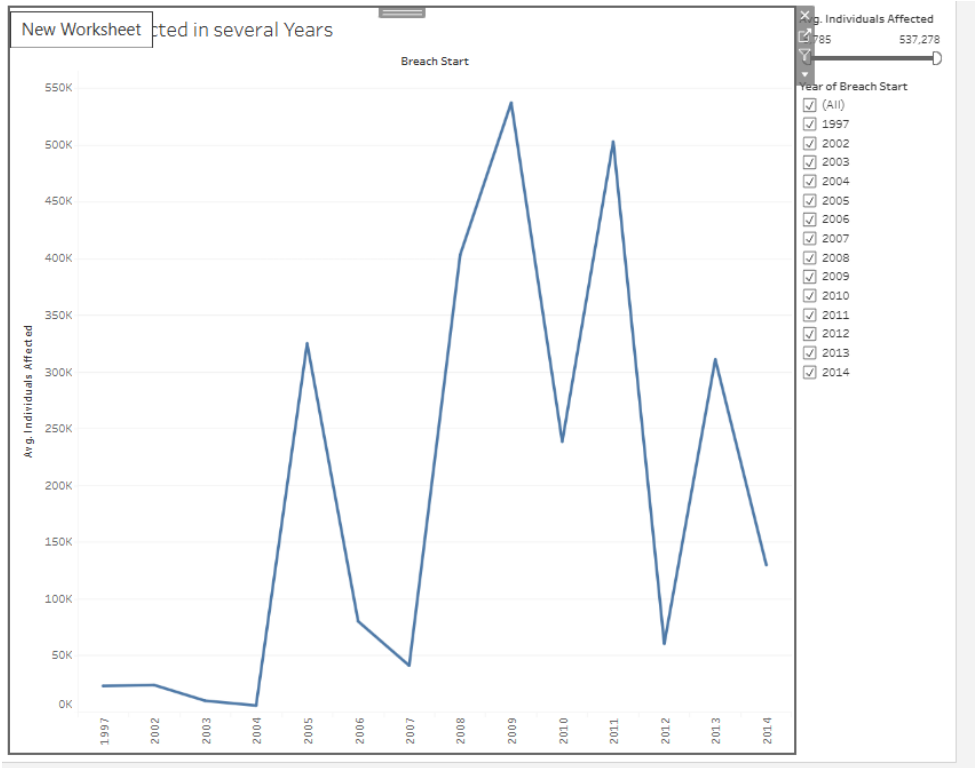


Figure 1: This Image illustrated to the Individual Based Breach Trends Analysis

Figure 1 shows a line diagram on the average figure of individuals exposed to data breaches annually between 1997 and 2014 using the Security Breach data set. The figure shows variations in the scale of violations over time, and it is easy to see how the severity of incidents changed over the specified period. Based on the graph, the amount of people who were affected was quite small and steady between the years 1997 and 2004. But there was an alarming increase in 2005, which means a major compromise or an accumulation of cases that exposed more than 300,000 individuals. Following a minor dip in the year 2006 and 2007, there is a sharp increase once again in 2008 and 2009, and the year 2009 seems to be the highest point wherein the average number of people affected has surpassed 500,000. This allows comparison with the general flow of digital transformation since the time other organizations also changed to digital systems and started using cloud-based BI tools and in many cases without established systems that secure them. Since 2010, it is evidently going down with some inconsistency but the average is still quite high compared to the pre-2005. In 2012 and 2014, the days of breach appear to have less impact, which could be either the result of better regulation compliance or better security maturity in organizations. The trends point to the fact that the spread of data on the cloud platforms is accompanied by growing vulnerability to cybersecurity attacks. Access controls, encryption, and the mechanisms of governance are specifically important due to their roles in striking the correct balance between usability and security in BI systems as highlighted by the upward trends.

4.2 Distribution of Breaches by geography: Number Breached by State

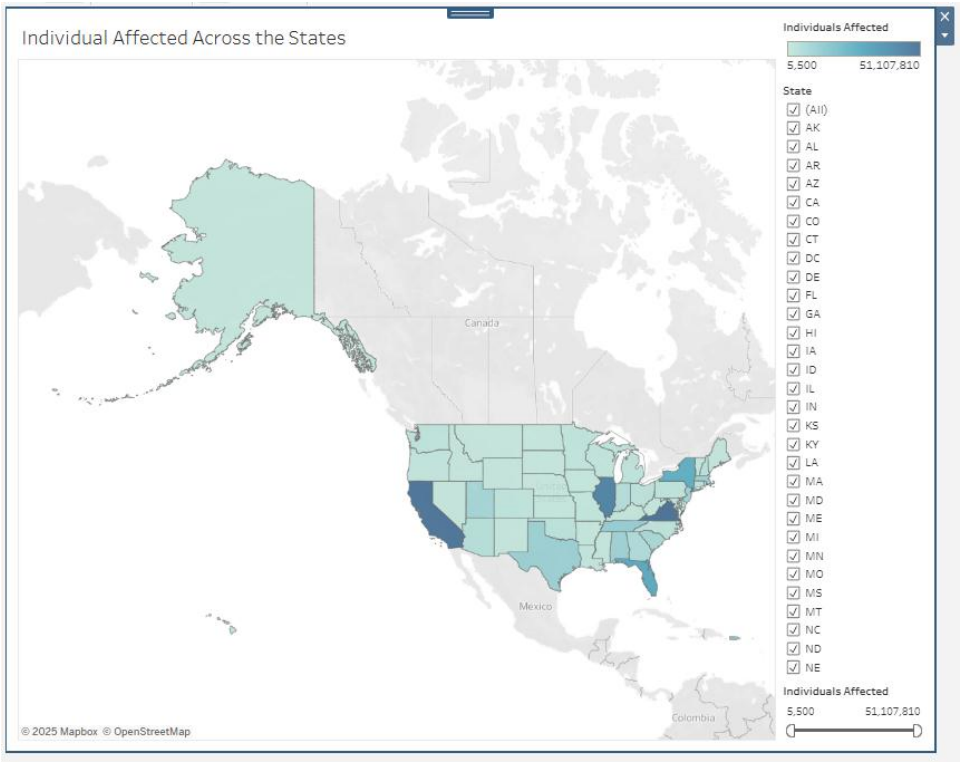


Figure 2: This Image presents a geographic heatmap of several individuals

Figure 2 presents a geographic heatmap of several individuals who have been subject to data breaches in various states of the United States, according to the Security Breach dataset. The darker the color the greater the number of persons affected in such an area. This image gives a nice explanation of the geographical aspect of the severity of a breach and which states were most affected by data compromise. As indicated in the map, California, Texas, Florida, and Illinois have been most greatly affected with millions of people being reported in each of those states. Dense populations and the location of head offices of many big businesses and health care providers in these states are all possible reasons why some large enterprises apply a BI in the

cloud on its working intelligence. In that regard, the statistics also indicate that there may be correlation between the use of BI systems and exposure to high security incidents especially in the technologically advanced or even data intensive areas. Comparatively, the states that experience fewer breaches include Wyoming, Montana, and South Dakota whose breach impacts are quite low. This can either be an occurrence of lesser breach occurrences or can be associated with underreporting or reduced cloud BI adoption. This geospatial analysis acknowledges the significance of the regional compliance-readiness and security activities, particularly in those organizations working in risky or densely populated regions. The figure reiterates the fact that the BI systems based on clouds create more attack surface as more data becomes accessible to individuals in different states and different locations [47]. It identifies the necessity of geographically course-grained security measures, vendor management, and compliance surveillance, so that the ease of access to the information in the high-traffic areas does not occur at a cost to the security level.

4.3 Breach Types and Their Effect on Individuals

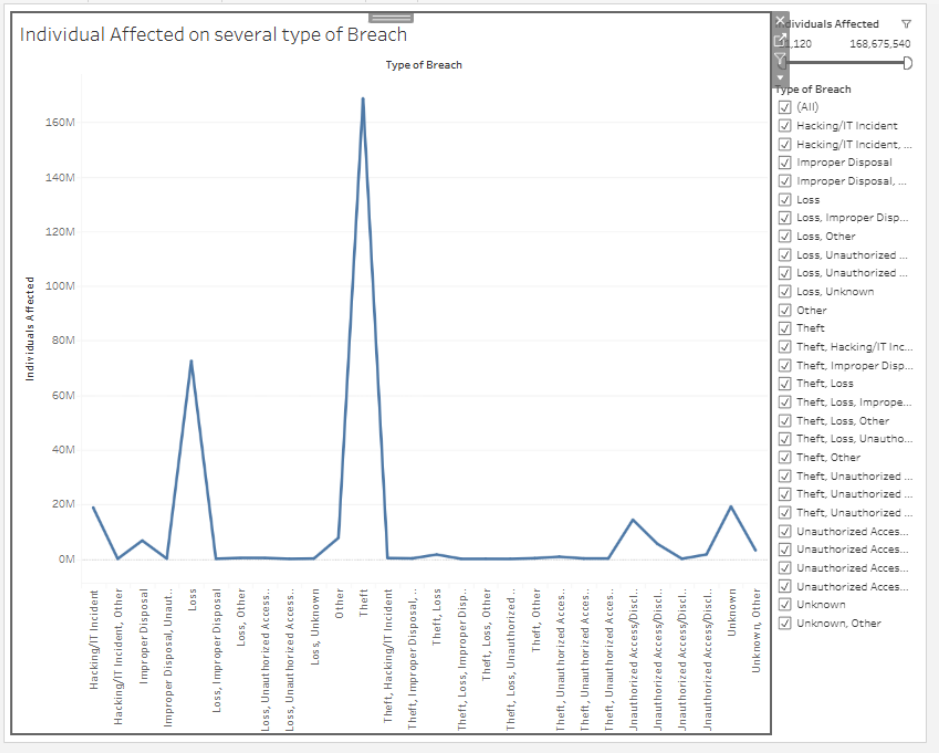


Figure 3: This image shows the number of people involved in different security breaches

As Figure 3 shows, according to the Security Breach dataset, there are a significant number of people affected by different types of security breaches. All types of breach, such as combinations of breach like Theft, Hacking or IT Incident or Loss, Unauthorized Access are plotted in relation to the number of affected individuals, providing the overview of which categories of breach bring the most significant results. The highest point in the graph is noting that there is a huge jump in the number of individuals who were affected by breach belonging to the category of Theft, Hacking/IT Incident with almost 170 million people being affected. This is an indication that both physical theft and cyberattacks are the most harmful in case of breaches in terms of magnitude. The following major breach types speak about the connection with the matter of the Improper Disposal, and the one of the Loss and Unauthorized Access, so it means that even the spoliation of data and the unsatisfactory practices of data administration is a leading cause of data exposure. Even within highly technological BI settings with well-established security protocols, other conventional breach vectors, such as stealing physical devices or loss because of a mistake, continue to affect millions of people, which indicates a lapse in protection. Such results reveal the

multi-factorial aspect of threats to cloud-based BI systems where threat sources are a combination of human error and cybercrime [48]. The wide range of breach types only underlines that the enhanced level of data accessibility, though positive in terms of business necessities, can lead to the occurrence of vast vulnerabilities unless the principles of security controls are implemented at each level. Since BI systems are connected to mobile devices, third-party applications, and external data sources, there is a risk of becoming subject to hybrid types of breach such as theft in addition to hacking. protected organizations must focus not only upon the protection of external attacks, but also develop internal practices such as secure data disposal, encryption standards and endpoint protection to mitigate risk. Such analysis supports the necessity of a layered, context-sensitive security approach that would adjust to various vectors of the breach that exist in cloud BI systems.

4.4 Methodological Assessment of Breaches More Influencing People

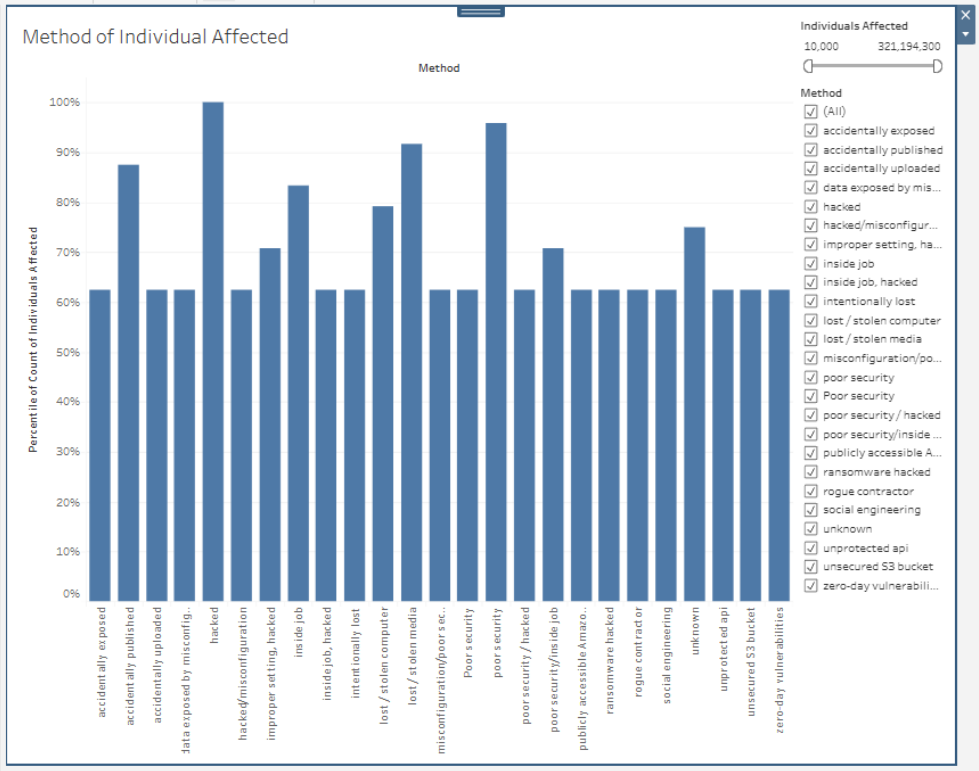


Figure 4: The figure depicts the distribution of breach methods according to the proportion of affected persons

The spread of methods of breach considering the percentage of people affected to do the breach is presented in figure 4 and it represents the frequency of attack methods exposure methods. The chart incorporates the wide variety of breach vectors, ranging between careless errors to more advanced hacking attacks, which signifies a diverse threat environment that cloud-based BI systems are at. The biggest hitters in the picture are “hacked/misconfiguration,” “improper setting, hacked, " and “inside job, hacked,” wherein more than 90 percent of all the individuals in the respective categories are infected. Brisk figures imply that one case of these types is likely to affect enormous amounts of sensitive information, giving the harsh implications of improper setup, inner malfeasance, and ineffectively fixed flaws in BI systems. The others are of importance and are named as accidently exposed, publicly accessible Amazon S3 bucket and unprotected API, which point to the vulnerability that tends to increase with the convenience of accessing data and the use of clouds. In many cases, such vectors are the result of weak authentication, the absence of encryption, and the inadequate application of access controls, which are even worse in open or self-service BI systems. Interestingly, even at a lower scale, there are

the occurrences of such miscellanea as social engineering, rogue contractor, and ransomware hacked, which proves the power of human factor and specific manipulation in the case of successful breach. The analysis underlines the importance of the fact that the enhancement of accessibility in cloud BI systems is to be performed with strong consideration of the data exposure, sharing, and storage. The combination of technical and human-based vectors of attack indicates that an integrated approach to security should be employed, including an automation of policy enforcement and employee awareness and enforcement. Therefore, given the recent trend within organizations towards democratization of data access provided with the help of BI platforms, it is important to note that the same organizations need to implement context-sensitive security measures to diminish the probability and consequences of breaches that such approaches are subject to.

4.5 Post-Breach analysis: The effect of breach closure on the subject of the breach

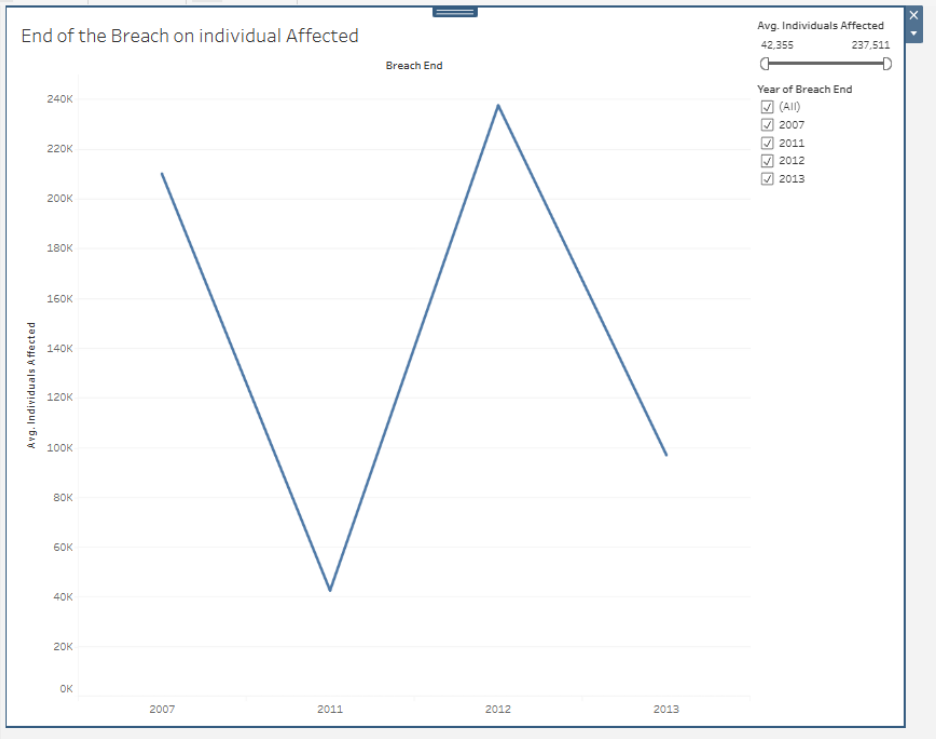


Figure 5: this picture illustrates to the mean number of people that are involved

The fifth figure offers a line graph showing the average number of people affected according to the year in which data breach terminated, with special concentration of 2007, 2011, 2012, and 2013. This time chart scheme gives good indication of the impact there is, after the incident of the data breaches not to mention as applied to the resolution work, mitigation, and the subsequent reverberations of the expose in cloud-based BI systems. What is shown in the chart is a fluctuating trend. The average number of infected people was high indeed, nearly 210,000 in 2007, which implies big-scale attacks that were either not addressed well or identified only in the late stages of their occurrence. By 2011 this number had fallen sharply to only over 40,000, which may have shown that breach response strategies were being improved, detected earlier, or effective mitigation practices enacted. But the mean cases have been on a spurt in 2012, reaching about 240,000, which became the highest point of the data collection. This revival can be explained by the fact that at that time the number of cloud BI platforms began to be more popular and the level of security was not advanced enough and the access controllers were not properly configured with the failure to encrypt the data. The abrupt increase in the time emphasizes the great impact that detection late and delayed response to the incident can result in enhancing the extent of attacks. This further dropped to below 100,000 by 2013 noting the enhanced control over security

governance that may have been attributed to the tight registration checks and active defense-related security measures [49]. The following analysis draws attention to the need to organize efficient incident response and rapid closure procedures to reduce the consequences of a data breach. Containment of security incidents in real time is critical in cloud-based BI systems, where data is continually accessed and shared in distributed settings, and whose portion of security measures in maintaining balance between data accessibility and protection. Effective preventive controls are not the only requirement organizations must take care of because they may want to maintain an agile response and recovery system to mitigate the damage caused to an organization by any significant security failure in the long run.

4.6 Breach Impact by Data Location: Ranking of Affected persons by source of Breach

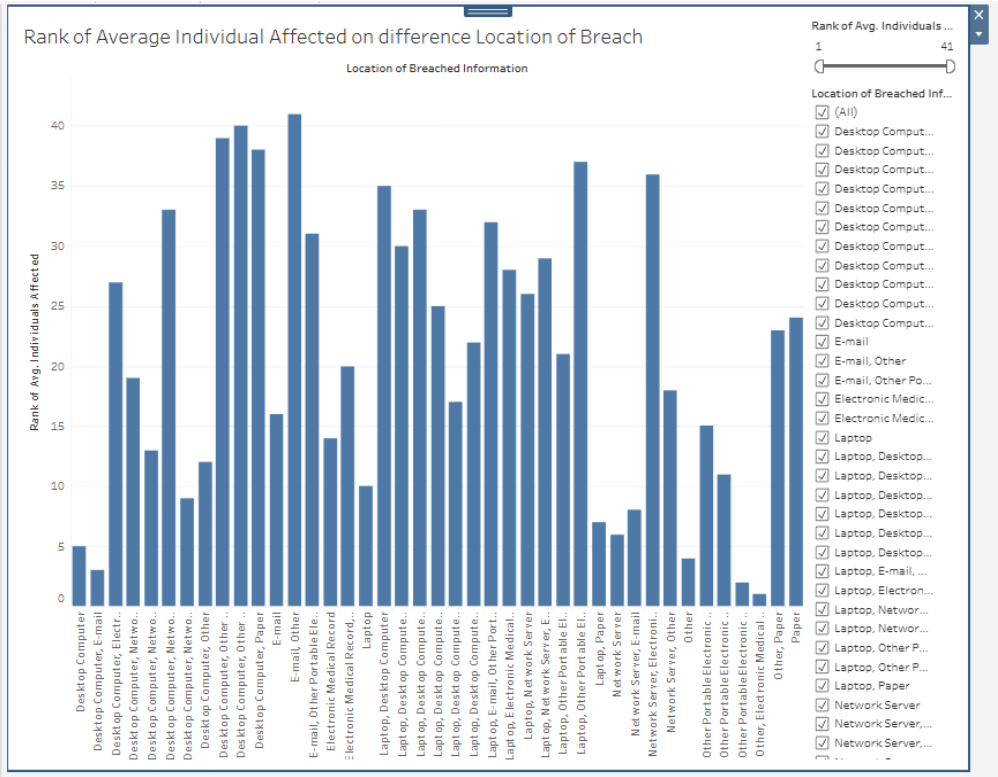


Figure 6: This Image shows the a graphical view of the rank of average persons affected in different places

Figure 6 presents a graphical view of the rank of average persons affected in different places where data breach has taken place, which is a pertinent piece of information on how different breach points are able to influence the severity of the breach. The figure classifies sources of data breach, e.g. desktop computers, laptops, network servers, emails, and EMR, according to the level of a person it impacts in assisting the identification of the riskiest locations of data repositories in businesses utilizing cloud-based BI systems. In the chart, desktop computers once combined with others, such as emails, external hard drives or even paper records, are always ranked high regarding the breach severity. This shows that an endpoint that involves a lot of user interaction and can be physically accessible are the best targets or vulnerable data spots. Such a combination as Desktop Computer and Other and Desktop Computer and Paper takes quite a high ranking, which can be explained by hybrid documentation systems, which erase digital-physical boundaries. Laptops and handheld devices are no exception, as they are also often found in the upper tier revealing the susceptibility in mobile data accessibility; which in a cloud BI environment is an essential attribute. Curiously, even network servers, which are more often classified as secure and centralized, are found in the upper positions when combined with endpoints, such as laptops or emails of different types, indicating the complexity of interconnected

access dangers. In this analysis, it is striking that a fundamental conclusion of the study is that, as much as cloud-based BI systems can make data more accessible, it also widens the scope of attack across multiple access points. The more extending and decentralized the data locations are, the more complicated and multilevel the security provision should be. To achieve such a balance, companies should consider having contextual access policies in their fields, recently encrypting data at rest and in transit, and introducing the endpoint detection and response (EDR) to all types of devices that connect to the BI landscape realms.

5. Dataset Overview

The main empirical base of this study will be the data set labelled as Security Breach- Facing Digital Threats: Data Security in the Digital Age. It gives an elaborate detail of a total of 173 reported cases of security breaches that have been reported in different organizations in the United States. The data points in the dataset contain such ordered attributes as breach type, breach method, breach date, occurrence state, the involvement of a business associate, and the number of affected individuals [60]. It also records the organization type, location where the data is breached such as on paper, network server, mobile device, and a summary of the incident. The data set displays the growing number of cyberattacks and their sophistication and highlights major obstacles related to unauthorized access, physical loss of devices, theft, and deliberate cyberattacks. Phishing, malware delivery, system intrusion are methods of attack; they are some of the common attack vectors in cloud-based BI systems. It also shows how vulnerable are personal health information (PHI), financial data, and others when there are no strong security frameworks. The dataset has a high contextual and quantitative value, which means that it is possible to analyze breach trends in time, geolocation heatmaps, access point vulnerabilities the severity by methods. All the information is anonymized, publicly placed on MIT license, and it is updated once every year, being compliant with ethical norms and research openness. This data set can be instrumental in bridging the gap between theoretical security models and their application in the real-world situations of breach dynamic to actionable insights of securing cloud-based BI systems.

6. Discussion and Analysis

This area focuses closely on the results of the study obtained using the dataset on security breaches with a critical perspective based on their application in cloud-based Business Intelligence (BI) systems. Examining the tendencies of breaches using their geographic concentration, techniques, and the possibility of attacks on devices, the discussion outlines the problems that must be overcome to provide organizations with the requirements of data accessibility leaving the security intact [46]. In this section, how the breach dynamics can influence strategic decisions in cloud BI architecture is investigated through 6 sub-analyses based on themes. It is hoped that these observations will help clarify how data-driven operational efficiency can be married with well-structured cybersecurity architectures so that operational accessibility is enabled by security policies and procedures rather than jeopardized by them.

6.1 Data Availability and Security Risk Interaction in Cloud BI

With Business Intelligence (BI) systems that are cloud-based, truly extraordinary access to data can be realized, in which individuals located in geographically diverse departments and locations are able to access and analyze data in real-time. This democratization of data is a strong tool of organizational agility, innovation and strategic decision making [47]. According to Figure 1 and Figure 3, the greater the openness, the higher the probability of data leak. Furthermore, this effect is even more likely in environments where the security policies and technical protection have failed to adapt to the usage. The sudden increase in the number of the affected people in the years of peak popularity of cloud usage is an indicator that making it easier to obtain business intelligence made it no less easy to be obtained by malicious actors. The vast number of types of

the breaches such as hacking, internal thefts, malware, and so forth makes it even harder to balance among the data sharing and protection [48]. The message is obvious, in case of the lack of appropriate governance, the access can soon become the exposure. Important security topics that should be taken into focus by the Cloud BI vendors and the adopting organizations include secure configuration, use of controls based on the roles of individuals, and continuous risk evaluation. The concept of security must not be regarded as an impediment to the accessibility but as a facilitator of the sustained, safe, and trusted usage of BI capabilities. It is a balancing act that is important to avail the real value in cloud-based analytics, without compromising data integrity and customer trust.

6.2 Paradigmatic Hotspots and Organizational Vulnerability

The spatial analysis of Figure 2 has shown a significant geographical contrast in the severity of breach with states of California, Florida, and Illinois being hit more disproportionately. These states serve as centers of the large-scale corporations, healthcare systems, and tech industries fields where the operations in these sectors highly depend on the use of data with the help of the BI systems that are based on clouds [49]. This unbalanced allocation shows that highly populated and data rich states have higher chances of being breached with high volumes because by the nature of the organization, the exposure to the usage of multifactor systems is more rampant. This geographical bias is caused by differences in local preparedness to cybersecurity, enforcement of regulations, and the maturity of infrastructure. The challenges experienced in these hotspots are increased in organizations. They also have to maneuver through the actual compliance demands of the industry in addition to the regional demands of privacy and breach response [50]. The leaders in cloud BI adoption are also the prime indicator of the dynamic threat environment. The lessons that have been learnt after these incidents occurred in these regions (how to vet vendors, train employees, and conduct proactive audits) can find application in other regions. This discussion supports that physical location is an issue of cloud BI security. Due to the nature of their geographical environment, the strategies that national and global organizations use to defend themselves should be based on a region-specific approach and the policies of data accessibility cannot neglect the local risks. Site-Specific Risk Profiling as a prerequisite to Enterprise-Wide Cloud BI Strategy Location-specific risk profiling ought to become part of the fabric of enterprise-wide cloud BI strategy.

6.3 Complication of the type of breaches and attack vectors

The wide array of breach categories presented in Figure 3 demonstrates that the range of cyber threats in the context of cloud-based BI has become highly complex. Breaches are no longer restricted to one-dimensional attacks but tend to be richer, in the sense of combining many tactics, e.g., physical theft coupled with hacking, or an insider attack exploiting the system misconfigurations. Such mixed breaches are most likely to impact the highest number of people implying that attackers are advancing at a higher rate than most organizations [51]. That is why this multifaceted Ness increases the stakes of security professionals and BI system architects. What is needed is not the security of perimeter networks but the security of all endpoints, users and roles third party integration. In addition, disposal of devices and documents as mentioned is still a major cause of mass breaches. The figures imply that simple cybersecurity hygiene is already a struggle even in the current age of technological development. Cloud BI systems further increase these risks because they are distributed and, in many cases, decentralized. Potential exploits can be offered by misconfiguration of uploaded user permissions, shared access keys and data export without oversight [52]. The answer is to take a multi-layered security stance building in Firewalls, Intrusion detection systems, encryption, identity access management (IAM) and user behavior analytics (UBA). Finally, the increasing sophistication of the techniques of breaching highlights the dire necessity that security should be more of an ever-evolving strategic process,

and less of a checklist. Proactive, predictive, and pervasive protection should be used in BI ecosystems, the data in which drives critical decisions in real-time.

6.4 Systemic vulnerabilities are captured by breach methods

Figure 4 gives a more detailed view on breaches occurrence, and the results are frightening. According to the methods, sophisticated cyberattacks are not the only cause of many breaches since they were made due to the overall poor security and a lack of protection of APIs as presented by variations that evolve as from "accidentally exposed" to "poor security" and "unprotected API." As an example, the APIs and cloud storage facilities such as Amazon S3 buckets used in cloud BI architecture have been repeatedly revealed to be publicly open because they were improperly configured [53]. These tools will present no difficulties in application and data transfer, but their generosity between systems makes them exposed to high risks unless secured adequately. More worrying are the breaches due to inside jobs or rogue contractors which signifies danger of uncontrolled access to data and the absence of any internal tracking. Such breaches are hard to trace and block unless very complex analytical behavior and strict access policies are in place [54]. These breach methods have reached the prevalence rates showing that there is a lack of association between speedy cloud adaptation and proper cybersecurity plan. Security procedures, where any exist, are usually behind, or have been implemented insufficiently, in a BI setting. Organizations do not infuse security in the design stage of BI system development in most of the cases. In the analysis, it is emphasized that cloud-based BI platforms require leaving the checkbox compliance alone and instead take up the demands to effect continuous monitoring, real-time alerting policies that have automation in effect [55]. Organizations are advised to take the methods of breaches as a mirror- they can have an idea on what to improve so that the incidence and severity of breaches can be tremendously reduced.

6.5 Timelines to Breach and Critical Incident Response

The dynamics of the number of people affected by the breach end year highlight the role of detection speed and response speed in reducing breach impact since the trend line in Figure 5 shows that the average number of affected individuals decreases with increased response speed. The statistics show that the longer the breach is unnoticed, the more people it can lead to an even exponential number. The sharp increase in 2012, at which point an average impact reached its height, points to a failure in terms of tracking the breach or a belated response [56]. These delays are especially harmful to the cloud BI environment where the data moves around the systems and the users at a fast rate. Without the detection of a compromise in a BI system, malicious parties can get access to critical reports required to make decisions, financial sensitivities, and customer information in weeks or months. This highlights the issue of the imperative of a clear-cut Incident Response Plan (IRP) along with a high-order fusion of security operations (SecOps) as part of BI systems. Real time anomaly detection, monitoring of logs, and using automation to alert early is vital in identifying threats [57]. What is more important, such tools should be supported with the organizational culture that values high speed and collaborative work across organizational functions in case of security events. Besides, the breach closure must be well-documented and forensic analysis should be made to ensure that the same case does not happen. An incident response is not merely a device to manage damage, but it is an element of operational resilience in the digital era. Fast detection and response should not be a novelty when it comes to cloud BI where we can expect the velocity of threats to be equal to the velocity of data access.

6.6 BI Access Endpoint and Vulnerability in Devices

Figure 6 reveals that the place of breached information, better termed as desktops, laptops, emails, and servers, is indeed very critical in impact calculation [58]. The Endpoints are one of the weakest links of a BI ecosystem, especially in cases where users access sensitive dashboard & datasets via personal or mobile devices over non-secure networks. Such combinations as Desktop

Computer & Paper, Laptop & Email or Net Server & External Drive are ranked high, which is an indication that data sprawl across various configurations and devices is a major cause of breach severity. The fact of hybrid work and the policy of BYOD (Bring Your Own Device) can only enhance such a state, and organizations have problems with controlling access and ensuring the same level of security on all touchpoints. Cloud BI systems may seek to be platform-independent (that is, available everywhere and everywhere). Increasing productivity, this doubles the exposure points. Security cannot therefore end at the server layer. The use of encryption on the device along with other forms of multi-factor authentication and vessel capacity to remotely delete data should be standard. Also, endpoint activities need to be monitored continuously by the endpoint detection and response (EDR) solutions. Security teams can get notice of possible breach before it happens because behavioral analytics can raise alerts on anomalous access times, unusual downloads, or other activity. This analysis underpins one of the main ideas of this study that the problem is not only technological, but also operation and cultural. To get a real balance between accessibility and security, companies must shift the scope of their interest toward the periphery where data is consumed, manipulated, and, in many cases, lost.

7. Recommendations

The organizations need to be strategic and proactive to balance the data accessibility and security in the cloud-based Business Intelligence (BI) system. The granular access control measures like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) must be implemented because they will make sure that the users will receive only the data that relates to their job, thus decreasing the likelihood of unauthorized access. A combination of regular security audits, real time-monitoring capabilities and automated anomaly detection mechanisms should be used to detect possible breaches and act quickly to stop them. Training of employees should be placed among a top priority, because human error and social engagement tricks still are among the most popular ways of data compromise; continued education in the sphere of cybersecurity can decrease exposure rather significantly [59]. Every sensitive data must be encrypted at both the medium and rest state to secure data even in case of the breach. To efficiently deal with breaches, it is essential to have a defined incident response plan (IRP), which includes clearly defined procedures of containment, communication, and data recovery. The BI components delivered by cloud providers could also assist companies by deploying compliance-ready functionality to comply with the regulatory requirements, like GDPR, HIPAA, and SOC 2, to minimize legal and reputational risk. The security of cloud BI systems should also be integrated into the systems at an early stage of the systems design and not when the systems are already deployed. When implemented as a set of measures, these acts not only enhance data protection structures but will also allow safe access to vital business intelligence with impediments, encouraging the trust, operational stability, and data-driven decision-making in agile business situations.

8. Future Works

Although this paper has presented valuable findings on the trade-off between data access and security in cloud-based Business Intelligence (BI) systems based on the real breach data, several avenues remain open to future exploration and improvement [57]. Future studies might enlarge the sample to cover additional events of breaches going on in other countries and concentrate specifically on cloud-indigenous BI systems to produce more evident connections among the cloud structure and the probability of a breach. The integration of operation cloud BI system logs and real-time threat intelligence feed traffic would enable the prediction modeling and detection of anomalies using machine learning algorithms, which would provide a more optimistic method of preventing threats. It is possible in future to investigate integrating Zero Trust Architecture (ZTA) and Decentralized identity systems, including blockchain-based access control, to determine their applicability in improving the accessibility and security of data in distributed environments [58]. With evolving regulations in the world, the other promising avenue is to

evaluate the dynamic nature of compliance challenges of multinational organizations that maintain BI systems in diverse jurisdictions. Insights into the vulnerability and best practice of a certain sector can also be exposed through comparative studies among: instances of industries divergence like healthcare, finance, and e-commerce [59]. A qualitative study in the form of a survey or interviews with BI practitioners, security analysts and cloud architects may provide a complement to the perspective on data-driven solutions to real-life operational issues and strategic advantages and disadvantages. Lastly, a standardized security-accessibility index or framework may be an effective practice that an organization may use as a benchmark of its system to determine its policies. These research directions open in the future will lead to development of more secure, effective, and regulatory compliant cloud BI platforms that will serve the businesses without interfering with the data quality or its availability.

8. Conclusion

This study has explored the intricate relationship between accessibility and security of data in cloud-based Business Intelligence (BI) environments based on the empirical data of actual breach cases and sought real practice-based answers. With the rising number of organizations moving their operations to cloud platforms in the efforts of achieving an agile operation and alignment of decisions to data, the need to ensure efficient security of data and the provision of ready access becomes a greater issue. The examination of the dataset named the Security Breach showed that security breaches continue to be common and diverse as much as the result of cyberattacks, theft of devices, unauthorized access and poor governance systems. These cases do not only threaten confidentiality and integrity of the essential data but also put organizations in danger of reputational and court consequences. Meanwhile, access policies so tight that they interfere with productivity, cooperation, decision-making in a timely manner is also among the main benefits of cloud BI systems. The results demonstrate the necessity of the middle ground that will not only depend on the current security best practices including Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), encryption, multi-factor authentication, and real-time monitoring of threats, but also allow smooth access to the authorized user. The aspect of human factors, poor training, and low level of policy enforcement also tells a lot about the role of organizational culture and employee awareness in stopping the breaches. The decision to implement regulatory compliance frameworks including GDPR and HIPAA is not something that should be considered a burden but the set of principles of a solid data governance process. This study can find in its analysis that the best balance cannot be obtained only through technical controls but through an entire strategy which includes policy creation, training of stakeholders, security-by design infrastructure.

9. References:

1. El Ghalbzouri, H., & El Bouhdidi, J. (2021). Integrating business intelligence with cloud computing: State of the art and fundamental concepts. Networking, Intelligent Systems and Security: Proceedings of NISS 2021, 197-213. https://link.springer.com/chapter/10.1007/978-981-16-3637-0_14
2. Rahman, S., & Hossain, M. Z. (2024). Cloud-based management information systems opportunities and challenges for small and medium enterprises (SMEs). Pacific Journal of Business Innovation and Strategy, 1(1), 28-37. https://scienceget.org/index.php/pjbis/article/view/14
3. Alwaheidi, M. K., & Islam, S. (2022). Data-driven threat analysis for ensuring security in cloud enabled systems. Sensors, 22(15), 5726. https://www.mdpi.com/1424-8220/22/15/5726
4. Devi, K. D. S., Sumathi, D., Vignesh, V., Anilkumar, C., Kataraki, K., & Balakrishnan, S. (2023). CLOUD load balancing for storing the internet of things using deep load balancer

with enhanced security. Measurement: Sensors, 28, 100818. https://www.sciencedirect.com/science/article/pii/S266591742300154X

5. Boopathi, S. (2024). Balancing Innovation and Security in the Cloud: Navigating the Risks and Rewards of the Digital Age. In Improving Security, Privacy, and Trust in Cloud Computing (pp. 164-193). IGI Global Scientific Publishing. https://www.igi-global.com/chapter/balancing-innovation-and-security-in-the-cloud/338354
6. Leonard, Z. (2023). Ethical Challenges in Cloud Environments: Redefining Business Intelligence with AI. https://www.researchgate.net/profile/Zander-Leonard/publication/387021658_Ethical_Challenges_in_Cloud_Environments_Redefining_Business_Intelligence_with_AI/links/675c55522547a96a923051da/Ethical-Challenges-in-Cloud-Environments-Redefining-Business-Intelligence-with-AI.pdf
7. Chowdhury, R. H. (2021). Cloud-Based Data Engineering for Scalable Business Analytics Solutions: Designing Scalable Cloud Architectures to Enhance the Efficiency of Big Data Analytics in Enterprise Settings. Journal of Technological Science & Engineering (JTSE), 2(1), 21-33. https://www.rsepress.org/index.php/jtse/article/view/93
8. Hosen, M. S., Islam, R., Naeem, Z., Folorunso, E. O., Chu, T. S., Al Mamun, M. A., & Orunbon, N. O. (2024). Data-driven decision making: Advanced database systems for business intelligence. Nanotechnology Perceptions, 20(3), 687-704. https://www.researchgate.net/profile/Esther-Folorunso-3/publication/382695215_Data-Driven_Decision_Making_Advanced_Database_Systems_for_Business_Intelligence/links/66a9e30775fcd863e5eae75d/Data-Driven-Decision-Making-Advanced-Database-Systems-for-Business-Intelligence.pdf
9. Hamidinava, F., Ebrahimy, A., Samiee, R., & Didehkhani, H. (2021). A model of business intelligence on cloud for managing SMEs in COVID-19 pandemic (Case: Iranian SMEs). Kybernetes, 52(1), 207-234. https://www.emerald.com/insight/content/doi/10.1108/k-05-2021-0375/full/html
10. Geetha, C., Neduncheliyan, S., & Khang, A. (2023). Dual access control for cloud-based data storage and sharing. In Smart Cities (pp. 321-336). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003376064-17/dual-access-control-cloud-based-data-storage-sharing-geetha-neduncheliyan-alex-khang
11. Abioye, T. E., Arogundade, O. T., Misra, S., Adesemowo, K., & Damaševičius, R. (2021). Cloud-based business process security risk management: A systematic review, taxonomy, and future directions. Computers, 10(12), 160. https://www.mdpi.com/2073-431X/10/12/160
12. Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. Microprocessors and Microsystems, 81, 103722. https://www.sciencedirect.com/science/article/abs/pii/S014193312030867X
13. Dornala, R. R. (2023). Ensemble security and multi-cloud load balancing for data in edge-based computing applications. International Journal of Advanced Computer Science and Applications, 14(8). https://www.proquest.com/openview/38ba356e19f34bb190e453029260ccb3/1?pq-origsite=gscholar&cbl=5444811
14. Rehan, H. (2024). AI-driven cloud security: The future of safeguarding sensitive data in the digital age. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 1(1), 132-151. https://newjaigs.com/index.php/JAIGS/article/view/89

15. Vashishth, T. K., Sharma, V., Kumar, B., & Sharma, K. K. (2024). Cloud-Based data management for behavior analytics in business and finance sectors. In Data-Driven Modelling and Predictive Analytics in Business and Finance (pp. 133-155). Auerbach Publications. https://www.taylorfrancis.com/chapters/edit/10.1201/9781032618845-9/cloud-based-data-management-behavior-analytics-business-finance-sectors-tarun-kumar-vashishth-vikas-sharma-bhupendra-kumar-kewal-krishan-sharma

16. Mishra, S., & Mishra, P. (2022). Analysis of platform business and secure business intelligence. International Journal of Financial Engineering, 9(03), 2250002. https://www.worldscientific.com/doi/abs/10.1142/S2424786322500025

17. Oloruntoba, O. (2024). Business continuity in database systems: The role of data guard and oracle streams. World Journal of Advanced Research and Reviews, 22(3), 2266-85. https://www.researchgate.net/profile/Oluwafemi-Oloruntoba/publication/389653148_Business_continuity_in_database_systems_The_role_of_data_guard_and_oracle_streams/links/67cb53487c5b5569dcb83577/Business-continuity-in-database-systems-The-role-of-data-guard-and-oracle-streams.pdf

18. Banerjee, S., Whig, P., & Parisa, S. K. (2024). Leveraging AI for Personalization and Cybersecurity in Retail Chains: Balancing Customer Experience and Data Protection. Transactions on Recent Developments in Artificial Intelligence and Machine Learning, 16, 16. https://www.researchgate.net/profile/Somnath-Banerjee-13/publication/391460557_Leveraging_AI_for_Personalization_and_Cybersecurity_in_Retail_Chains_Balancing_Customer_Experience_and_Data_Protection/links/681979cedf0e3f544f5210cf/Leveraging-AI-for-Personalization-and-Cybersecurity-in-Retail-Chains-Balancing-Customer-Experience-and-Data-Protection.pdf

19. Khunger, A. (2023). Fault-Tolerant Load Balancing In Cloud-Based Financial Analytics: A Reinforcement Learning Approach. International Journal of Innovation Studies. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5146521

20. Bauskar, S. (2024). A Review on Database Security Challenges in Cloud Computing Environment. Available at SSRN 4988780. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4988780

21. Akinbolaji, T. J. (2024). Novel strategies for cost optimization and performance enhancement in cloud-based systems. International Journal of Modern Science and Research Technology.

22. Ravichandran, P., Machireddy, J. R., & Rachakatla, S. K. (2022). AI-Enhanced data analytics for real-time business intelligence: Applications and challenges. Journal of AI in Healthcare and Medicine, 2(2), 168-195. https://www.researchgate.net/profile/Jeshwanth-Reddy-Machireddy/publication/389139259_AI-Enhanced_Data_Analytics_for_Real-Time_Business_Intelligence_Applications_and_Challenges/links/67b6b9bf8311ce680c6b089c/AI-Enhanced-Data-Analytics-for-Real-Time-Business-Intelligence-Applications-and-Challenges.pdf

23. Aljawarneh, S., & Malhotra, M. (Eds.). (2020). Impacts and Challenges of Cloud Business Intelligence. IGI Global. https://books.google.co.in/books?hl=en&lr=&id=OXkSEAAAQBAJ&oi=fnd&pg=PR1&dq=Balancing+Data+Accessibility+and+Security+in+Cloud-Based+Business+Intelligence+Systems&ots=5PoSTTW_-r&sig=bGSFUPwyrJDNjzbMmARb9DqzEBo&redir_esc=y#v=onepage&q=Balancing%20Data%20Accessibility%20and%20Security%20in%20Cloud-Based%20Business%20Intelligence%20Systems&f=false

24. Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. Alexandria Engineering Journal, 84, 275-284. https://www.sciencedirect.com/science/article/pii/S1110016823009651

25. Yathiraju, N. (2022). Investigating the use of an artificial intelligence model in an ERP cloud-based system. International Journal of Electrical, Electronics and Computers, 7(2), 1-26. https://d1wqtxts1xzle7.cloudfront.net/85514837/IJEEC_01_march_april_2022-libre.pdf?1651730943=&response-content-disposition=inline%3B+filename%3DInvestigating_the_use_of_an_Artificial_I.pdf&Expires=1751011213&Signature=KGYNT7lIyrv~m4gSc-nc1fcktFw-~N4VL9mAQn7z5O-lx7ivM5X8AXJ5bGHtE7CdN2QcyWKLcroWqlTP5sKFItt~B4K6pWTbEqMIGnRtrUaNnUIo~Y81o~A0zwuh7fcCTFiWsonxICaeNnLWGgNdrnPC~85sqp3KjjBz-uvKcuQYBR8saSj7NcZY4u3Xa3ucGGizd1HcX33QuyOPFARSP0KjOzyCOKVYX7YYzKiq1u9XzYpeO38gzpRcKk9MA8-RIIOAdi6-DeWCrK1Ufgfjy5NqpkLNCl-YKmSnkmeP1Knywe205DSwmUPSLLcX6~cYGNpfh8Tz9APGmJC4D7hwkw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

26. Moparthi, N. R., Balakrishna, G., Chithaluru, P., Kolla, M., & Kumar, M. (2023). An improved energy-efficient cloud-optimized load-balancing for IoT frameworks. Heliyon, 9(11). https://arxiv.org/abs/2304.13738

27. Moparthi, N. R., Balakrishna, G., Chithaluru, P., Kolla, M., & Kumar, M. (2023). An improved energy-efficient cloud-optimized load-balancing for IoT frameworks. Heliyon, 9(11). https://www.cell.com/heliyon/fulltext/S2405-8440(23)09155-7

28. Raghavendar, K., Batra, I., & Malik, A. (2023). A robust resource allocation model for optimizing data skew and consumption rate in cloud-based IoT environments. Decision Analytics Journal, 7, 100200. https://www.sciencedirect.com/science/article/pii/S2772662223000401

29. Daruvuri, R., Ravikumar, R., Mannem, P., & Aeniga, S. R. (2024). Augmenting Business Intelligence How AI and Data Engineering Elevate Power BI Analytics. International Journal of Innovative Research in Computer and Communication Engineering, 12(12), 13012-13022. https://www.researchgate.net/profile/Pravallika-Mannem-2/publication/386568132_Augmenting_Business_Intelligence_How_AI_and_Data_Engineering_Elevate_Power_BI_Analytics/links/67660b4f00aa3770e0af4c40/Augmenting-Business-Intelligence-How-AI-and-Data-Engineering-Elevate-Power-BI-Analytics.pdf

30. Bussa, S. (2023). Enhancing BI tools for improved data visualization and insights. International Journal of Computer Science and Mobile Computing, 12(2), 70-92. https://d1wqtxts1xzle7.cloudfront.net/119982050/V12I2202307-libre.pdf?1733248136=&response-content-disposition=inline%3B+filename%3DEnhancing_BI_Tools_for_Improved_Data_Vis.pdf&Expires=1751011380&Signature=fkqcnSziOe6WEuK3HhFTriNiFoUJQX9lWqfymmESGvcLqBQ4DFbWsUuYUatkXkvyVavX1h4V2Nt3DGpyxu~woBLXaHIHcwphLK9A9634yTgL2ueBNVClGSiK~c59M1t6gwjEqHZXautY9UD36nLSSZBcctrQLC-aFI8ceXOwTqeI4y4sJrjETXmM6QROuX1GCfk4Pc2zslZQpMwRrFwUOzo9vRWXYTzF9brUCmRz1D4bQmzBLbBMw5SfxtFe-XCdRz4at9soiQg1SfXF4Q2p9Aj9IwzC98rPQ4MWqtYTtHwEf0m70YOd4qLHKCfCVaR12Pd0Lwe7O2RD0up9~R4OOA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

31. Polamarasetti, A. (2024, November). Role of Artificial Intelligence and Machine Learning to Enhancing Cloud Security. In 2024 International Conference on Intelligent Computing and

Emerging Communication Technologies (ICEC) (pp. 1-6). IEEE. https://ieeexplore.ieee.org/abstract/document/10837120

32. Tatineni, S. (2023). Cloud-Based Reliability Engineering: Strategies for Ensuring High Availability and Performance. International Journal of Science and Research (IJSR), 12(11), 1005-1012. https://d1wqtxts1xzle7.cloudfront.net/109038178/SR231113060258-libre.pdf?1702686624=&response-content-disposition=inline%3B+filename%3DCloud_Based_Reliability_Engineering_Stra.pdf&Expires=1751011623&Signature=GwhBiS7dKKPJ3Ekk4mjM2Mx2C5-Tem2WSZeIoPknQlNgLC9eqxcqFSsozgsB7F~aCt1ajwUAS-4mUAps2Iu7UFM8OgNRxRHEAK2hPF27cujf2ZJIJaT0M9nOFIHkqZ6faDTTEsj4z1KxGvjUtYa2BI~kGPQp~Hs1Rbm1FjfjV-Y393k~XxgCTogDysFh5DPcFrmuNv6W-uMeSmaRIgruBcPVXe4j~3ZDePoXKR1rhhZOg4MP6m2POpb1LGahEa-IVJDIFheT6VNQ8xfWaSQIs4n5q11xzk-o8hjAQ-gtv3EG2Kg0hg6QCiEFFXzHh7e1wPOY7DpZ2~lKxzvTkqnHiQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

33. Egbuhuzor, N. S., Ajayi, A. J., Akhigbe, E. E., Agbede, O. O., Ewim, C. P. M., & Ajiga, D. I. (2021). Cloud-based CRM systems: Revolutionizing customer engagement in the financial sector with artificial intelligence. International Journal of Science and Research Archive, 3(1), 215-234. https://www.researchgate.net/profile/Nnaemeka-Egbuhuzor/publication/389906574_Cloud-based_CRM_systems_Revolutionizing_customer_engagement_in_the_financial_sector_with_artificial_intelligence/links/67d84acc7d56ad0a0f059b5d/Cloud-based-CRM-systems-Revolutionizing-customer-engagement-in-the-financial-sector-with-artificial-intelligence.pdf

34. Das, J. (2020). Leveraging Cloud Computing for Medical AI: Scalable Infrastructure and Data Security for Advanced Healthcare Solutions. INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS, 7, 504-514. https://www.researchgate.net/profile/Jyotipriya-Das/publication/389782177_Leveraging_Cloud_Computing_for_Medical_AI_Scalable_Infrastructure_and_Data_Security_for_Advanced_Healthcare_Solutions/links/67d1d741bab3d32d84414f4f/Leveraging-Cloud-Computing-for-Medical-AI-Scalable-Infrastructure-and-Data-Security-for-Advanced-Healthcare-Solutions.pdf

35. Boppana, V. R. (2021). Ethical Considerations in Managing PHI Data Governance during Cloud Migration. Educational Research (IJMCER), 3(1), 191-203. https://www.ijmcer.com/wp-content/uploads/2024/10/IJMCER_Z0310191203.pdf

36. Boddapati, V. N., Sarisa, M., Reddy, M. S., Sunkara, J. R., Rajaram, S. K., Bauskar, S. R., & Polimetla, K. (2022). Data migration in the cloud database: A review of vendor solutions and challenges. Available at SSRN 4977121. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4977121

37. Singha, S., & Singha, R. (2023). Protecting data and privacy: cloud-based solutions for intelligent transportation applications. Scalable computing: practice and experience, 24(3), 257-276. https://scpe.org/index.php/scpe/article/view/2381

38. Kendyala, S. H. (2023). High Availability Strategies for Identity Access Management Systems in Large Enterprises. Available at SSRN 5074869. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5074869

39. Mir, A. A. (2024). Optimizing mobile cloud computing architectures for real-time big data analytics in healthcare applications: Enhancing patient outcomes through scalable and

efficient processing models. Integrated Journal of Science and Technology, 1(2). https://ijstpublication.com/index.php/ijst/article/view/10

40. Wang, Y., & Kogan, A. (2020). Cloud-based in-memory columnar database architecture for continuous audit analytics. Journal of Information Systems, 34(2), 87-107. https://publications.aaahq.org/jis/article-abstract/34/2/87/1173/Cloud-Based-In-Memory-Columnar-Database

41. Parisa, S. K., Banerjee, S., & Whig, P. (2023). AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure: A Next-Generation Approach. International Journal of Sustainable Devlopment in field of IT, 15(15). https://www.researchgate.net/profile/Somnath-Banerjee-13/publication/390098789_AI-Driven_Zero_Trust_Security_Models_for_Retail_Cloud_Infrastructure_A_Next-Generation_Approach/links/67df803dfe0f5a760f896295/AI-Driven-Zero-Trust-Security-Models-for-Retail-Cloud-Infrastructure-A-Next-Generation-Approach.pdf

42. Pasham, S. D. (2023). Privacy-preserving data sharing in big data analytics: A distributed computing approach. The Metascience, 1(1), 149-184. http://yuktabpublisher.com/index.php/TMS/article/view/130

43. [39]. Dubey, H. A. R. S. H. I. T., Kumar, S. U. D. H. A. K. A. R., & Chhabra, A. N. U. R. E. E. T. (2022). Cyber security model to secure data transmission using cloud cryptography. Cyber Secur. Insights Mag, 2, 9-12. https://insights2techinfo.com/wp-content/uploads/2022/11/Cyber-Security-Model-to-Secure-Data-Transmission-using-Cloud-Cryptography_final_2.pdf

44. Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int J Res Publ Rev, 5(11), 1-15. https://www.researchgate.net/profile/Foluke-Ekundayo/publication/386144447_Predictive_Analytics_for_Cyber_Threat_Intelligence_in_Fintech_Using_Big_Data_and_Machine_Learning/links/67469330f309a268c00e696c/Predictive-Analytics-for-Cyber-Threat-Intelligence-in-Fintech-Using-Big-Data-and-Machine-Learning.pdf

45. Srivastava, G., S, M., Venkataraman, R., V, K., & N, P. (2022). A review of the state of the art in business intelligence software. Enterprise Information Systems, 16(1), 1-28. https://www.tandfonline.com/doi/abs/10.1080/17517575.2021.1872107

46. Kumar, R., & Agrawal, N. (2023). Analysis of multi-dimensional Industrial IoT (IIoT) data in Edge–Fog–Cloud based architectural frameworks: A survey on current state and research challenges. Journal of Industrial Information Integration, 35, 100504. https://www.sciencedirect.com/science/article/abs/pii/S2452414X23000778

47. Fatima, A., Khan, T. A., Abdellatif, T. M., Zulfiqar, S., Asif, M., Safi, W., ... & Al-Kassem, A. H. (2023, March). Impact and research challenges of penetrating testing and vulnerability assessment on network threat. In 2023 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-8). IEEE. https://ieeexplore.ieee.org/abstract/document/10111168

48. Kundavaram, V. N. K. (2024). Automated Data Migration in Cloud Environments: Challenges and Solutions. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 15(6), 262-274. https://d1wqtxts1xzle7.cloudfront.net/122798319/AUTOMATED_DATA_MIGRATION_IN_CLOUD_ENVIRONMENTS_CHALLENGES_AND_SOLUTIONS_IJCET_15_06_022-libre.pdf?1747279821=&response-content-disposition=inline%3B+filename%3DAUTOMATED_DATA_MIGRATION_IN_CLOUD_

ENVIRO.pdf&Expires=1751012621&Signature=b5T89L~lKXVVXjMwZCQxV-ACLTl-VffhaUQzohbrvTBWey5m0UpRPp7OI7Wko4Vyd6lqqNn2zl~KzuKW3LM0YFU1DYy0Q~K7T6XYwhA~zGgSdMcUDSpTeJc3Ptj43~9Shc1KmyXwQqWNqoG-1OJQY7v0hYfSVj4zcuaeP-9~q0L~rnrOqrXhEVB322cRIBw9bunbLIPGiQMJgrXRoUJ7l~BZZEih9v0VUV2rZ4cwvF7NPA-gyLzETQiwdDCm-OCCPFMg9xVV~dFCk4SAuwbLi4ya3~BQQawsADnI4zKe7IHgnMqI2vFPlGnm8TMAA3moB812af49AvLc97nVzMAzqQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

49. Katari, A. (2022). Data lakes and Optimizing Query. Available at SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4984244

50. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532. https://link.springer.com/article/10.1007/s11227-020-03213-1

51. Ravi, V. K., & Ayyagari, A. (2023). Data Lake Implementation in Enterprise Environments. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5068537

52. Tawfeeg, T. M., Yousif, A., Hassan, A., Alqhtani, S. M., Hamza, R., Bashir, M. B., & Ali, A. (2022). Cloud dynamic load balancing and reactive fault tolerance techniques: a systematic literature review (SLR). IEEE Access, 10, 71853-71873. https://ieeexplore.ieee.org/abstract/document/9815255

53. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16. https://www.mdpi.com/2079-9292/11/1/16

54. Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. World Journal of Advanced Engineering Technology and Sciences, 10(2), 155-181. https://pdfs.semanticscholar.org/46fd/8be19bebe31752f113312772dd18b04290b8.pdf

55. Ikegwu, A. C., Nweke, H. F., Anikwe, C. V., Alo, U. R., & Okonkwo, O. R https://link.springer.com/article/10.1007/s10586-022-03568-5

56. Dornala, R. R. (2023, August). An advanced multi-model cloud services using load balancing algorithms. In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1065-1071). IEEE. https://ieeexplore.ieee.org/abstract/document/10220892

57. Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024, March). Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 494-499). IEEE. https://ieeexplore.ieee.org/abstract/document/10489749

58. Sourav, M. S. A., Khan, M. I., & Akash, T. R. (2020). Data Privacy Regulations and Their Impact on Business Operations: A Global Perspective. *Journal of Business and Management Studies*, *2*(1), 49-67.

59. Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. Magna Scientia Advanced Research and Reviews. https://www.researchgate.net/profile/Olukunle-Amoo/publication/387727760_Advancing_cloud_networking_security_models_Conceptualizing_a_unified_framework_for_hybrid_cloud_and_on-premise_integrations/links/677992c6894c55208542f50c/Advancing-cloud-networking-

security-models-Conceptualizing-a-unified-framework-for-hybrid-cloud-and-on-premise-integrations.pdf

60. Sandhu, A. K. (2021). Big data with cloud computing: Discussions and challenges. Big Data Mining and Analytics, 5(1), 32-40. https://ieeexplore.ieee.org/abstract/document/9663258
61. Kumar, S., & Aithal, P. S. (2023). Tech-Business Analytics in Secondary Industry Sector. International Journal of Applied Engineering and Management Letters (IJAEML), 7(4), 1-94. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4674849
62. Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. Asian Journal of Research in Computer Science, 17(12), 66-88. http://journal.submanuscript.com/id/eprint/2644/
63. Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. Big Data and Cognitive Computing, 6(4), 101.
64. Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing data security of cloud based lms. Wireless Personal Communications, 130(2), 1123-1139. https://link.springer.com/article/10.1007/s11277-023-10323-5
65. Md, R., & Tanvir Rahman, A. (2019). The Effects of Financial Inclusion Initiatives on Economic Development in Underserved Communities. *American Journal of Economics and Business Management*, *2*(4), 191-198.
66. Tanvir Rahman, A., Md Sultanul Arefin, S., Sanjida Akter, S., & Md, R. (2023). Develop Automated Systems that Gather and Analyze Threat Data to Protect Business Systems Automatically from Cyberattacks. *American Journal of Engineering, Mechanics and Architecture*, *1*(6), 90-113.
67. Dataset Link: https://www.kaggle.com/datasets/xontoloyo/security-breachhh