International Journal of Data Informatics and Intelligent Computing (IJDIIC)
Vol. 4, No. 4, December 2025, pp. 28~40
DOI: 10.59461/ijdiic.v4i4.230

Orchestrating Data Leaks in Multi Cloud: Projects in Controlled Environments Approach

Rachel John Robinson[1]
[1]Department of Computer Science and Business Informatics, IU International University of Applied Science, Berlin, 14513, Germany.

Article Info

Article history:

Received September 04, 2025
Revised November 02, 2025
Accepted November 12, 2025

Keywords:

Hybrid Cloud Security
Data Leakage Risk
Misconfigured APIs
PRINCE2 Framework

ABSTRACT

Hybrid cloud environments offer organizations essential flexibility and scalability by integrating private and public infrastructure, but this complexity introduces the core research problem: a greatly expanded attack surface and inconsistent application of security controls, leading to critical vulnerabilities and data exposure risks. The study employed a mixed-methods design, analyzing extensive secondary data through quantitative findings combined with qualitative thematic analysis of security reports. The key results quantified the main contributors to data leakage, finding misconfigured APIs as the leading threat (35%), followed by endpoint vulnerabilities (30%), and encryption failures (25%). While efficient AES-256 encryption is common, the research noted critical challenges in key management and the continued use of outdated protocols. Furthermore, inadequate use of secure API management frameworks was highlighted as significantly increasing the risk of unauthorized access. The implications of these findings led to the development of a project management framework that addresses these gaps. This framework integrates cloud-specific solutions—including end-to-end encryption, secure API configurations, automated compliance monitoring, and advanced endpoint detection and response (EDR) tools—within a PRINCE2 method. This proposed multi-layer approach provides proactive risk management, effectively bridging architectural gaps and improving the overall security posture against technical and compliance issues across the hybrid environment.

Corresponding Author: Rachel John Robinson (e-mail: rachel.john-robinson@iu.org)

1. INTRODUCTION

The part of the hybrid cloud environment, which is only a combination of the public cloud with its own risks and regulatory requirements, and the private cloud with its own risks and regulatory requirements, must address data leakage within. By running on hybrid clouds, organizations can enjoy the scalability of the public cloud but also keep their sensitive data in the private cloud. As a result of this double nature, the intercloud data transfer vulnerability and compliance-enforced inconsistency pose a massive risk of data leakage [1]. One big issue in hybrid cloud environments is the consistency of data protection. Misconfigured APIs, exposed endpoints, and being lost to human error in moving data between public and private clouds are all common sources of data leakage.

But the challenge is that data flows continuously between these components, and if it involves multiple cloud service providers as well, we need to ensure governance is in place across it all, as well as ensure adherence to the compliance framework. What does your organization need to protect sensitive information on cloud infrastructures? Data leakage can be a fundamental problem within an industry context. For example, the financial industry has a legal requirement to satisfy a large number of associated stringent regulatory requirements like the GDPR or PCI DSS, and faces huge fines for non-compliance. A good example of where this is the case is GDPR, in which there are severe fines for data breach up to €20 20million or 4% of annual business turnover, whichever is higher [2]. Regulatory requirements, such as

these, force hybrid cloud users to deploy strict data protection with compliance across all the cloud components.

On the other hand, regulatory compliance makes things even harder still for multinational organizations, having to apply different regional requirements like GDPR, FedRAMP, and ISO standards at the same time. For instance, the GDPR prescribes strict regulation of sensitive data, and any disregard of which will result in penalties up to €20 million, or 4 per cent of annual turnover. Such compliance demands are further complicated when data needs to be stored in different regions, resulting in businesses adopting multi-cloud strategies so that all the regulated data is hosted in permitted territory. Cloud governance is another important way to fight data leakage. In the context of hybrid cloud environments, a delegated governance model is needed where centralized policy making is supported by decentralized enforcement. Then, through automated workflows for data protection, compliance monitoring, and auditing, this will ensure that flows are consistently applied across public and private environments. Organizations can ease compliance by automating it, and that means it will minimize the number of manual errors that can lead to data leakage and ensure the privacy regulations are followed. Due to these shortcomings, cloud environments become particularly complex and hard to secure; hence, adopting advanced security solutions that are specifically built for them. As cloud-based resources shift constantly [3], a cloud security strategy must include features such as cloud firewalls, automated detection, and compliance monitoring tools.

1.1. Project Objectives

To identify the dominant risks of data leakage in hybrid clouds, look at the typical defenseless exposures like lack of control, misconfigured APIs, compromised endpoints, and gaps in encryption. In a cloud, it will be different. Finally, using the NIST Cybersecurity Framework for a complete risk assessment of hybrid cloud configurations supports this aim.

To assess the organization's encryption and API management practices: Assess the encryption protocols; API management implementation using ISO/IEC 27001 standard for information security; to achieve a consistent and effective manner of protecting data in hybrid cloud components.

To develop a project management framework for data leakage prevention: The second step to be taken in making a hybrid cloud infrastructure is to create a project management framework that includes overall risk identification, control implementation, continuous monitoring, secure API management, and encryption strategies to prevent data leakage across the hybrid cloud infrastructure. The process entailed is provided in a graphical format in Figure 1.

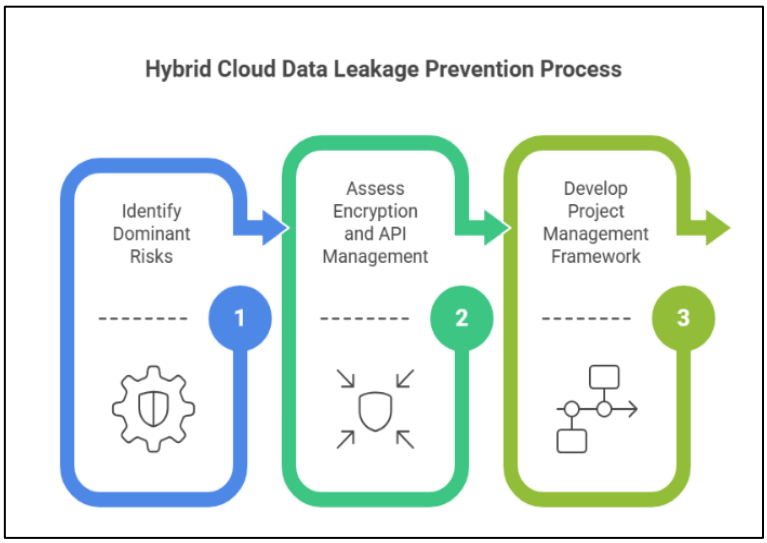

Figure 1. Percentage Distribution of Data Leakage Risks

1.2. Research Questions

What are the dominant risks of data leakage in hybrid cloud environments? This question aims to find the primary threats and vulnerabilities that could lead to data leakage, such as misconfigured APIs, compromised endpoints, or encryption gaps.

How effective are the current encryption and API management practices in securing hybrid cloud data? What are the key elements of a project management framework that can effectively mitigate data leakage in hybrid cloud environments?

This question focuses on evaluating the organization's current security measures, specifically related to encryption protocols and API management, using standards like ISO/IEC 27001. This question aims to define the necessary components of a project management framework, using PRINCE2 methodologies to prevent data leakage by implementing encryption, monitoring, and secure API practices.

2. LITERATURE REVIEW

Modern IT strategies have relied on hybrid cloud environments – enabling the scalability and cost effectiveness of public cloud services, while keeping control and security of private clouds. The dual structure lets organizations mix their operational needs with the data sensitivity requirements of diverse types. Although integration of these disparate systems adds a great deal of complexity, it brings with it challenges about governance, compliance, and security management. In this chapter, we investigate the theory behind hybrid cloud by considering the architecture involved, the benefits, and the challenges. It presents the framework for understanding the risks and the opportunities these systems constantly threaten to bring, to better contextualize how important such robust security frameworks become in such hybrid setups.

2.1. Multi-Cloud Architecture and Benefits

Hybrid cloud environments consist of a private and a public cloud infrastructure that work as a single ecosystem, which allows mobile data and applications to move from private cloud to public cloud and vice versa [4]. Organizations can have dedicated control over their critical data while keeping up with regulatory standards on private clouds or providing scalable and flexible resources at a cheaper price with public clouds. This architecture allows businesses to extract the strengths of both models without fully embracing one.

One of the big hallmarks of hybrid clouds is scalability. A dynamic resource allocation can be done; thus, organizations can react to real-time demand without the costly investment in hardware upgrades [5]. An example of this is an e-commerce company that takes full advantage of public cloud resources during high traffic events, such as Black Friday, but stores keys to its sensitive customer data in its private cloud.

2.2. Challenges and Risks of Multi Cloud

Hybrid cloud environments are a great fit for most organizations, but there are a number of challenges involved in using them effectively. This is a major hurdle in getting private and public cloud infrastructures to work together. As these systems tend to work on different platforms, sophisticated networking solutions and middleware happen to make it seamless connectivity and interoperability [4]. This creates compatibility problems, and especially as we integrate the legacy systems with the modern cloud technologies, it can cause your deployment costs to increase and the time to deploy to increase as well.

Another big issue with security is variability in cloud environments. Public cloud providers generally implement strong security measures to secure their multi-tenant environments, but they may not match an organization's private cloud protocols [6]. Security gaps are created from this misalignment, which can be exploited by attackers.

On top of that, challenges arise in the case of a hybrid cloud setup, as compliance with the regulatory standard is needed. Different countries' organizations must differentiate between data protection laws, including GDPR in Europe and the California CCPA. Compliance assurances from public cloud providers often aren't specific to your organization and may not even be applicable. To ensure consistent compliance across the private and public cloud environments, meticulous documentation and auditing are needed, and collaborating with service providers is inevitable [7].

2.3. Data Leakage Risks in Multi Clouds

Organizations looking for flexibility, scalability, and high availability to realize the full potential of their IT, without sacrificing sensitive data, can use hybrid cloud environments. Despite that, the integration of private and public cloud systems brings significant risk for the leaking of data. The risk comes from misconfigured systems, the complexity of compliance requirements, and the governance problem of hybrid setups. This section examines the top risks that cause data leakage, compliance, and governance issues for an organization, as well as illustrates with real-world examples of such vulnerabilities.

Compromised Endpoints are another critical risk. Attackers most often use endpoints, which encompass user devices and on-premises servers. In hybrid environments, the many endpoints multiply the attack surface. An attacker has access to either private or public cloud systems from a single compromised endpoint. Sentinel One reports that the endpoint vulnerability challenge continues to test the resolve of organizations that are adapting to remote working using increasingly cloud-centric work models.

Another huge source of data leakage is encryption failures. Data at rest is encrypted, and data in transit is encrypted. While securing sensitive data, however, it may be based on using outdated encryption

algorithms with improper key management practices, or by misconfiguration of encryption protocols. The Cloud Security Alliance sees encryption missteps as one of the key risks in hybrid cloud environments. A failure exposing that data to interception in between private and public cloud can compromise that confidentiality and integrity [8].

2.4. Examples and Case Studies

In 2024, the Storm-0501 ransomware attacks revealed new modern threats to hybrid cloud environments. Organizations with a hybrid setup were targeted by attackers with compromised endpoints moving laterally between premises and cloud systems. More data was exfiltrated, and more credentials were possibly stolen through the attacks, along with operational disruptions. The Microsoft report on that incident highlighted the importance of holistic endpoint security and broad cloud monitoring in a hybrid cloud [9].

These are representative of the dire need for organizations to place security at the top of their priorities as they embrace the hybrid cloud. Again, data leakage incidents center around misconfigured APIs, compromised endpoints, and weak encryption protocols. In addition, hybrid setups bring about complexity in compliance and governance and need robust frameworks to manage the risks. To do this, we must address these challenges with a combination of technical solutions, like encryption and endpoint protection, and organizational solutions, like standardized policies and continuous monitoring.

2.5. Existing Solutions and Best Practices-Encryption/ API Management

Symmetric and asymmetric methods are blended to form a hybrid encryption approach, which provides security as well as performance. It is possible to use such systems: asymmetric encryption takes care of the asymmetric key exchange, and symmetric encryption performs the bulk encryption. This framework is ideally suited to the hybrid cloud environment where data often flows between private and public clouds [10].

API gateways provide an added means for securing API operations by collecting and monitoring access control settings. These gateways all act as a single point of entry and enforce a consistent security policy across all API endpoints [11]. The dynamic nature of the hybrid cloud environment, where APIs tie together diverse public and private cloud systems, demands frequent updates of security configurations to address evolving threats.

2.6. Project Management Frameworks

While not specific to the cloud, project frameworks like PRINCE2 (Projects IN Controlled Environments) have become widely used across industries to structure and guide complex projects, even if one of those projects is a hybrid cloud deployment. The adoption of PRINCE2 on the hybrid cloud provides a process-based, defined role and responsibilities, along with a focus on risk management, enabling the adoption of PRINCE2 in dealing with the data security of hybrid cloud implementation. The focus on the identification of risks and controls in this method is in tune with the multiplicity and dynamism of hybrid cloud systems, a pattern where sensitive data moves between private and public cloud infrastructures [12].

PRINCE2, however, may not provide the full solution to the security issues presented by hybrid cloud environments. While it brings a structured approach to managing risks, it does not necessarily house specialized tools or strategies for working with cloud-specific issues, such as securing inter-cloud data transfers or traversing the shared responsibility model between organizations and cloud service providers [13]. Therefore, most companies employ the combination of PRINCE2 with a specific cloud security structure, for example, any cloud security toolset such as the Cloud Security Alliance's Cloud Controls Matrix (CCM) to cover all risks present in a hybrid cloud.

It is also possible that the stage-based approach of PRINCE2 may cause delays in fast-changing environments such as the cloud. Often, hybrid cloud systems need real-time detection and response to threats in principle, which doesn't properly align with PRINCE2's sequential processes. Organizations can bridge this gap by implementing agile methods along with PRINCE2, using the framework's structured benefits whilst being still agile to meet changing business needs [14]. Combining paperless tools for the cloud with agile methods and PRINCE2, organizations can address data security more effectively in hybrid cloud projects.

2.7. Research Gaps

The major problem is the lack of complete frameworks tailored to specific problems of hybrid cloud systems. While they are helpful tools, such as project management frameworks, like PRINCE2, and security guidelines, like the Cloud Security Alliance's Cloud Controls Matrix, they aren't fine-tuned enough for hybrid cloud environments. However, these systems usually involve various cloud service providers (CSPs), with

each having its own security standards and compliance requirements with fragmented and inconsistent security implementations [14].

A second critical gap in the literature is the lack of standardization of encryption protocols. Data security is built upon encryption, but many studies find limitations to the implementation of encryption in hybrid cloud systems. Sensitive information can be exposed during inter-cloud transfers [15], so disproportionately more attention has been placed on data at rest than on data in transit. Besides, the security of the encryption solutions is also decreased by poor key management practices, such as non-rotation of keys and insecure storage of the same.

3. RESEARCH METHODOLOGY

For achieving these goals, the study has used a secondary research method. This study draws an extensive review and analysis from existing literature such as peer-reviewed journal articles, industry reports, and credible publications. The main reason for using secondary research for this study is that the information can provide access to a lot of established knowledge and data on hybrid cloud environments and data security practices. This method synthesizes insights from a number of sources to allow an all-encompassing analysis of the challenges and solutions described in earlier studies.

Secondary research method supports the goals of examining the existing frameworks, encryption protocols, and API management strategies systematically. It gives the groundwork for suggesting gaps in current literature and the best practices. This method not only helps to develop a project management framework but also uses well-documented industry standards and practices, leading to evidence-based, practical proposed solutions. The study relies on secondary research to obtain a thorough, reliable, and cost-effective approach to addressing the research questions and achieving the set goals.

3.1. Research Design

A qualitative research method has been adopted, and the researcher employed secondary research to explore the challenges and solutions to the problem of mitigating data leakage risks in hybrid clouds. This approach is particularly well suited to the synthesis of existing knowledge, say, via examined use of peer-reviewed articles, industry reports, and case studies. The study, therefore, focuses on the secondary data to achieve a more comprehensive understanding of hybrid cloud systems, where the focus was on encryption practices, governance frameworks, and compliance challenges. Studying critical issues and providing solutions for the topics within the hybrid cloud infrastructures is made possible using the qualitative method [16].

The study is applied with the PRINCE2 (Projects IN Controlled Environments) project management framework to ensure systematic organization and execution. PRINCE2 provides a structured, process-driven approach that breaks down the research into processes by breaking it into properly sized and defined stages with the roles and responsibilities of each. With respect to the research goals definition and feasibility study to be clarified, PRINCE2 supports this at the outset. The research plans happen at the initiation stage and are quite specific. An outline for performing literature reviews and synthesizing their findings is prepared at this stage. Monitoring progress is important as the framework pays attention to closing the doors on crucial findings such as encryption gaps and API misconfigurations [17].

3.2. Data Collection

This study adheres to the established guidelines that the research is carried out in a responsible, ethical way, which is the ethical approval process. The use of secondary data requires approval of the research design, including the validity of the design, from a relevant institutional ethics review board. Without the direct involvement of participants, risks arising from primary data collection are minimal. Nevertheless, confidentiality and data integrity remain ethical issues: This is true, especially due to confidentiality and integrity of the data [18].

The sources cited, including journal articles and industry reports, are all openly available. To uphold academic integrity and avoid plagiarism, all sources are meticulously cited, specifically referring to the format shown by [18]. Furthermore, an unwavering commitment to confidentiality is supported through the anonymization of any sensitive data derived from case studies or reports. Since this research relies solely on publicly available secondary data, the direct requirement for informed consent does not apply. Nevertheless, ethical standards are strictly enforced by ensuring data sources are fully transparent and strictly adhering to fair use policies for every source, setting up a rich and ethically sound research process [19].

3.3. Data Analysis

The method of descriptive statistics under quantitative and qualitative data analysis is chosen for the purpose of this study, which is thematic analysis, given that this method allows you to obtain a deep

understanding of the data's patterns and themes, which was also stipulated. As an exploration of challenges and solutions to mitigate data leakage risks in hybrid cloud environments, this approach is particularly proper.

Thematic analysis is justified due to its flexibility and rigor. This is adaptable to a range of research contexts and allows the deep examination of complex phenomena, including how public and private cloud components interact. The analysis follows several iterations of coding and theme building, with transparent documentation of the process [19], to ensure credibility. This approach is rigorous and adds to trustworthiness while also enabling other researchers to replicate the same analytical steps.

3.4. Limitations

These challenges facing research limit its scope and its implications. A major limitation is that it is dependent on secondary data, which, though large, does not allow for direct validation against findings through primary data collection. Due to this limitation, a reliance might be placed on the accuracy and comprehensiveness of presently available studies and reports [20]. The contexts in which hybrid cloud environments are used are varied, making it hard to generalize findings across different industrial and organizational environments.

Furthermore, the complexity of deploying hybrid cloud systems prevents us from addressing all the potential risks as well as a comprehensive range of solutions, given the fast pace of cloud technology evolution and security threats. However, for thematic analysis, we have robust tools, but it is subjective and likely to introduce bias during coding and interpretation. To address these challenges, careful interpretation of results is needed, and further studies using mixed-method approaches to confirm the findings are needed.

4. RESULTS AND DISCUSSION

Quantitative analysis at the start of the chapter shows which risks are found most often in hybrid cloud environments. Among the problems are poorly configured application programming interfaces (APIs), hacked devices at endpoints, and not having encryption everywhere it is needed. Various graphs and illustrations of data leakage show how widespread and specific problems are in finance, healthcare, and retail organizations. Researchers also check the popularity of encryption standards such as AES-256 and RSA to gauge how industries handle the safety of their cloud information. Later, theme-based display on the qualitative element under four different topics is to be covered.

4.1. Quantitative Results

The section covers the numbers behind the main data leakage risks, helpful breach stats from different industries, and how often encryption is used in hybrid clouds. The report is built from secondary data provided by the Cloud Security Alliance in 2020, 2021, Sentinel One in 2023, and CrowdStrike in 2024. The outcomes are connected to the main research questions and analyzed to decide their use in improving cloud security.

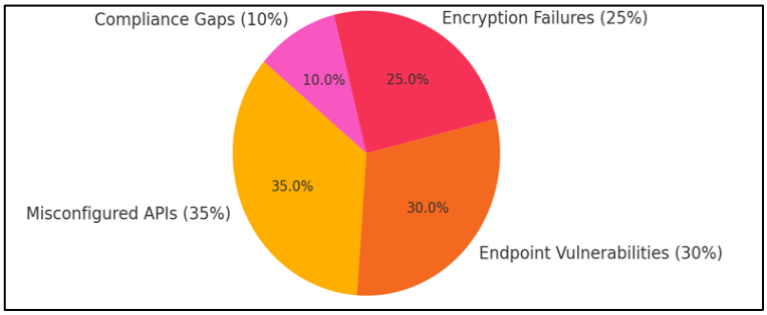

Figure 2. Percentage Distribution of Data Leakage Risks

According to Figure 2, 35% of leaked data in hybrid cloud setups is due to misconfigured APIs. As a result, we see that a major problem for hybrid systems is that APIs act as the primary tool for linking public cloud to private cloud components. When organizations have weak authentication methods, send too much information without proper protection, or abandon encryption between their services, important data may become available to unapproved users [21].

Almost 30% of leakage incidents come from issues with endpoints. They range from compromised devices and systems with missing security patches to hacking on weakly defended mobile devices. Because more people are using technology for work from different devices, this kind of risk is on the rise. This discovery is supported by Sentinel One in 2023, which found a 45% jump in endpoint-related events after

2020. A quarter of all data leaks can be traced to problems with data encryption. Such attacks are possible due to old cipher procedures, ineffective key handling, or a lack of uniform encryption practices in mixed IT systems. As a result of these failures, unencrypted data is exposed, often made worse when different cloud vendors have their own encryption rules.

In the end, a lack of compliance is the cause of 10% of all the risks found. Though this may seem trivial when put next to the profound consequences, missing compliance can trigger strict government action and affect a company's reputation. The inconsistency in handling security and privacy across countries confused service level agreements and led to audit problems, according to CrowdStrike in 2024.

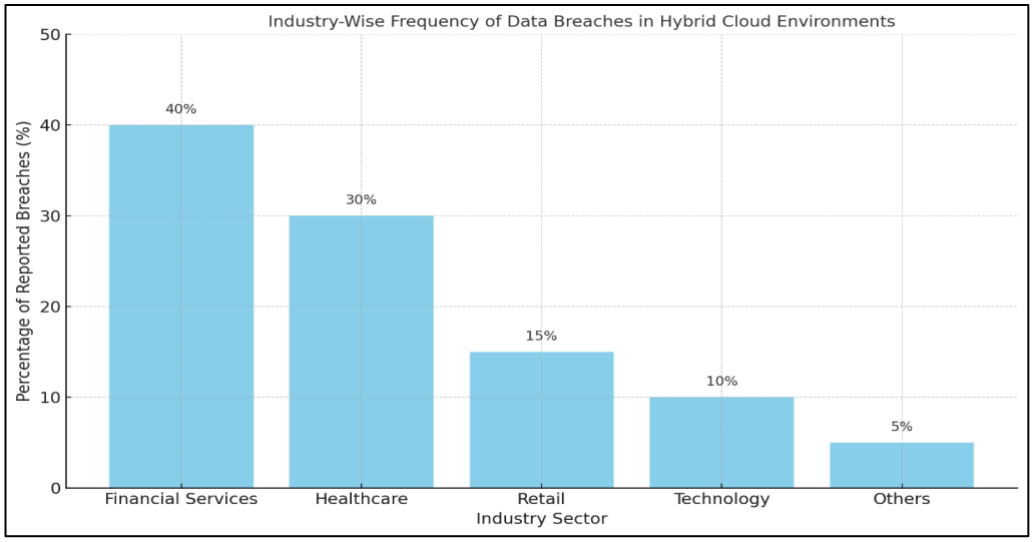

Figure 3. Frequency of Data Breaches in Hybrid Cloud Environments

Figure 3 outlines where data breaches were first spotted in the hybrid cloud by major industry sectors. Of all types of breaches, those in financial services are more common, affecting around 40% of companies, with healthcare close behind 30% and retail around 15%. Technology companies and a large category called "other" make up just 5% and 10% of all listings.

Healthcare comes shortly after with 30% of attacks, just as [19] and Sentinel One in 2023 report. PHI is an attractive target to hackers, largely because it can be sold for a long time and is regulated by HIPAA and GDPR. Organizations in the healthcare sector regularly mix legacy with cloud systems, which makes it difficult to keep endpoints safe and properly control access. Also, when data from public health is transferred across both national and private sectors, the poor coordination of such environments can mean more mistakes.

Most retail sector security breaches (occurring in 15%) result from threats to point-of-sale systems, unguarded transaction information, and cloud-based customer relationship management systems. Because adopting public clouds for scale is common during periodic high demand (like Black Friday), it creates uncertainty about how sensitive or unimportant different data or workloads really are, which can lead to greater risk. The authors argue that weak enforcement of policies about who accesses systems plays a key role in retail breaches, which is worsened when there isn't good protection for endpoints. Both technology firms and the category labelled "Others" contributed to about 15% of all breaches. Most technological organizations have developed strong cloud capabilities, yet they still deal with bugs caused by rising scale or the use of third-party APIs. Just because the automation rate in these areas is not high doesn't mean they are riskier; it often results from mature practices in managing the cloud. The results fulfil the first research goal by showing what factors in different industries either increase or decrease the threat of data leakage.

Encryption practices, as in Figure 4, in hybrid cloud systems clearly prove which areas require more security and where current practices are effective. Seeing Figure 3, 60% of organizations are using AES-256 as their encryption choice. Its success is explained by its strong symmetric encryption, which enables it to support high-traffic situations in hybrid cloud settings. These recommendations are consistent with those of [22], who call AES-256 the preferred method to safeguard top enterprise data. Symmetric encryption is used by 25% of those who have adopted RSA. Although it helps protect important exchange and authentication activities, it is too slow to be widely applied to large datasets. Usually, its only purpose is to secure messages and implement API communication in the public areas of hybrid applications. Of all organizations surveyed, just 10% rely on hybrid encryption approaches. However, because managing the two encryption systems is rather complex in dynamic cloud setups, many are likely put off by this challenge. Research from [20]

confirms that this lack of hybrid models is mainly because companies struggle to implement the necessary technical requirements. A further 5% consists of obsolete or alternative encryption, increasing the danger. Not using updated systems may cause organizations to miss current compliance rules, which increases their risk of data breaches and legal problems. Results reveal causes mentioned by [22], such as unsuccessful management and unreliable data protection policies, for the data leaks.

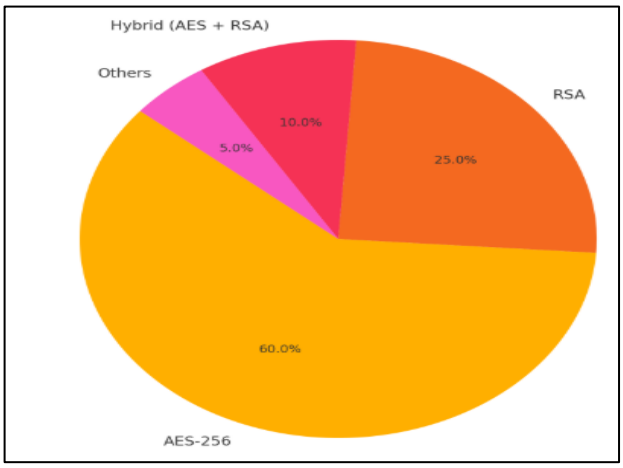

Figure 4. Encryption Standards Adoption in Hybrid Cloud Environments

4.2. Thematic Qualitative Analysis

Theme 1: Misconfigured APIs- The primary reason for misconfigured APIs (refer to Figure 4) being a danger for hybrid platforms is their crucial role in linking and communicating among multiple cloud services, platforms, and parts of the system. Because organizations value security and reach their cloud solutions, APIs are now the main support for cloud connections. At the same time, such interfaces can become targets when they are allowed unrestricted access. Based on the analysis, three major problems follow from not securing APIs. The main problem, according to Figure 5, is unauthorized access, with exposing data ranking second (30%), and there were gaps in compliance for 20% of cases. The findings come from pulling together cloud security incident reports, reviews of what happened at Capital One and Chaos DB, and writings by [23][24].

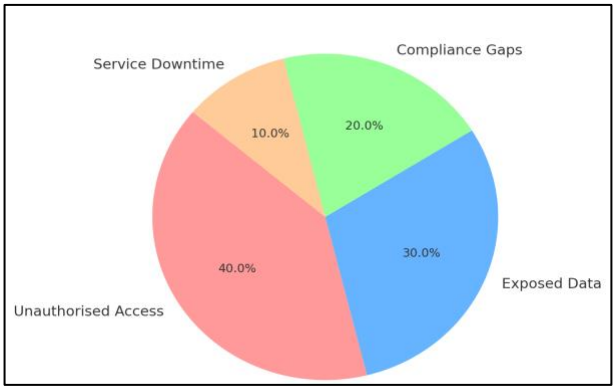

Figure 5. Impact of Misconfigured APIs in Hybrid Cloud Environments

Poor authentication, no restricted access by roles or tokens made public in open APIs, all cause unauthorized access. In situations where services are used in private and public clouds, inconsistency in how APIs are set up can result in major security problems. Because of these misconfigurations, attackers can easily move from system to system without being caught, unless you have powerful API monitoring tools.

An API with over-available data is commonly the cause of the second most frequent security issue. Developers could reveal important customer or system information without realizing it if they do not use data filters appropriately. This problem gets worse when working with cloud-native microservices, with every API reaching out to back-end databases or queues on its own. When APIs fall short of the needs for transferring, recording, or protecting data, compliance gaps occur. A small mistake in using APIs in healthcare or finance

might run afoul of GDPR, HIPAA, or PCI DSS. It's clear from the 20% increase in problems linked to compliance that putting rules in place in multiple regions is a challenging task. Even though service downtime contributes only 10% of the total, it has important operational effects. A misconfigured API gateway in 2019 caused the Capital One breach, letting an attacker remove over 100 million records. As a result, Capital One faced both a loss of data and negative public attention.

Theme 2: Endpoint Vulnerabilities- Both hybrid cloud adoption and a rise in working from home have made endpoint vulnerabilities more important than before. It appears from our assessment that user systems, which include laptops, smartphones, and fixed access points, are the most common point of vulnerability in a hybrid setting. When effectively used, these endpoints allow users to access both public and private clouds safely. If not secured properly, though, they let attackers gain access, leave malware behind, and move around inside the system. As can be seen in Figure 6, attacks through endpoint vulnerabilities increased from 25% in 2020 to a large 70% in 2024. The rise in users we see corresponds to an increase in cloud usage and the rapid move to work remotely during the pandemic. Sentinel One in 2023 and Veeam in 2024 found that most attacks in 2021 and later took advantage of outdated user devices that didn't use the best EDR technology.

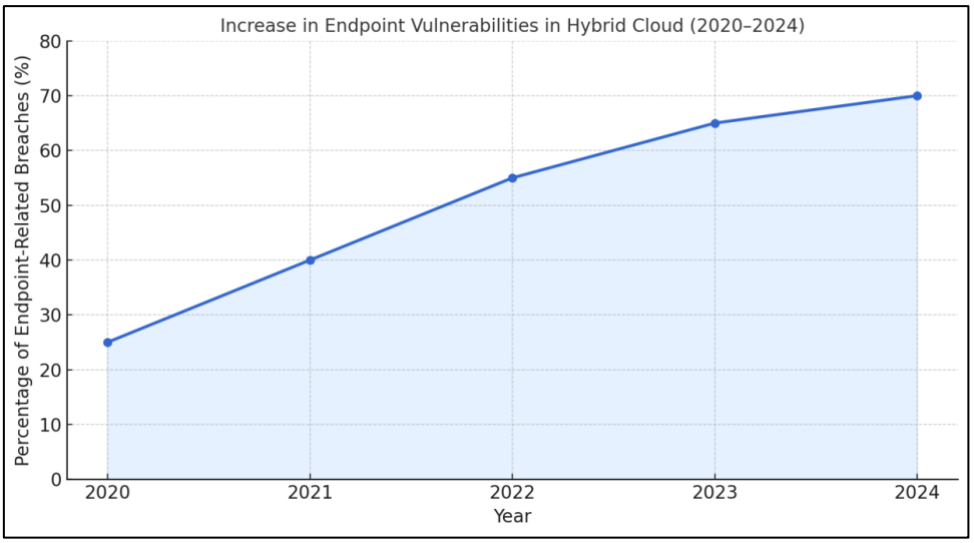

Figure 6. Increase in Endpoint Vulnerabilities

A big reason is that endpoint security practices are not kept the same across systems that use cloud services. While much work is moved to the cloud with adequate security, many companies have fewer protections on the endpoints that their employees use. Devices present outside the main network can dodge standard checks, so passwords can be taken, privileges may be upgraded, and attacks may be carried out on hybrid servers. Remote employees are also making workplaces more complicated because many businesses have adopted bring-your-own-device (BYOD) policies. Yet, because of these policies, endpoints now run a variety of systems, patches, and security solutions, so it is hard to control them all from one place. According to the mix of device types, it makes it nearly impossible to standardize protection or keep an eye on all active endpoints that use the company's sensitive cloud services. The research proves that security risks at endpoints cause a problem in systems that blend cloud and user-managed areas. The results prove that organizations should use integrated solutions such as EDR, MFA, and MDM, which are able to tell them about device activity in real time.

Theme 3: Encryption Inconsistencies- The pie chart in Figure 6 proves the main problems that cause inconsistency of encryption in hybrid cloud environments. The key management point is the most critical of them all, being 45%, followed by outdated cipher protocols, at 35%, making the data vulnerable to breaches. The 20% contribution is lastly due to inconsistently applied standards around encryption, which is caused by varying security policies between different cloud providers. Such problems call for strong key management solutions, periodic updates for encryption protocols, and uniform adoption of the same in all cloud components to protect the data during cross-cloud transfer. Despite encryption's importance in cloud security, variations in its use in hybrid clouds give rise to major vulnerabilities. At the same time, some companies use strong encryption tools, but have holes in how keys are managed, the use of outdated ciphers, and a lack of consistent application that weaken their encrypted systems.

Figure 7 makes it clear that poor management of keys is by far the biggest factor in 45% of encryption-related flaws. Proper encryption depends on safely creating, holding, switching, and getting rid of

cryptographic keys. Using a hybrid cloud means dealing with multiple key vaults, different rules from each cloud service, and implementing it with older systems. Not setting up centralized key management systems (KMS) regularly causes keys to be either abandoned or too visible to attackers, according to [17]. Using Triple DES and old RSA configurations accounts for 35% of these problems. Many organizations continue to find these legacy protocols in their everyday operations, which is often because they have not yet updated to current cloud technology. Relying on guidance from the National Institute of Standards and Technology [22], which suggests using AES-GCM, many organizations still do not meet the security standards, as they either cannot meet the compatibility needs or do not have the required workers.

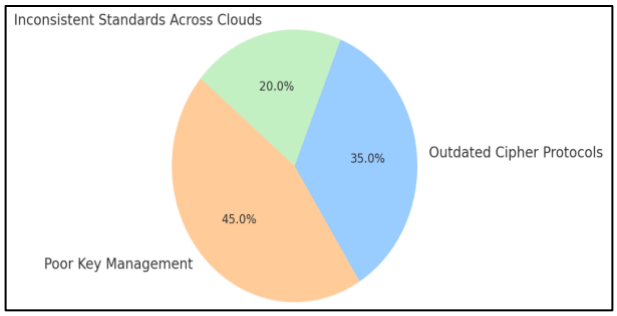

Figure 7. Issues with Inconsistent Encryption Practices

As a result, the system's security declines, raising the chance that data is hijacked during transmission. The analysis confirms that encryption risks arise from sources other than technology alone. IT security teams do not work well with application developers; a lack of set encryption policies and a lack of documentation cause these problems. Even though few technical texts cover this topic, having this insight is essential for keeping risks under control for a longer period.

Theme 4: Compliance and Regulatory Gaps- In a hybrid cloud arrangement, ensuring that all data is correctly protected remains a challenging task. Because of GDPR, HIPAA, and PCI DSS, organizations must exercise strict rules when handling and storing data. Even so, the challenges of these mixed networks often make it harder for controls to be put in place the same way everywhere.

As can be seen in Figure 8, 35% of the cases we analyzed characterized the common compliance problem as inconsistent policies on where data is stored. The rules about where data should be kept often require organizations to keep some types of data within certain regions. It gets more difficult to do when cloud resources move around and are managed by multiple companies. According to [25], this situation often leads to errors where personal information is dealt with in areas that do not follow the right laws.

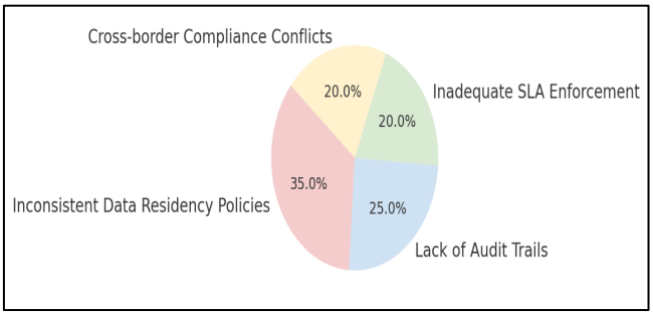

Figure 8. Compliance and Regulatory Gaps

Insufficient audit trails are to blame for about one in four compliance failures. Because many hybrid clouds don't provide total visibility, companies have difficulty knowing who used their data, when it was used, and under which circumstances. Unifying log systems is important for organizations to quickly produce audit information during compliance checks, which is often needed for cloud and on-premises setups at the same time. This issue played a key role in the regulatory punishments multinational healthcare and finance companies have had to pay.

Both insufficient monitoring of Service Level Agreement terms and disagreements caused by different regulations across countries account for 20% of why compliance fails. Much of the time, SLA issues happen because organizations want security protections that aren't part of the vendor contract. This means that organizations have no obvious way to access their vendors' encryption tools, fix patches, or

develop crisis management plans. If services are offered in several different countries, with each following different rules, it becomes hard to support the same compliance approach. This research confirms that compliance unpredictability is an important and increasing challenge in moving to the hybrid cloud.

5. DISCUSSION AND RECOMMENDATIONS

The study has explored the top risks in hybrid cloud systems, evaluated encryption and API management practices, and developed a structured project management framework for risk mitigation in the context of 'A Project Management Framework for Securing Data Transmission." These findings confirm that misconfigured APIs, endpoint vulnerabilities, and encryption inconsistencies are your primary risk of data leakage. This research aligns with the research on Cloud Security. The study further illustrates the gaps in governance, compliance, and encryption in public and private cloud infrastructure, creating problems for consistent data protection. The cloud-specific solutions, like API gateways, end-to-end encryption, and automated compliance monitoring, are integrated with PRINCE2 methodologies in the developed project management framework. This multi-layer approach provides proactive risk management and improves the security posture of the hybrid cloud.

To effectively mitigate data leakage risks in hybrid cloud environments, organizations need to deploy an end-to-end security strategy encompassing advanced encryption, API security, compliance monitoring, endpoint security, and centralized governance. To secure data in hybrid cloud systems, end-to-end encryption is mandatory. For data in transit (where the data must be read in flight) and data at rest (data that is stored on disk, or out on the wire), hybrid encryption methods such as Advanced Encryption Standard (AES) and Transport Layer Security (TLS), respectively, provide a highly robust defense against unauthorized access. But key management strategies must, of course, include secure key storage, key rotation often, and the synchronization of the components of all clouds. Such measures are properly implemented so that during inter-cloud transfers and when at rest, sensitive data is safe and protected.

Securing API management is another critical aspect in case of vulnerabilities found in poorly configured interfaces. Strong authentication protocols like OAuth 2.0 are needed by organizations to enforce who can access APIs. Finding areas in which sensitive information could be exposed and how to mitigate them is critical and requires regular penetration testing. Moreover, API gateways should be introduced to give a single control point for API operations, enforce uniform security policies, and detect unexpected API activity. In a hybrid cloud setup, these practices reduce unauthorized access and data exposure risks, which are so common.

Just like supporting regulatory compliance and governance, automated compliance monitoring tools, or tools such as Cloud Security Posture Management (CSPM), are equally important for monitoring compliance. Cloud Service Providers (CSPs) can continuously check their cloud environment with real-time ongoing tools and adhere to different standards such as GDPR, HIPAA, or PCI DSS. Automated solutions reduce manual oversight, provide visibility, and guarantee detection of compliance violations in time.

6. CONCLUSION

To the extent that the findings of the study are based on secondary data, they are not, as they could not be confirmed by primary research methods such as surveys, interviews, or case studies. Although it provides a broad, well-documented understanding of hybrid cloud environments, secondary data depends on the accuracy, quality, and comprehensiveness of the advertised literature. As a result, the results are limited to the extent and reliability of the sources of the review, which may not include the entire range of emerging trends or organizational experiences. The inability to provide real-time, context-specific validation of the proposed framework and real application is due to a lack of primary data.

Future research can take the form of developing AI-based solutions that are easily integrated with existing cloud infrastructures and offer real-time insights with minimal manual oversight. They will be able to swiftly address the compliance challenges found in public and private cloud components on an as-needed basis. Together with the growth in remote work, endpoint security is also growing in vulnerability. For monitoring and risk mitigation of compromised user devices, deploying advanced Endpoint Detection and Response (EDR) tools is crucial. EDR tools spot threats in real time and help with quick responses to incidents as well as securing laptops, tablets, and mobile devices. It is critical to have this proactive approach to reduce the attack surface and to deny unauthorized access to hybrid cloud environments from vulnerable endpoints.

Finally, a centralized governance structure must be developed that will guarantee consistency in data security practices on private and public cloud components. Security controls, access management, and compliance protocols are all required to be unified in policies, so they are applicable to all the cloud service providers (CSPs). Centralized governance sets up a level playing field for all that builds security into the architecture of your application and solution, cutting inconsistencies in security implementation, closing gaps

in compliance, and giving visibility into the overall ecosystem. It unifies technical processes with governance measures to secure hybrid clouds effectively.

DATA AVAILABILITY STATEMENT

The data presented in this study are available on request from the corresponding author.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest in this work.

REFERENCES

[1] S. U. Khan and N. Ullah, "Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review," *J Eng*, vol. 2016, no. 5, pp. 107–118, May 2016, doi: 10.1049/joe.2016.0089.

[2] S. Basu *et al.*, "Cloud computing security challenges & solutions-A survey," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2018, pp. 347–356. doi: 10.1109/CCWC.2018.8301700.

[3] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual Res Psychol*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[4] Hitesh Premshankar Rai, Pavan Ogeti, Narendra Sharad Fadnavis, Gireesh Bhaulal Patil, and Uday Krishna Padyana, "Integrating Public and Private Clouds: The Future of Hybrid Cloud Solutions," *Univers Res Reports*, vol. 8, no. 2, pp. 143–153, Aug. 2024, doi: 10.36676/urr.v9.i4.1320.

[5] A. Castleberry and A. Nolen, "Thematic analysis of qualitative research data: Is it as easy as it sounds?," *Curr Pharm Teach Learn*, vol. 10, no. 6, pp. 807–815, Jun. 2018, doi: 10.1016/j.cptl.2018.03.019.

[6] Koushik S. and A. P. Patil, "An Approach to Ensure Secure Inter-Cloud Data and Application Migration Using End-to-End Encryption and Content Verification," *Int J Ambient Comput Intell*, vol. 13, no. 1, pp. 1–21, Apr. 2022, doi: 10.4018/IJACI.293148.

[7] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," *Symmetry (Basel)*, vol. 15, no. 11, p. 1981, Oct. 2023, doi: 10.3390/sym15111981.

[8] R. J. Robinson, "Insights on Cloud Security Management," *Cloud Comput Data Sci*, pp. 212–222, Jul. 2023, doi: 10.37256/ccds.4220233292.

[9] R. J. Robinson, "IoT Solutions for Smart Parking- Sigfox Technology," *Comput Sci Eng An Int J*, vol. 14, no. 2, pp. 01-13, Apr. 2024, doi: 10.5121/cseij.2024.14201.

[10] H. Pitkar, "Cloud Security Automation Through Symmetry: Threat Detection and Response," *Symmetry (Basel)*, vol. 17, no. 6, p. 859, Jun. 2025, doi: 10.3390/sym17060859.

[11] S. Ali *et al.*, "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions," *Comput Secur*, vol. 157, p. 104599, Oct. 2025, doi: 10.1016/j.cose.2025.104599.

[12] G. C. Silva, L. M. Rose, and R. Calinescu, "A Systematic Review of Cloud Lock-In Solutions," in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, IEEE, Dec. 2013, pp. 363–368. doi: 10.1109/CloudCom.2013.130.

[13] D. K. Shetty *et al.*, "Analyzing AI regulation through literature and current trends," *J Open Innov Technol Mark Complex*, vol. 11, no. 1, p. 100508, Mar. 2025, doi: 10.1016/j.joitmc.2025.100508.

[14] H. Kamma, "A Comparative Analysis of Resource Management and Cost Efficiency in AWS, Google Cloud and Microsoft Azure," *Int J Innov Res Sci Eng Technol*, vol. 14, no. 02, Feb. 2025, doi: 10.15680/IJIRSET.2025.1402008.

[15] D. Seth, M. Najana, and P. Ranjan, "Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis," *Int J Glob Innov Solut*, Jun. 2024, doi: 10.21428/e90189c8.68b5dea5.

[16] R. J. Robinson, "Cloud systems with its security, privacy and trust claims to a sustainable solution," in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, IEEE, Jul. 2023, pp. 1–6. doi: 10.1109/ICECCME57830.2023.10252796.

[17] Jillian A. Tullis Owen, C. Ellis & E. Goffman "Naturalistic Inquiry," in *The SAGE Encyclopedia of Qualitative Research Methods*, 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2008. doi: 10.4135/9781412963909.n280.

[18] F. Jimmy, "Cloud security posture management: tools and techniques," *J Knowl Learn Sci Technol ISSN 2959-6386*, vol. 2, no. 3, Nov. 2023, doi: 10.60087/jklst.vol2.n3.p622.

[19] A. Warrier, "Securing and Scaling API Gateways in Hybrid Environments," *J Artif Intell Mach Learn Data Sci*, vol. 3, no. 3, pp. 2914–2920, Sep. 2025, doi: 10.51219/JAIMLD/Arjun-warrier/607.

[20] L. S. Nowell, J. M. Norris, D. E. White, and N. J. Moules, "Thematic Analysis," *Int J Qual Methods*, vol. 16, no. 1, Dec. 2017, doi: 10.1177/1609406917733847.

[21] R. Saxena and E. Gayathri, "A study on vulnerable risks in security of cloud computing and proposal of its remedies," *J Phys Conf Ser*, vol. 2040, no. 1, p. 012008, Oct. 2021, doi: 10.1088/1742-6596/2040/1/012008.

[22] R. J. Robinson and E. Onyango, "Cutting-edge AI Techniques for Remarkable New Product Promotions," in *2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA)*, IEEE, Feb. 2024, pp. 1–6. doi: 10.1109/ACDSA59508.2024.10467567.

[23] H. J. Singh and S. Bawa, "Scalable Metadata Management Techniques for Ultra-Large Distributed Storage Systems -- A Systematic Review," *ACM Comput Surv*, vol. 51, no. 4, pp. 1–37, Jul. 2019, doi: 10.1145/3212686.

[24] D. Dhinakaran, N. Jagadish Kumar, N. P. Ponnuviji, and B. Praveen kumar, "Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm," *Expert Syst Appl*, vol. 279, p. 127584, Jun. 2025, doi: 10.1016/j.eswa.2025.127584.

[25] S. U. Khan, H. U. Khan, N. Ullah, and R. A. Khan, "Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach," *Secur Commun Networks*, vol. 2021, pp. 1–20, Sep. 2021, doi: 10.1155/2021/1024139.

BIOGRAPHIES OF AUTHORS

Rachel John Robinson is an accomplished scholar whose research contributes significantly to the fields of Cybersecurity, IT Management, and Active Digital Learning. As a Researcher & an Academic in Cybersecurity, she holds a double master's and a doctorate in Economic IT Security, along with many professional certifications and years of industrial experience in the field of IT Security and Higher Education. She can be contacted at email: rachel.john-robinson@iu.org