International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

CLOUD INFRASTRUCTURE SECURITY FOR CRITICAL FINANCIAL INFRASTRUCTURES AND NATIONAL SECURITY

Pavan Nutalapati
Pnutalapati97@gmail.com

Abstract

This research examines the security of the cloud infrastructure within the critical financial area and national security system. These sectors rely increasingly on cloud computing for efficiency, scalability along cost-effectiveness. This research seeks to develop a vigorous security framework that copes with the unique requirements of financial institutions and national security agencies. It critically analyses the existing security practices, addresses specific vulnerabilities, and proposes advanced strategies to mitigate risk factors. The research used secondary qualitative data, and the fostering of the simulation assisted this study to enhance the efficiency of these security measures.
This research offered valuable insights into improving cloud security in the financial sector. It also emphasized the protection of personal data and the flexibility of critical infrastructure in the face of emerging threats.

Keywords: Cloud Infrastructure Security, Cybersecurity, Risk Mitigation, National Security, Critical Financial Infrastructure, Data Protection.

I. INTRODUCTION

In today's digital landscape, the security of cloud infrastructure has become paramount to ensure the integrity of critical financial infrastructure and national security systems. One of the most important technological concerns impeding both economic stability and the national interest is ensuring the security of the cloud infrastructure [1].

1. Project Specification

This research puts emphasis on the evaluation and enhancement of security within the cloud infrastructure utilized in critical financial systems and national security mechanisms. This project focuses on identifying potential vulnerabilities, developing advanced security methods, and thoroughly reviewing existing security protocols.

2. Aims and Objectives

Aims

The main aim of this research is to develop a comprehensive framework for the enhancement of the security cloud infrastructure in critical financial and national security environments.

Objectives

- To assess the present state of cloud infrastructure security in financial and national security sectors
- To address and analyze the vulnerabilities and threats specific to these sectors
- To evaluate how effective these security measures are, simulations will be conducted.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

3. Research Questions

- What are the primary security challenges faced through cloud infrastructure in critical financial systems and national security measures?
- What are the most efficient strategies for the mitigation of identified through security risks in these sectors?
- How well do the current security measures in cloud infrastructures meet the unique needs of financial institutions and address the national security risks in these sectors?

4. Research Rationale

The financial institutions and national security agencies migrated their operations to the cloud platforms rapidly. The higher level of data value maintained through the entities makes them prime prey for cyberattacks [2]. This research is crucial for gaining a deep understanding of the specific security needs in these sectors and developing strategies to effectively address and eliminate potential risks.

II. LITERATURE REVIEW

1. Research background

The increasing adoption of cloud computing through financial institutions and national security agencies has transmuted the operational process within critical infrastructure. A maximum number of financial institutions rely significantly on cloud platforms for increasing scalability, cost-effectiveness and efficiency. The present landscape is evolving which underlines the frequency of cyberattacks through targeting vulnerabilities within the cloud infrastructure [3]. This research seeks to explore the cloud infrastructure security measures that navigate the specific requirements for the national and financial security sectors that ensure the flexibility of this infrastructure.

2. Critical assessment

The present cloud infrastructure security practices along with the national securities often recognized as inadequate to identify the unique issues posed by critical environments. The existing frameworks focus on general cloud security without the consideration of the specific challenges. Besides, the regulatory demands which are crucial for the financial sectors have been also focused [4]. This research analyses the existing measures through the identification of potential limitations and procedures that target the strategies. It focuses on strategies that are more aligned with the requirements of financial institutions. Critical Infrastructure Security and Resilience provides guidance for supporting the local, state, and industry partners in the identification of critical infrastructure that is required for maintaining the functions [5]. However, this paper aims to fill the gap between general cloud security practices and the specialized requirements of these sectors.

3. Linking with aim

The goal of the proposed research is to provide a secure framework that can be used to alter cloud architecture in environments that are crucial for national security and finance. Through the identification of the potential challenges and recommending targeted solutions, this research study aims to enhance the flexibility of the financial sectors against rapid cyber threats. Hence, the aim of this research is linked with the requirement for specialized and streamlined security measures that align with the generic cloud security protocols. The successful alignment between the research aims and requirements of the financial sector is essential to achieve a better outcome.

4. Encapsulation of applications

This research shows a wider application in the security enhancement within the cloud infrastructure that is used by national security agencies and financial institutions. The proposed research also highlights the effectiveness of cloud infrastructure security measures for effectively protecting sensitive data. Besides, it also ensures regulatory compliance and prevents issues in cyber-attacks [6]. The findings of this research can be applied in the development of training initiatives for IT professionals and improvement of the responsive strategies. In addition to this, this research provides a significant framework that provides guidance for maintaining flexibility within the critical infrastructure. The application of this proposed research extends the international contexts on which various security challenges have not been considered in terms of the wider area of the cyber security domain.

5. Theoretical framework

The theoretical framework for the proposed research is devoted to the intersection of cloud computing security theories, critical infrastructure protection and risk management. In order to maintain cloud infrastructural security, financial institutions use various application security to mitigate potential threats. The "Virtual Private Network" (VPN) is one of the crucial security networks that deliver security within cloud platforms for network users [7]. The theories related to access control, encryption and threat modelling can provide actionable insights into the maintenance of security within financial institutions. In this area, the "Cyber Security" theory is also presented as an essential theory that underlines the application of technologies, procedures and controls for the protection of network systems, devices and programs [8]. This theory assists in the reduction of cyber-attack risks and protects against the unauthorized exploitation of the system.

6. Literature gap

Despite the inclusive and integrated research on cloud security, there exists a significant gap within the studies through focusing on the unique demands of the national security systems and financial infrastructures. There exists limited research about the successful integration of detecting advanced threats and response approaches adjusted to these sectors. A maximum number of literature identifies cloud security in a general way without highlighting the specialized requirements of these environments.

III. SECURITY CHALLENGES IN CLOUD INFRASTRUCTURE

3.1 Data Breach And Privacy Issues

One of the most critical security challenges in cloud infrastructure is the risk of data breaches. Highly sensitive material is handled by CFIs and national security agencies, and illegal access can have serious repercussions that include financial loss, harm to one's image, and threats to national security.

Example: Back in 2013, the Target breach led to the theft of 40 million credit card numbers, along with 70 million additional records. The breach was traced back to the compromised credentials of a third-party vendor, highlighting the vulnerabilities in supply chain security.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

3.1.1 Insider Threats

Insider threats, posed by employees or contractors with authorized access to the cloud infrastructure, represent a significant risk. These threats can result from malicious intent or negligence, making it imperative to implement stringent access controls and monitoring mechanisms.

```
import boto3

# Create IAM client
iam = boto3.client('iam')

# Create a new IAM user
response = iam.create_user(UserName='new_user')

# Attach policy to user
response = iam.attach_user_policy(
    UserName='new_user',
    PolicyArn='arn:aws:iam::aws:policy/AmazonS3FullAccess'
)
```

3.1.2 Advanced Persistent Threats (APTs)

APTs are sophisticated, long-term cyber attacks aimed at stealing sensitive information. These threats often involve multiple stages, including initial infiltration, lateral movement within the network, and data exfiltration. CFIs and national security agencies are prime targets for APTs due to the value of the information they hold.

3.1.3 Compliance and Regulatory Requirements

to ensure compliance with these requirements while using cloud services since it necessitates a deep comprehension of both the legal environment and the technological components of cloud security.

Example: The European Union's General Data Protection Regulation (GDPR) imposes stringent data protection requirements on organizations, with severe penalties for non-compliance.

3.1.4 Multi-Tenancy Risks

Cloud environments are typically multi-tenant, meaning that multiple customers share the same physical infrastructure. This sharing can lead to potential security risks, such as data leakage between tenants and resource exhaustion attacks.

3.1.5 Incident Response and Forensics

Effective incident response and forensic analysis are crucial for mitigating the impact of security incidents. However, the dynamic and distributed nature of cloud environments can make it challenging to quickly detect, investigate, and respond to security breaches.

Using AWS CloudTrail for monitoring and logging:

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

```python
import boto3

# Create CloudTrail client
cloudtrail = boto3.client('cloudtrail')

# Create a new trail
response = cloudtrail.create_trail(
    Name='MyTrail',
    S3BucketName='my-cloudtrail-bucket'
)

# Start logging
response = cloudtrail.start_logging(Name='MyTrail')
```

3.2 Threat Vectors in Cloud Infrastructure

External Threats

External threats include attacks from cybercriminals, hacktivists, and state-sponsored actors. These adversaries employ various tactics, such as phishing, malware, and denial-of-service attacks, to compromise cloud infrastructure and gain unauthorized access to sensitive data.

Example: In 2012, the Saudi Aramco cyber-attack, attributed to the Shamoon virus, wiped out data on approximately 30,000 computers. The attack demonstrated the potential for significant damage from external threats.

3.2.1 Internal Threats

Internal threats can be intentional or accidental, and can come from within the company. A few instances are when staff members divulge private information, mismanage cloud resources, or fall prey to social engineering scams.

3.2.2 Supply Chain Threats

Supply chain threats involve vulnerabilities in third-party services and components that are integrated into the cloud infrastructure. Compromised third-party providers can serve as entry points for attackers, leading to potential breaches in the primary cloud environment.

3.2.3 Human Error

Human error, such as misconfigurations and poor security practices, is a significant contributor to cloud security incidents. Ensuring proper training and adherence to security protocols is essential to minimize these risks.

Example: A misconfigured Amazon S3 bucket in 2017 exposed the personal data of 198 million American voters. This incident highlighted the importance of proper configuration and access control in cloud environments.

3.3 Mitigation Strategies

3.3.1 Data Encryption

Encrypting data at rest and in transit is a fundamental security measure for protecting sensitive information in the cloud. This ensures that even if data is intercepted or accessed without authorization, it remains unreadable to attackers.

Encrypting data using AWS Key Management Service (KMS):

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

```python
import boto3

# Create CloudTrail client
cloudtrail = boto3.client('cloudtrail')

# Create a new trail
response = cloudtrail.create_trail(
    Name='MyTrail',
    S3BucketName='my-cloudtrail-bucket'
)

# Start logging
response = cloudtrail.start_logging(Name='MyTrail')
```

3.3.2 Access Controls

Implementing robust access control mechanisms, such as multi-factor authentication (MFA) and role-based access control (RBAC), helps prevent unauthorized access to cloud resources. Regular audits and monitoring of access logs are also crucial for detecting and responding to suspicious activities.

3.3.3 Network Security

Securing the network infrastructure within the cloud environment involves using firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs). These measures help protect against external attacks and ensure secure communication between cloud resources.

Example: Using AWS Security Groups to control inbound and outbound traffic to EC2 instances.

3.3.4 Incident Response Planning

Developing and regularly updating an incident response plan is critical for effectively managing security incidents. This plan should outline the steps to be taken in the event of a breach, including containment, eradication, and recovery procedures.

Automating incident response using AWS Lambda:

```python
import boto3

def lambda_handler(event, context):
    ec2 = boto3.client('ec2')

    # Stop an instance when a security event occurs
    instance_id = event['detail']['instance-id']
    response = ec2.stop_instances(InstanceIds=[instance_id])

    return response
```

3.3.5 Continuous Monitoring and Auditing

Continuous monitoring of cloud infrastructure helps detect anomalies and potential security threats in real-time. Automated tools and security information and event management (SIEM) systems can assist in aggregating and analyzing security logs to identify and respond to incidents promptly.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

3.3.6 Vendor Management

Evaluating and managing the security posture of third-party vendors is essential to mitigate supply chain risks. This includes conducting regular security assessments, establishing clear security requirements, and ensuring compliance with industry standards and regulations.

3.3.7 Importance of Cloud Infrastructure in National Security

National security agencies increasingly rely on cloud computing to manage vast amounts of data, perform complex analyses, and enable agile and efficient operations. Cloud infrastructure provides the scalability and flexibility required to support national security missions, from intelligence gathering and analysis to operational planning and execution. However, the sensitivity and critical nature of the data handled by these agencies make cloud infrastructure security paramount.

3.4 Specific Security Challenges for National Security

3.4.1 Data Classification and Segregation

National security data is often classified at various levels, from unclassified to top-secret. Ensuring that data is properly classified and segregated within the cloud environment is crucial to prevent unauthorized access and maintain data integrity.

Example: Using AWS S3 bucket policies to restrict access based on data classification:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::top-secret-bucket/*",
      "Condition": {
        "StringNotEquals": {
          "aws:userid": [
            "classified-user-id-1",
            "classified-user-id-2"
          ]
        }
      }
    }
  ]
}
```

3.4.2 Secure Communication Channels

National security operations often require secure communication channels to transmit sensitive information between cloud environments and on-premises systems. This includes ensuring end-to-end encryption and protecting against man-in-the-middle attacks.

Using AWS KMS to encrypt data in transit:

3.4.3 Identity and Access Management

Robust identity and access management (IAM) is critical for national security agencies to ensure that only authorized personnel can access sensitive data and systems. This involves implementing multi-factor authentication (MFA), strict role-based access controls (RBAC), and continuous monitoring of access logs.

Example: Using Azure Active Directory (Azure AD) for RBAC:

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

```python
import boto3

# Create a KMS client
kms = boto3.client('kms')

# Encrypt the data
plaintext = b'Sensitive national security data'
response = kms.encrypt(
    KeyId='alias/secure-key',
    Plaintext=plaintext
)

ciphertext = response['CiphertextBlob']

# Decrypt the data
response = kms.decrypt(
    CiphertextBlob=ciphertext
)

decrypted_text = response['Plaintext']
print(decrypted_text.decode('utf-8'))
```

3.4.4 Threat Intelligence and Monitoring

National security agencies must have access to real-time threat intelligence to detect and respond to advanced cyber threats. This involves integrating threat intelligence feeds with security information and event management (SIEM) systems to analyze and correlate data for potential security incidents.

Integrating threat intelligence with AWS GuardDuty:

```python
import boto3

# Create a KMS client
kms = boto3.client('kms')

# Encrypt the data
plaintext = b'Sensitive national security data'
response = kms.encrypt(
    KeyId='alias/secure-key',
    Plaintext=plaintext
)

ciphertext = response['CiphertextBlob']

# Decrypt the data
response = kms.decrypt(
    CiphertextBlob=ciphertext
)

decrypted_text = response['Plaintext']
print(decrypted_text.decode('utf-8'))
```

3.5 Best Practices for Enhancing Cloud Security in National Security

3.5.1 Zero Trust Architecture

Adopting a Zero Trust Architecture (ZTA) ensures that no entity, whether inside or outside the network, is trusted by default. This involves continuously verifying the identity and integrity of users and devices, enforcing least-privilege access, and segmenting networks to prevent lateral movement.

3.5.2 Continuous Compliance Monitoring

National security agencies must ensure continuous compliance with regulatory and policy requirements. Automated compliance monitoring tools can help identify and remediate compliance issues in real-time, reducing the risk of non-compliance.

Example: Using AWS Config for compliance monitoring:

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

```
import boto3

# Create AWS Config client
config = boto3.client('config')

# Create a compliance rule
response = config.put_config_rule(
    ConfigRule={
        'ConfigRuleName': 's3-bucket-public-read-prohibited',
        'Source': {
            'Owner': 'AWS',
            'SourceIdentifier': 'S3_BUCKET_PUBLIC_READ_PROHIBITED
        },
        'Scope': {
            'ComplianceResourceTypes': ['AWS::S3::Bucket']
        }
    }
)
```

3.5.3 Security Training and Awareness

Continuous training and awareness programs are essential to ensure that all personnel understand the security policies and best practices for handling sensitive information within the cloud environment. Regular training helps mitigate the risk of human error and insider threats.

IV. METHODOLOGY

1. Research Philosophy

This research incorporates interpretivism research philosophy for understanding the complicated social phenomenon and subjective experiences related to cloud infrastructure security within the financial and national security contexts. This philosophy enables the research in the exploration of the different human behaviors, cultural factors and organizational dynamics.

2. Research approach

The deductive research approach is utilized for testing the existing frameworks and theories associated with cloud infrastructure security in the national and financial security sectors. Through the application of this approach, researchers can evaluate the efficiency and applicability of the security strategies in these specific contexts.

3. Research design

The secondary qualitative research design is selected for leveraging existing data on cloud infrastructure security. This approach includes the analysis of previously gathered qualitative data such as academic literature and reports for the identification of the themes and patterns which is relevant to the research questions. This method is useful for studying complicated and well-documented fields such as cloud security.

4. Data collection method

This research used the peer review data collection method that can provide significant insights into industry reports, academic articles, and governmental publications. This method would ensure that the information used in the paper is reliable, authentic, and scrutinized by professionals. Sources that are reviewed extensively provide high-quality evidence and different perspectives that are crucial for the comprehensive analysis of the cloud infrastructure security challenges.

5. Ethical consideration

The protection of confidentiality for personal and sensitive data is one of the most vital factors in research. This study has ensured that the data related to the security protocols or vulnerabilities is

stored securely for the prevention of unauthorized access. It is essential to ensure the integrity and accuracy of the data during the data collection. This study significantly used reliable and associated sources besides verifying the gathered information to avoid spreading misinformation.

V. RESULTS

1. Findings and Discussion

Theme 1: Present state of cloud infrastructure security in financial and national security sectors

The current concepts of cloud infrastructure security within the financial and national security sector hold significant opportunities. The study by Mahalle et al. (2018) highlights the critical issues regarding data privacy along with system security within the banking sector. However, cloud adoption provides substantial opportunities such as cost-effectiveness and scalability. Yet, it also has significant risks. These risk factors include vulnerabilities to unauthorized access, data breaches, and other cyber threats [9]. Hence, it is vital to implement an effective security framework within the cloud environments that integrate multi-layered security strategies that include access control, encryption, and security strategies. Ensuring compliance with the regulator system is necessary for the successful integration of digital technologies such as machine learning and artificial intelligence [10]. It further assists in detecting the potential challenges and taking necessary measures to mitigate these issues. This will significantly contribute to the maintenance of resilience within the critical financial infrastructure within the cloud environment.

Theme 2: vulnerabilities and threats specific to these sectors

The financial and national security institutions pose significant threats and challenges that hinder the effectiveness of cloud security measures within the financial and national security-maintained institutions. Allodi and Massacci (2017) highlight the utilization of security events and the vulnerabilities in data for the estimation of cybersecurity risks by emphasizing the financial and national security sectors. The main vulnerabilities in this area include unpatched systems, flaws in software, and misconfigurations that can be exploited by cyber attackers. Challenges such as targeted attacks, advanced persistent threats (APTs), and zero-day exploits are particularly concerning due to their potential to cause significant disruption [11]. As the traditional risk assessment and control method is insufficient for mitigating these issues, it is necessary to incorporate the data-driven approaches which assist in the identification of real-time vulnerability along with the threat intelligence in data structure.

This approach can enhance the prediction and mitigation of risks, ensuring the protection of vital assets in financial and national security infrastructures.

Theme 3: Effectiveness of these security measures through simulations

Successful integration of the potential security measures can able to mitigate the issues related to cloud security. Lu et al. (2018) conducted a holistic survey of the security, privacy and trustworthy challenges within the vehicular network by emphasizing on the efficiency of the various security measures through simulations. Those simulations that underline the cryptographic framework, privacy-maintaining protocols and trust management techniques can eliminate the common security threats within the vehicular networks [12]. The simulation of the cryptographic schemes assures the comprehensibility of the security management system for maintaining communication between the vehicles. These measures are performed in a strategic way within the controlling field, network dynamics and high mobility which can reduce the efficiency.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

2. Evaluation

The research related to cloud infrastructure security for critical financial infrastructure and national security underlines the necessity of the implementation of a vigorous risk-eliminating system to identify and mitigate the emerging concerns related to the cloud-based system. This research identifies the unique threats faced by financial institutions by underlining the insufficiency of general cloud security measures. This research poses a significant strength related to the integration of regulatory, technical and human-centric approaches for the overall analysis. The incorporation of secondary qualitative data highlights the potential of this research to provide insights into the peer-reviewed data sources [13]. The proposed security frameworks within the practical applicability can be tested through the simulation which offers solid evidence of their effectiveness.

VI. Limitations/Challenges for Implementation

Implementing enhanced cloud infrastructure security for critical financial infrastructures (CFIs) and national security systems faces several limitations and challenges. While cloud technology offers scalability, efficiency, and cost-effectiveness, integrating robust security frameworks tailored to these sensitive sectors introduces unique obstacles. These challenges can significantly impact the practical application of proposed security strategies, as outlined below:

1. Complexity of Regulatory Compliance

Both CFIs and national security agencies are subject to stringent and often overlapping regulations, such as GDPR in Europe or FINRA regulations in the United States. Ensuring that cloud-based infrastructures comply with these requirements across multiple jurisdictions poses significant challenges. Given that cloud providers typically operate across borders, achieving compliance with varying national regulations for data protection and cybersecurity can be time-consuming and resource intensive. Moreover, regulations frequently change, necessitating constant updates to security protocols to maintain compliance.

2. Resource Constraints

For smaller financial institutions or national security agencies with limited budgets, the cost of implementing advanced cloud security solutions, such as encryption mechanisms, continuous monitoring systems, and incident response frameworks, can be prohibitive. High upfront costs for transitioning to a secure cloud environment, along with the ongoing expenses for maintaining compliance and addressing new security threats, may delay the implementation of comprehensive security frameworks. Additionally, cloud security requires continuous investment in workforce training and the adoption of new technologies, which may not be feasible for organizations with constrained resources.

3. Increased Attack Surface

Migrating critical operations to the cloud, particularly in multi-tenant environments, increases the attack surface that must be secured. Cloud environments often host multiple users, creating the risk of data leakage or accidental access to sensitive information across tenant boundaries. Additionally, vulnerabilities in third-party software or cloud provider infrastructure could be exploited to compromise sensitive data, exacerbating security concerns in sectors where data breaches could have catastrophic consequences.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

4. Lack of Cloud Expertise and Skilled Workforce

Implementing advanced security protocols requires specialized expertise in cloud technologies, cybersecurity, and threat intelligence. Many financial institutions and national security agencies may lack the internal expertise to design, deploy, and manage secure cloud environments. While outsourcing these responsibilities to cloud providers is possible, reliance on third-party vendors introduces its own risks, such as potential breaches of contract, lack of transparency, or loss of control over sensitive data.

5. Security in Shared Responsibility Model

Cloud service providers use a shared responsibility model in which the client is in charge of protecting the data, apps, and configurations that are put in the cloud, while the provider handles the security of the cloud infrastructure. This division of responsibilities can create gaps in security if institutions fail to fully understand their role or misconfigure cloud resources. Misconfigurations, such as unsecured storage or lax access controls, have historically been a major cause of cloud security breaches. Ensuring that CFIs and national security agencies adhere to best practices in their areas of responsibility is crucial but challenging given the complexity of cloud environments.

6. Handling Insider Threats

While cloud environments offer robust external security measures, internal threats remain a persistent challenge. Insider threats, whether through negligence or malicious intent, pose significant risks to cloud infrastructure security. Financial institutions and national security agencies typically handle highly sensitive information, and any compromise could lead to major financial losses or national security breaches. Monitoring and detecting insider threats in real-time, while ensuring compliance with privacy regulations, requires advanced security measures such as anomaly detection and behavioral analysis—technologies that may be difficult to implement effectively.

7. Latency and Performance Concerns

Cloud infrastructure, particularly for national security operations, often requires real-time or near-real-time performance. Implementing encryption, multi-factor authentication (MFA), and other security measures can introduce latency, which may be unacceptable in critical scenarios, such as in national defense or high-frequency financial transactions. A major difficulty is striking a balance between security and performance, particularly in settings where time is of the critical.

8. Dependency on Cloud Providers

Another challenge is the dependency on cloud providers for certain critical functions. Cloud providers may impose restrictions on certain security features, limit transparency, or lack support for certain regulatory compliance requirements. Additionally, financial institutions and national security agencies may not have full visibility into the physical location of their data or the processes that cloud providers use to secure their infrastructure, raising concerns about data sovereignty and the ability to perform adequate audits and forensic investigations in the event of a breach.

International Journal of Core Engineering & Management
Volume-6, Issue-12, 2021 ISSN No: 2348-9510

9. Supply Chain Risks

Supply chain vulnerabilities can be exploited by adversaries to target cloud infrastructure. An attacker's point of entry into a crucial system may be a compromised third-party provider or service within the cloud ecosystem. Given the interconnected nature of cloud services, ensuring the security of third-party components is complex, as vulnerabilities in supply chain services could have far-reaching implications for CFIs and national security agencies.

10. Challenges in Incident Response and Forensic Analysis

Incident response and forensic investigation are made more difficult by the dynamic, swiftly formed, scaled, and terminated character of cloud infrastructures. It can be challenging to retain necessary logs or investigate security incidents if proper monitoring and auditing mechanisms are not in place from the start. Moreover, traditional on-premises forensic techniques may not be directly applicable to cloud environments, requiring specialized cloud forensic tools and expertise. There could be serious consequences from failing to recognize and address security issues in a timely manner, especially for organizations in charge of vital infrastructure and national security.

VII. CONCLUSION

1. The national security system and financial considerations are essential for developing business processes in the FinTech industry.
2. Cloud systems enhance the data protection system, aiding in the development of internal security measures.
3. Cloud infrastructure improves security by reducing risks in data management processes.
4. Privacy protocols and trust-building activities are critical to addressing common security issues, particularly in vehicular tasks.
5. Risk mitigation and trust enhancement through cloud management are essential for secure operations.
6. The cloud structure's ability to store and manage secure access to data improves security in the FinTech industry while offering financial benefits to customers.
7. The security of financial organizations and the FinTech industry is crucial for protecting the national economy.
8. The national security system also encompasses information security for the military, large organizations, and IT sectors.

VIII. RESEARCH RECOMMENDATION

In order to promote proper research this research paper could focus on different cloud platforms to enhance financial and national security. Again, this study depends on secondary source information; hence, information from primary sources, such as the managers could be more beneficial to understanding the cloud infrastructure for financial and national security systems.

IX. FUTURE WORK

This research process focuses on the way cloud computing is beneficial for managing security infrastructure for increasing national and financial security. However, this research paper does not present different cloud platforms and their works on the financial and national security services. Hence, further research can be conducted on this aspect. Furthermore, this study can present the

way different countries are working with cloud infrastructure to strengthen their national and financial security system. Hence, this combination can be crucial for future work.

REFERENCES

1. M. N. Birje, P. S. Challagidad, R. H. Goudar, and M. T. Tapale, "Cloud computing review: concepts, technology, challenges and security," Int. J. Cloud Comput., vol. 6, no. 1, pp. 32-57, 2017. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJCC.2017.083905.
2. R. Mandel, Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks. Georgetown University Press, 2017. Available: https://books.google.com/books?hl=en&lr=&id=cCEQDgAAQBAJ&oi=fnd&pg=PP1&dq=The+higher+level+of+data+value+maintained+through+the+entities+makes+them+prime+prey+for+cyberattacks.+&ots=9jxhvtz9wF&sig=otVySCqHpQZvTbz7fnFe6r7mSoc.
3. A. Yeboah-Ofori, J. D. Abdulai, and F. Katsriku, "Cybercrime and risks for cyber physical systems: A review," Preprints, Apr. 2018. Available: https://www.preprints.org/manuscript/201804.0066.
4. U. M. Ismail, S. Islam, M. Ouedraogo, and E. Weippl, "A framework for security transparency in cloud computing," Future Internet, vol. 8, no. 1, p. 5, 2016. Available: https://www.mdpi.com/1999-5903/8/1/5.
5. R. K. Koehler, "When the lights go out: vulnerabilities to US critical infrastructure, the Russian cyber threat, and a new way forward," Georgetown Secur. Stud. Rev., vol. 7, no. 1, pp. 27-36, 2018. Available: https://georgetownsecuritystudiesreview.org/wp-content/uploads/2019/01/GSSR-7.1-final-text-updated.pdf#page=27.
6. R. Barona and E. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," in 2017 Int. Conf. Circuit, Power and Comput. Technol. (ICCPCT), 2017, pp. 1-8. Available: https://ieeexplore.ieee.org/abstract/document/8074287/.
7. A. Vishwakarma, "Virtual private networks," in Network Security Attacks and Countermeasures, IGI Global, 2016, pp. 78-114. Available: https://www.igi-global.com/chapter/virtual-private-networks/143967.
8. M. Bhusan, R. S. Rathore, and A. Jamshed, Fundamental of Cyber Security: Principles, Theory and Practices. BPB Publications, 2018. Available: https://books.google.com/books?hl=en&lr=&id=BY1jDwAAQBAJ&oi=fnd&pg=PR7&dq=the+%E2%80%9CCyber+Security%E2%80%9D+theory+is+also+presented+as+an+essential+theory+that+underlines+the+application+of+technologies,+procedures+and+controls+for+the+protection+of+network+systems,+devices+and+programmes.&ots=_lrvcPZaqh&sig=xQAuFbszo6Br8O2f7O-eJHdUHvM.
9. A. Mahalle, J. Yong, X. Tao, and J. Shen, "Data privacy and system security for banking and financial services industry based on cloud computing infrastructure," in 2018 IEEE 22nd Int. Conf. Comput. Supported Cooperative Work Des. (CSCWD), 2018, pp. 407-413. Available: https://ieeexplore.ieee.org/abstract/document/8465318/.
10. A. Banwo, "Artificial intelligence and financial services: Regulatory tracking and change management," J. Securities Oper. Custody, vol. 10, no. 4, pp. 354-365, 2018. Available: https://www.ingentaconnect.com/content/hsp/jsoc/2018/00000010/00000004/art00009.
11. L. Allodi and F. Massacci, "Security events and vulnerability data for cybersecurity risk estimation," Risk Analysis, vol. 37, no. 8, pp. 1606-1627, 2017. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12864.

12. Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 2, pp. 760-776, 2018. Available: https://ieeexplore.ieee.org/abstract/document/8345196/.
13. W. Bandara, E. Furtmueller, E. Gorbacheva, S. Miskon, and J. Beekhuyzen, "Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support," Commun. Assoc. Inf. Syst., vol. 37, no. 1, p. 8, 2015. Available: https://aisel.aisnet.org/cais/vol37/iss1/8/.
14. Viega, J. (2009). Cloud computing and the common man. Computer, 42(8), 106-108.
15. Bowers, K. D., Juels, A., & Oprea, A. (2009). HAIL: A high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 187-198).
16. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2010). Toward secure and dependable storage services in cloud computing. IEEE transactions on Services Computing, 5(2), 220-232.
17. Kamara, S., & Lauter, K. (2010). Cryptographic cloud storage. In International Conference on Financial Cryptography and Data Security (pp. 136-149). Springer, Berlin, Heidelberg.
18. Grobauer, B., Walloschek, T., & Stöcker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
19. Akin, O., & Akbulut, N. (2011). Security issues in cloud computing: A survey. In 2011 International Symposium on Innovations in Intelligent Systems and Applications (pp. 238-243). IEEE.
20. Leavitt, N. (2009). Is cloud computing really ready for prime time? Computer, 42(1), 15-20.
21. Sun, D. Z., Zhang, G. R., Chen, L. M., & Zhang, J. X. (2011). Formal security analysis and verification of cloud storage systems. In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (pp. 279-284). IEEE.
22. Ko, R. K., Lee, B. S., & Pearson, S. (2011). Towards achieving accountability, auditability and trust in cloud computing. In International Conference on Advances in Computing and Communications (pp. 432-444). Springer, Berlin, Heidelberg.
23. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of cloud computing. The Journal of Supercomputing, 63(2), 561-592.
24. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.
25. Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702).
26. Li, J., Li, Y., Lee, P. P., & Wang, X. (2012). Secure deduplication with efficient and reliable convergent key management. IEEE transactions on parallel and distributed systems, 25(6), 1615-1625.
27. Gellman, R. (2009). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. World Privacy Forum.
28. Wei, J., Zhang, X., & Ammons, G. (2009). Managing security of virtual machine images in a cloud environment. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 91-96).
29. Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security? (No. UCB/EECS-2010-5). University of California, Berkeley.
30. Bernd, L., & Marx, G. (2010). The cloud computing strategy of the European Commission: The challenges of cloud computing for the EU policy. Journal of Law and Governance, 5(1).

31. Chhabra, S., & Dixit, A. (2012). Cloud computing: State of the art and security issues. ACM Computing Surveys (CSUR), 44(3), 1-24.
32. Kandukuri, B. R., & Rakshit, A. (2009). Cloud security issues. In 2009 IEEE International Conference on Services Computing (pp. 517-520).
33. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386.
34. Xu, H., & Teo, H. H. (2009). Alleviating consumer's privacy concerns in location-based services: a psychological control perspective. In ICIS (p. 84).
35. Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards trusted cloud computing. In Proceedings of the 2009 conference on Hot topics in cloud computing (pp. 1-6).
36. Behl, A., & Behl, K. (2012). An analysis of cloud computing security issues. In 2012 World Congress on Information and Communication Technologies (pp. 109-114).
37. Stanoevska-Slabeva, K., Wozniak, T., & Ristol, S. (2010). Grid and cloud computing: A business perspective on technology and applications. Springer Science & Business Media.
38. Popovic, K., & Hocenski, Z. (2010). Cloud computing security issues and challenges. In The 33rd International Convention MIPRO (pp. 344-349).
39. Boss, G., Malladi, P., Quan, D., Legregni, L., & Hall, H. (2007). Cloud computing. IBM white paper, 8(2), 214-226.
40. Cavoukian, A. (2008). Privacy in the clouds. Identity in the Information Society, 1(1), 89-108.
41. Chieu, T. C., Mohindra, A., Karve, A. A., & Segal, A. (2009). Dynamic scaling of web applications in a virtualized cloud computing environment. In 2009 IEEE International Conference on e-Business Engineering (pp. 281-286).
42. Brown, A. S. (2008). Cloud computing: A security meltdown. Network Security, 2008(12), 4-8.
43. King, N., & Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308-319.