Secure Cloud Network Architecture for Multi-Tier Application

Dr. Rubaiyat Islam
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
rubaiyatislam17002sets@iub.edu.bd

Kazi Mahbub Morshed Limon
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
2231316@iub.edu.bd

Rudrita Rahman
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
2021059@iub.edu.bd

MD. Protik Hasan
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
2022133@iub.edu.bd

Shatabde Debnath
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
2020552@iub.edu.bd

MD Abu Sauri Sufian
Computer Science and Engineering
Independent Unviversity, Bangladesh
Dhaka, Bangladesh
1930839@iub.edu.bd

***Abstract*—Cloud computing has become an integral part of modern business operations, offering scalability and flexibility. However, ensuring the security and integrity of data in the cloud remains an unanswered concern. This project, titled ”Secure Cloud Network Architecture for Multi-Tier Applications,” presents a comprehensive approach to address these challenges. The primary objective of this project is to provide secure cloud services tailored to the unique needs of organizations in Bangladesh. The methodology encompasses manual configuration of network architectures using Amazon Web Services (AWS) to meet immediate requirements, alongside the development of an automated service for future scalability. This dual-pronged approach combines data security, network segmentation, and ease of deployment. By implementing a Secure Cloud Network Architecture for Multi-Tier Applications, we seek to enhance data security and application reliability in the cloud environment. This project not only addresses critical security challenges but also paves the way for improved scalability and efficiency, contributing to the growth and security of organizations in Bangladesh.**

***Index Terms*—segmentation, component, formatting, manual configuration, encompass**

I. Introduction

In an ever-evolving information technology landscape, cloud computing has changed the way how businesses operate drastically. This paradigm shift has enabled them to have scalable, flexible, reliable, sustainable, and affordable access to products and services without significant capital investment in hardware and infrastructure. With the advent of cloud technology, there has been an increasing demand for efficient, cost-effective solutions. As organizations, particularly small businesses, increasingly seek to leverage the potential of cloud services provided by industry giants like AWS, Azure, Alibaba Cloud, OCI, and GCP a crucial challenge arises in ensuring the security and efficient management of the complex cloud network architecture. In particular, multi-tier applications are vulnerable to a variety of attacks, such as DDoS attacks, data breaches, and unauthorized access. This paper introduces a groundbreaking approach, presenting a novel and pivotal intermediary that connects cloud providers and consumers. The approach involves the development of a secure cloud network architecture tailored for multi-tier applications. This architecture prioritizes data confidentiality, integrity, and availability, while also ensuring scalability and efficiency.

The ever-growing demand for cloud services has brought to the forefront the need for a reliable mediator that not only orchestrates the allocation of cloud resources but also guarantees the safeguarding of sensitive data and the seamless functioning of multi-tier applications. Our proposed architecture not only acts as a broker between cloud providers and small business holders, but it also introduces a comprehensive security framework to address the intricate nature of cloud-based interactions. This framework is tailored to accommodate the evolving landscape of cloud technology, ensuring that confidentiality, integrity, and availability of data remain uncompromised.

This paper delves deeper into the cloud-based service-providing industry, focusing on creating a secure and robust network infrastructure designed for the small business vendor ecosystem. In the initial phase, this architecture will involve the manual allocation of resources to meet the specific needs of consumers. However, the roadmap for the future envisions a transition towards automated resource allocation, wherein the system adapts dynamically to the changing requirements of customers. By aligning resource allocation with customer demands, this transition aims to enhance the efficiency and effectiveness of cloud service consumption.

The main idea of the cloud is the pay-per-use model, which has attracted both individuals and businesses looking to profit from this new approach. A survey in 2020 of 750 global cloud professionals revealed that due to the COVID-19 impact, organizations planned to increase their spending on cloud services by 47 percent in 2021. The fastest-growing cloud service consumers, such as IoT, machine learning/AI, data warehouses, and server-less markets, are expected to grow by an average of 47.2 percent. Although companies like Google, Microsoft, and IBM compete to offer the best solutions, more research is needed in the field of security solutions. Despite the clear advantages of cloud computing, there are security concerns due to the complex nature of the model and shared technologies. The various components involved in the cloud paradigm, including networks, architectures, APIs, and hardware, make security issues more intricate. As a result, both cloud providers and clients can encounter security vulnerabilities due to different combinations of cloud configurations. The National Institute of Standards and Technology (NIST) has established the service-based model as a standard for cloud computing.

II. Literature Review

The paper [1] underscores the significance of Cloud Access Security Brokers (CASBs) in addressing cloud security challenges and offers insights into their functionalities and real-world applications. It emphasizes CASBs' pivotal role in securely embracing cloud computing while maintaining strong security postures. However, a drawback is its limited technical depth and quantitative analysis. To improve, the paper should incorporate technical details, and quantitative data, expand case studies, offer comparative analysis, provide practical guidance, discuss security standards, and address future trends and challenges. This would make it a more comprehensive and practical resource for individuals and organizations navigating cloud security concerns.

The paper [2] tackles cloud resource acquisition challenges and introduces STRATOS as a solution, valuable for cloud professionals and organizations seeking to enhance resource management. However, it lacks technical implementation details, limiting its practical utility. To address this, the authors should include a section with technical specifics like code examples and diagrams to aid readers in implementing similar cloud broker services effectively.

The paper [3] serves as a comprehensive guide for organizations in evaluating the security capabilities of different Cloud Service Providers (CSPs), emphasizing systematic assessment and informed decision-making for a secure cloud environment. It caters to cloud architects, IT professionals, and organizations seeking to bolster their cloud security posture. However, a drawback is the absence of real-world examples or case studies to illustrate the guidance provided. To address this limitation, the paper should incorporate practical scenarios, tools, and interactive discussions with experts or organizations to enhance its practical applicability and provide concrete insights for readers.

The paper [4] addresses issues with cloud connectivity and suggests a platform for improved cloud service integration in web applications. Although it is a helpful tool for cloud architects and web developers, it is largely focused on middleware and lacks actual implementation details. The document should be improved by adding real-world examples, discussing more complex cloud integration concerns, and reducing middleware dependencies.

The paper [5] highlights the challenges and opportunities in cloud computing, emphasizing the need for mature operational models like cloud bursting, brokerage, and aggregation to facilitate broader enterprise adoption. It addresses security, integration, and platform vulnerabilities as key barriers and outlines the capabilities and requirements of these models, with a focus on cloud brokerage. While valuable for shedding light on cloud challenges and concepts, it lacks practical implementation examples and assumes prior cloud knowledge. To overcome these limitations, the paper suggests including real-world examples, clarifying basic cloud concepts, conducting practical testing, collaborating with industry, and expanding its coverage to provide a more comprehensive guide to cloud operational models.

The paper [6] explores the landscape of cloud computing in Bangladesh, focusing on security concerns and the rising adoption of cloud services. It serves as a valuable resource for various stakeholders, including researchers, policymakers, and IT professionals, by providing insights into the opportunities and challenges within this emerging field. While effectively addressing security issues in the context of Bangladesh, the paper could enhance its impact by broadening its scope to cater to a global audience, offering more technical depth, delving into data privacy and policy considerations, and providing real-world examples and case studies from Bangladeshi organizations.

The paper [7] discusses the significance of multi-cloud computing in meeting the evolving needs of organizations and emphasizes the importance of unified platforms. It highlights the challenges and solutions associated with multi-cloud adoption and identifies the SUPERCLOUD project model as a promising direction for future multi-cloud architecture development, though further research and implementation are needed to fully realize its potential. The paper effectively delivers valuable insights into multi-cloud computing, its challenges, and potential solutions, making it a valuable resource for researchers and practitioners in the field of cloud computing. However, it has weaknesses related to specificity, depth of analysis, practical examples, and organization. To address these weaknesses, the paper recommends providing specific details about the SUPERCLOUD model, discussing challenges with real-world examples, including insights from actual multi-cloud implementations, and enhancing security analysis while diversifying information sources.

The paper [8] introduces the CLOUD-OF-CLOUD protocol, a novel solution addressing privacy and security concerns in multi-cloud data storage and sharing. It emphasizes the protocol's two-factor access control, incorporating one-time passwords (OTPs) and secret keys, preventing unauthorized key exchange, and ensuring user anonymity. Practical implementation tests validate the system's feasibility and efficiency. The paper effectively tackles a significant issue in cloud computing, presenting an innovative and practical solution that advances knowledge in the field. However, it acknowledges areas for improvement, including the need for enhanced evaluation metrics and a comparative analysis with existing protocols, addressing potential vulnerabilities, discussing scalability, and considering real-world deployment challenges. Balancing security measures with user-friendliness is also emphasized to enhance the protocol's real-world relevance.

The paper [9] delves into the intricate relationship between virtualization, security, and cloud computing, offering valuable insights through a taxonomy of attacks, an evaluation of existing solutions, and an emphasis on collaboration between cloud service providers and customers for cloud-based virtualized system security. While effective, the paper lacks real-world examples, and in-depth vulnerability analysis, occasionally uses complex terminology, offers limited practical implementation guidance, and could benefit from the improved organization. Nevertheless, it bridges theory and real-world concerns, providing a vital resource for cloud security stakeholders by clarifying roles, offering a taxonomy of threats, and guiding security measures while suggesting future research directions.

The growing concern about data security in cloud storage, with 61 percent of organizations considering it a significant issue is discussed in paper [10]. It highlights the use of data encryption to address these concerns, focusing on the challenge of enabling efficient searches within encrypted data. The paper introduces a Cloud Access Security Broker (CASB)-based framework as a potential solution, aiming to maintain search functionality while enhancing security. The proposed approach builds a local search index and addresses technical challenges such as key management, offering a promising balance between data security and search capabilities.

In paper [11] the focus is on assessing security concerns in service-based cloud computing. The paper's contributions include presenting recent vulnerabilities, proposing a taxonomy for these vulnerabilities and their countermeasures, exploring research challenges and future directions, and classifying vulnerabilities and countermeasures into four categories: IaaS, PaaS, SaaS, and generic. The study emphasizes the prevalence of issues like DoS/DDoS attacks, shared technology vulnerabilities, and session hijacking in cloud security discussions. It underscores the need for continued research due to the evolving complexity of cloud architecture and the introduction of new security threats as cloud services diversify. Both providers and customers should be vigilant about the risks associated with their specific configurations in this dynamic cloud environment.

III. Proposed System Methodology

This section outlines the methodology employed in conducting research on secure cloud network architecture for multitier applications. The methodology encompasses the research design, data collection, analysis techniques, and ethical considerations undertaken to achieve the research objectives.

A. Research Design

The research adopts a mixed-methods approach, combining both quantitative and qualitative methods to comprehensively address the multifaceted aspects of secure cloud network architecture for multi-tier applications.

B. Data Collection

1) Literature Review: A comprehensive literature review is conducted to understand the current state of research, and identify key security concerns, architectural paradigms, and best practices. This forms the foundational knowledge for the research.

2) Case Studies: Real-world case studies are collected from organizations that have successfully implemented secure cloud network architecture for multi-tier applications. These case studies provide insights into practical challenges, solutions, and lessons learned.

3) Surveys: Surveys are distributed to IT professionals, cloud architects, and security experts to gather quantitative data on the prevalence of security challenges, adoption rates of architectural approaches, and effectiveness of security measures.

4) Interviews: Semi-structured interviews are conducted with industry experts and practitioners to delve deeper into nuanced aspects of secure cloud network architecture. These qualitative insights offer a holistic understanding of the subject matter.

C. Data Analysis

1) Literature Synthesis: The findings from the literature review are synthesized to identify recurring themes, security concerns, architectural approaches, and emerging trends. This synthesis forms the foundation for framing research questions.

2) Case Study Analysis: Case studies are analyzed qualitatively to extract best practices, challenges faced, and innovative solutions implemented in the context of secure cloud network architecture.

3) Survey Analysis: Quantitative survey data is analyzed using statistical techniques to quantify the prevalence of security concerns, adoption rates of architectural approaches, and correlations between variables.

4) Interview Transcription and Coding: Qualitative interview data is transcribed and coded using thematic analysis. Common themes, patterns, and unique insights are identified to enrich the research findings.

D. Ethical Considerations

1) Informed Consent: Participants in surveys and interviews are provided with clear information about the research objectives and their role. Informed consent is obtained before data collection.

2) Anonymity and Confidentiality: Participants' identities and responses are kept confidential. Any identifying information is removed from interview transcripts and survey data to ensure anonymity.

3) Data Security: Data collected, including survey responses and interview transcripts, are securely stored and accessible only to authorized researchers.

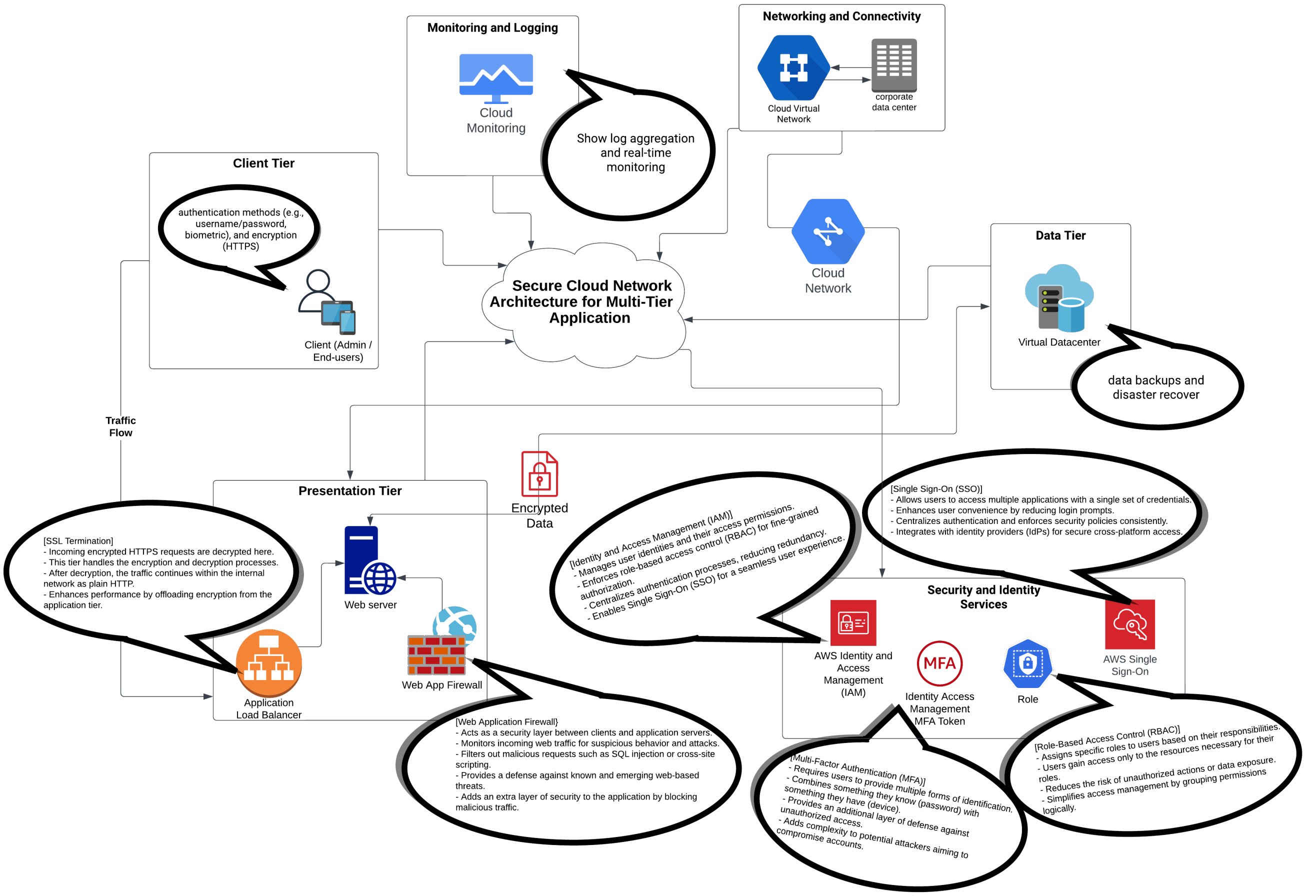
Monitoring and Logging
Cloud Monitoring
Show log aggregation and real-time monitoring
Networking and Connectivity
Cloud Virtual Network
corporate data center
Client Tier
authentication methods (e.g., username/password, biometric), and encryption (HTTPS)
Client (Admin / End-users)
Secure Cloud Network Architecture for Multi-Tier Application
Cloud Network
Data Tier
Virtual Datacenter
data backups and disaster recover
Traffic Flow
Presentation Tier
Encrypted Data
[SSL Termination] - Incoming encrypted HTTPS requests are decrypted here. - This tier handles the encryption and decryption processes. - After decryption, the traffic continues within the internal network as plain HTTP. - Enhances performance by offloading encryption from the application tier.
Web server
Application Load Balancer
Web App Firewall
[Identity and Access Management (IAM)] - Manages user identities and their access permissions. - Enforces role-based access control (RBAC) for fine-grained authorization. - Centralizes authentication processes, reducing redundancy. - Enables Single Sign-On (SSO) for a seamless user experience.
[Single Sign-On (SSO)] - Allows users to access multiple applications with a single set of credentials. - Enhances user convenience by reducing login prompts. - Centralizes authentication and enforces security policies consistently. - Integrates with identity providers (IdPs) for secure cross-platform access.
Security and Identity Services
AWS Identity and Access Management (IAM)
MFA
Identity Access Management MFA Token
Role
AWS Single Sign-On
[Web Application Firewall} - Acts as a security layer between clients and application servers. - Monitors incoming web traffic for suspicious behavior and attacks. - Filters out malicious requests such as SQL injection or cross-site scripting. - Provides a defense against known and emerging web-based threats. - Adds an extra layer of security to the application by blocking malicious traffic.
[Multi-Factor Authentication (MFA)] - Requires users to provide multiple forms of identification. - Combines something they know (password) with something they have (device). - Provides an additional layer of defense against unauthorized access. - Adds complexity to potential attackers aiming to compromise accounts.
[Role-Based Access Control (RBAC)] - Assigns specific roles to users based on their responsibilities. - Users gain access only to the resources necessary for their roles. - Reduces the risk of unauthorized actions or data exposure. - Simplifies access management by grouping permissions logically.

Fig. 1. Rich Picture

E. Limitations and Delimitations

The research acknowledges potential limitations such as selection bias in case study participants and survey respondents, as well as the dynamic nature of cloud technology that might render certain findings outdated over time.

F. Contribution to Knowledge

This research aims to contribute by providing a comprehensive understanding of secure cloud network architecture for multi-tier applications, highlighting effective security measures, architectural strategies, and emerging trends.

G. Technical analysis

The proposed problems and solutions are as follows:

1) **Problem:** Sensitive data is not properly encrypted, which could lead to data breaches.
   Solution: Implement end-to-end encryption for data in transit and at rest, using industry-standard encryption algorithms. This will ensure that only authorized users can access the data, even if it is intercepted in transit or stored on a compromised system.
2) **Problem:** User roles and permissions are not properly managed, which could lead to unauthorized access to sensitive data.
   Solution: Implement robust IAM solutions to manage user roles, permissions, and authentication. This will ensure that only authorized users have access to the data they need, and that their access is properly controlled.
3) **Problem:** Application tiers are not properly isolated, which could allow attackers to move laterally within a system. Solution: Utilize network segmentation to isolate application tiers. This will limit the potential impact of a security breach in one tier to other tiers.
4) **Problem:** Security threats are not being monitored or mitigated in real time.
   Solution: Deploy IDPS to monitor and mitigate threats in real-time. This will help to identify and respond to security threats quickly, before they can cause damage.
5) **Problem:** Security protocols are not automated, which could lead to delays in responding to security breaches or vulnerabilities.
   Solution: Implement automated security protocols for

rapid response to potential security breaches or vulnerabilities. This will help to ensure that security incidents are handled quickly and effectively.

6) **Problem:** The architecture is not scalable, which could make it difficult to add new features or users without compromising security.
   Solution: Design an architecture that allows for seamless scalability while maintaining security standards. This will ensure that the system can grow and adapt to meet the needs of the organization without sacrificing security.

These are just some of the technical aspects that need to be considered when designing a secure system. The specific solutions that are implemented will vary depending on the specific needs of the organization. However, the principles outlined above should provide a good starting point for any security implementation.

In addition to the technical aspects, it is also important to consider the human element of security. Employees need to be trained on security best practices and how to identify and report suspicious activity. They also need to be held accountable for their actions, both in terms of following security procedures and reporting security incidents. By taking a holistic approach to security, organizations can significantly reduce their risk of data breaches and other security incidents

In conclusion, the methodology outlined above ensures a rigorous and holistic approach to exploring secure cloud network architecture for multi-tier applications. By combining quantitative and qualitative methods and adhering to ethical considerations, this research strives to uncover valuable insights that enhance the understanding of secure cloud architecture in a multi-tier context.

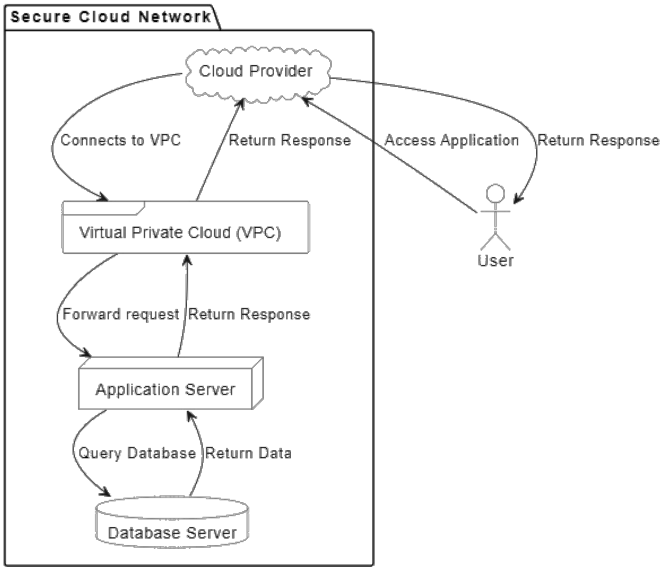

Fig. 2. UML Diagram of Request Sending for Cloud Service

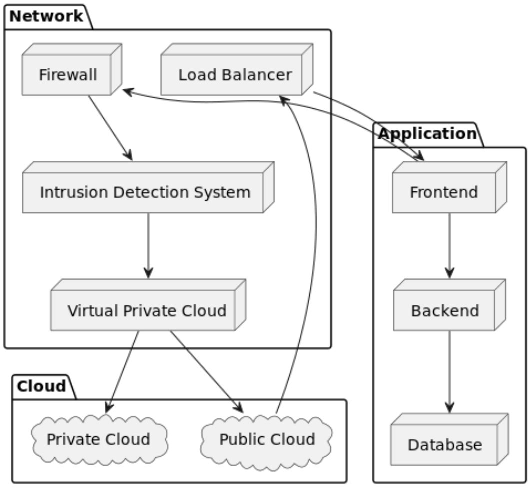

Fig. 3. UML Diagram of Web Hosting

IV. Security Challenges and Approach

By implementing a secure cloud network architecture for multi-tier applications, we aim to provide a robust and scalable solution that ensures the security of data and the reliability of applications in the cloud environment. This project addresses critical security challenges while providing opportunities for enhanced scalability and efficiency. However, in the context of virtualization, it is quite tough to maintain security, privacy, and data scalability. We tried to find the security challenges that might occur during the implementation and approaches to mitigate those vulnerabilities in Cloud environments.

A. Problem Identification

1) Data Security: Cloud environments are susceptible to security breaches, data leaks, and unauthorized access due to the inherent nature of remote storage and processing. The challenges include securing data both in transit and at rest.
2) Network Vulnerabilities: Multi-tier applications require intricate network configurations, which can lead to potential vulnerabilities and inefficiencies. Ensuring the network's robustness is crucial to prevent unauthorized access and data breaches.
3) Lack of Standardization: Many organizations struggle with inconsistent security practices and a lack of standardized approaches to cloud security. This lack of standardization can result in security gaps and vulnerabilities.
4) Data Loss: Inadequate data backup and recovery strategies can lead to potential data loss. This poses a significant risk to businesses, as data is a valuable asset.
5) Scalability Challenges: Scaling applications in the cloud while maintaining security and performance is a complex task. Rapidly changing infrastructure can introduce vulnerabilities if not managed effectively.

B. Proposed Solutions and Opportunities

1) Advanced Encryption: Implementing advanced encryption techniques is essential for safeguarding data. Employ end-to-end encryption, which ensures that data remains protected not only during transmission but also when stored in the cloud.
2) Identity and Access Management (IAM): Establish a comprehensive IAM strategy that includes user authentication, authorization, and access control. Implement role-based access control (RBAC) to define who has access to what resources and under what circumstances. Employ multi-factor authentication (MFA) to enhance user identity verification.
3) Network Segmentation: Implement network segmentation by dividing your cloud infrastructure into distinct segments or virtual networks. This approach isolates different application tiers, such as web servers, application servers, and databases, reducing the attack surface. Use security groups and access control lists (ACLs) to enforce segmentation rules.
4) Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS solutions to continuously monitor network traffic and system activities. These systems employ anomaly detection and signature-based methods to identify potential threats. In the event of a detected intrusion or suspicious activity, the IDPS can automatically respond by blocking or alerting administrators.
5) Automation: Leverage automation for security tasks. Implement automated incident response processes that can swiftly address security incidents. For example, automatically isolate compromised resources, initiate incident response playbooks, and update security policies in real time. Automation can also help with security patch management and vulnerability assessments.
6) Scalability Architecture: Design a scalable cloud architecture that ensures security isn't compromised when resources scale up or down. Use load balancers and auto-scaling groups to distribute traffic and resources efficiently while maintaining security controls. Employ containerization and serverless computing to facilitate dynamic scaling without compromising security.
7) Regular Auditing and Compliance Checks: Conduct regular security audits and compliance assessments of your cloud environment. Use tools and services to continuously scan for vulnerabilities and compliance violations. Schedule periodic penetration testing to identify weaknesses in your security posture and address them promptly.
8) Employee Training and Awareness: Invest in comprehensive training programs to educate employees about cloud security best practices. Cover topics such as secure password management, phishing awareness, and social engineering prevention. Create a culture of security awareness within the organization to reduce the risk of insider threats.

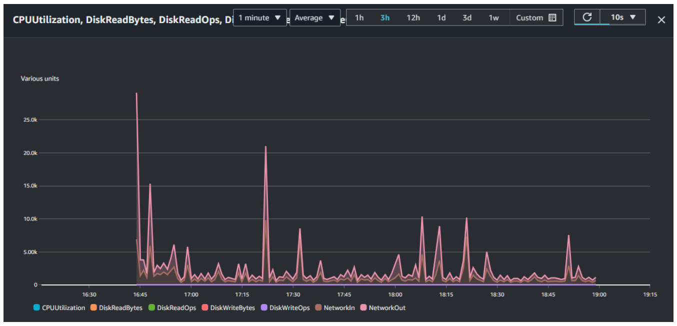

Fig. 4. CloudWatch Amazon EC2 Instance Monitoring

9) Incident Response Plan: Develop a well-documented incident response plan that includes predefined procedures, roles, and responsibilities. Ensure that the plan covers detection, analysis, containment, eradication, and recovery phases. Conduct tabletop exercises and drills to test the effectiveness of the plan and identify areas for improvement.

In conclusion, addressing security challenges in cloud environments requires a multi-faceted approach, combining advanced technologies, robust policies, and a proactive security posture. By implementing these solutions and continuously adapting to evolving threats, organizations can enhance their cloud security and protect their sensitive data and resources.

V. Analysis and Discussion

Amazon CloudWatch is a comprehensive monitoring and observability service provided by Amazon Web Services (AWS). It is developed to help user collect and track metrics, collect and monitor log files, and set alarms. CloudWatch provides valuable insights into user AWS resources, applications, and services, allowing user to troubleshoot issues, optimise performance, and ensure the overall health of AWS environment. Table 1 shows metrics that come from Amazon EC2 Instances.

TABLE I
CloudWatch Monitoring Data (Amazon EC2 Instance)

Label	CPU Utilization	Network In	Network Out
9/5/2023 16:45	0.066666667	2406.20	2892.00
9/5/2023 17:00	0.083625081	698.00	524.00
9/5/2023 17:15	0.083342595	838.80	633.60
9/5/2023 17:30	0.150583974	1961.80	817.40
9/5/2023 17:45	0.083351857	888.40	736.40
9/5/2023 18:00	0.083342595	967.20	1396.00
9/5/2023 18:15	0.083625081	629.20	479.40
9/5/2023 18:30	0.066411518	559.20	469.60

In table 2 to 5 we compare cloud hosting costs of 3 different cloud hosting providers. The data were collected from websites on September 5, 2023. There cost only based on the space given by the company. Most of the cases that companies we analyze for the project do not mention the processor configuration. Two companies did not mention the hourly cost in their website and only one company mentioned the hourly cost.

TABLE II
CONFIGURATIONS OF INSTANCES OFFERED BY ALPHA NET, BANGLADESH (CLOUD HOSTING)

Memory	vCPUs	Transfer	Storage	$/MO
1 GiB	1	300 GiB	30 GB	16.95
2 GiB	2	450 GiB	50 GB	27.95
4 GiB	2	750 GiB	75 GB	35.95
8 GiB	4	1 TB	150 GB	56.95

Source:https://alpha.net.bd/Cloud/Hosting/

TABLE III
CONFIGURATIONS OF INSTANCES OFFERED BY DIGITALOCEAN (CLOUD HOSTING)

Memory	vCPUs	Transfer	Storage	$/HR	$/MO
1 GiB	1	1000 GiB	25 GiB	0.00893	6.00
2 GiB	1	2000 GiB	50 GiB	0.01786	12.00
2 GiB	2	3000 GiB	60 GiB	0.02679	18.00
4 GiB	2	4000 GiB	80 GiB	0.03571	24.00

Source:https://www.digitalocean.com/pricing/droplets

TABLE IV
CONFIGURATIONS OF INSTANCES OFFERED BY LINODE AKAMI (CLOUD HOSTING - SHARED)

Memory	vCPUs	Transfer	Storage	$/MO
1 GB	1	1 TB	25 GB	5.00
2 GB	1	2 TB	50 GB	12.00
4 GB	2	4 TB	80 GB	24.00
8 GB	4	5 TB	160 GB	48.00

Source:https://www.linode.com/pricing/

TABLE V
CONFIGURATIONS OF INSTANCES OFFERED BY LINODE AKAMI (CLOUD HOSTING - DEDICATED)

Memory	vCPUs	Transfer	Storage	$/MO
4 GB	2	4 TB	80 GB	36.00
8 GB	4	5 TB	160 GB	72.00
16 GB	8	6 TB	320 GB	144.00
32 GB	16	7 TB	640 GB	288.00

Source:https://www.linode.com/pricing/

In table 6 to 8 we mentioned our proposed budgets for cloud computing with proper security, step by step implementation and proper support. For the country perspective we suggest budget friendly packages with proper security among the other companies. Think about the users, we also implement pay as you go service and as per user requirement we also provide service whatever users want.

TABLE VI
CONFIGURATIONS OF PACKAGE 1 (OPERATING SYSTEM IMAGE: AMAZON AWS)

Package Type	Memory	vCPUs	Storage	$/HR	$/MO
Basic 1	1	1	30 GB	0.0137	10.00
Basic 2	2	1	30 GB	0.0260	19.00
Standard 1	4	2	50 GB	0.0384	28.00
Standard 2	8	2	50 GB	0.0726	53.00
Standard 3	16	2	50 GB	0.1055	77.00
Advanced 1	16	4	100 GB	0.1438	105.00
Advanced 2	32	4	100 GB	0.2123	155.00
Advanced 3	64	4	100 GB	0.3435	250.00

*With Proper Security Configuration

TABLE VII
CONFIGURATIONS OF PACKAGE 2 (OPERATING SYSTEM IMAGE: UBUNTU)

Package Type	Memory	vCPUs	Storage	$/HR	$/MO
Basic 1	1	1	30 GB	0.0083	6.00
Basic 2	2	1	30 GB	0.0213	9.00
Standard 1	4	2	50 GB	0.0315	23.00
Standard 2	8	2	50 GB	0.0548	40.00
Standard 3	16	2	50 GB	0.0740	54.00
Advanced 1	16	4	100 GB	0.1096	80.00
Advanced 2	32	4	100 GB	0.1510	110.00
Advanced 3	64	4	100 GB	0.2192	160.00

*With Proper Security Configuration

TABLE VIII
CONFIGURATIONS OF PACKAGE 3 (OPERATING SYSTEM IMAGE: WINDOWS)

Package Type	Memory	vCPUs	Storage	$/HR	$/MO
Basic 1	1	1	30 GB	0.0206	15.00
Basic 2	2	1	30 GB	0.0342	25.00
Standard 1	4	2	50 GB	0.0548	40.00
Standard 2	8	2	50 GB	0.1230	90.00
Standard 3	16	2	50 GB	0.2260	165.00
Advanced 1	16	4	100 GB	0.2603	190.00
Advanced 2	32	4	100 GB	0.4521	330.00
Advanced 3	64	4	100 GB	0.6650	485.00

*With Proper Security Configuration

VI. Future Work

While our initial phase involves manual resource allocation in AWS, our vision for the future entails a transition to automated resource allocation, ensuring that cloud services dynamically adapt to customer demands. This transition promises enhanced efficiency and effectiveness in cloud service consumption. We also intend to test our system with different objectives such as availability and/or latency. We recognize the importance of exploring other cloud service providers for future scope. Our intention is to conduct a comprehensive evaluation and comparison of various cloud service providers, including but not limited to AWS, to make our approach more cost-efficient, flexible, and strategically aligned with the evolving cloud landscape. This comparative analysis will entail a thorough examination of factors such as pricing structures, performance metrics, service-level agreements (SLAs), geographic availability, and the compatibility of each provider's offerings with our architecture. By doing so, we aim to identify the cloud provider that not only offers competitive pricing but also aligns seamlessly with our scalability and security requirements.

In addition, as part of our ongoing research and development efforts, we will continuously monitor the cloud service landscape for emerging providers and innovative solutions. This proactive approach will enable us to stay at the forefront of cloud technology, allowing us to harness the most suitable services and platforms to meet the evolving needs of our small business customers. As the cloud technology landscape continues to evolve, our architecture is poised to play a vital role in shaping the future of cloud-based interactions, safeguarding sensitive data, and optimizing the utilization of cloud resources.

VII. Conclusion

This paper has explored the transformative impact of cloud computing on modern businesses and the challenges they face in ensuring the security and efficient management of complex cloud network architectures, particularly for multi-tier applications. The advent of cloud technology has ushered in an era of scalability, flexibility, and cost-effectiveness, but it has also raised concerns about data security and resource allocation. Our innovative approach introduces a pivotal intermediary that bridges the gap between cloud providers and consumers, with a specific focus on small businesses. This intermediary not only orchestrates the allocation of cloud resources but also establishes a comprehensive security framework. This framework is adaptable to the evolving cloud landscape, guaranteeing the confidentiality, integrity, and availability of data.

In summary, our work represents a significant step forward in the quest for secure and efficient cloud service provisioning for small businesses. It addresses the pressing need for a reliable mediator in the cloud ecosystem, one that balances resource allocation with data protection.

References

[1] A. Abbas, "Cloud Access Security Brokers (CASBs): Enhancing Cloud Security Posture," 2023.

[2] P. Pawluk, B. Simmons, M. Smit, M. Litoiu, and S. Mankovski, "Introducing STRATOS: A Cloud Broker Service," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 891-898.

[3] A. Abbas and K. Khan, "Addressing Cloud Provider Security: Evaluating and Selecting Secure Cloud Services," 2023.

[4] U. Khan, "Towards Secure Cloud Bursting, Brokerage and Aggregation," in Proceedings of the Eighth IEEE European Conference on Web Services, 2010, pp. 189-196.

[5] E. Pinho, L. B. Silva, and C. Costa, "A Cloud Service Integration Platform for Web Applications," presented at the International Conference on High-Performance Computing and Simulation (HPCS), Bologna, Italy, 2014.

[6] A.A. Ibrahim "Cloud Computing Security Issues and Challenges in Bangladesh", 2019. https://dspace.daffodilvarsity.edu.bd:8080/handle/123456789/4955

[7] D. Saxena, R. Gupta, and A. Singh, "A Survey and Comparative Study on Multi-Cloud Architectures: Emerging Issues and Challenges for Cloud Federation," 2021 [Online]. Available: https://arxiv.org/pdf/2108.12831.pdf

[8] K. Pranay Raj and U. R. Mogili, "CLOUD-OF-CLOUD: A Novel Protocol for Secure Data Storage and Sharing in Multi-Cloud Environment," Journal of Interdisciplinary Cycle Research, vol. XII, no. VI, pp. 2201-2209, June 2022.

[9] Darshan Tank, Akshai Aggarwal, Nirbhay Kumar Chaubey, "Virtualization vulnerabilities, security issues, and solutions: A Critical Study and Comparison", 2019. DOI: 10.1007/s41870-019-00294-x

[10] Chuanyi Liu1, Guofeng Wang, Peiyi Han, Hezhong Pan, Binxing Fang, "A Cloud Access Security Broker Based Approach for Encrypted Data Search and Sharing" January, 2017.

[11] Fatemeh Khoda Parast, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, and Saqib Hakak, "Cloud Computing Security: A Survey of Service-based Models" in Computers and Security, December, 2021. doi: 10.1016/j.cose.2021.102580