Security and SLA Monitoring for Cloud Services

Elias Seid, Mosammath Nazifa, Sneha Gupta, Oliver Popov and Fredrik Blix
Department of Computer and Systems Sciences, Stockholm University, Sweden

Keywords: Cloud Database Services, Cybersecurity, IT-Incidents, Availability, Monitoring, SLAs.

Abstract: The present demand for cloud computing is driven by its scalability and adaptability, making it widely employed in enterprises. A Service Level Agreement (SLA) is a contractual arrangement between cloud providers and clients that ensures the stated level of services will be available. In order to evaluate the compliance of the services to the SLA, it is critical to monitor the availability of the cloud services. Cloud service companies offer several monitoring tools. However, such assessments are often influenced by bias, which prompts demands for impartial assessment of service level agreements (SLAs). The objective of this study is to address the issue of monitoring service availability characteristics, specifically uptime and downtime, in relation to SLA. To achieve this, a monitoring tool called SLA Analyser is proposed. The solution comprises a centralised application that generates and collects data in the primary registry database, along with a compliance report generator that computes cloud service availability using previously gathered data and compares it to the SLA availability parameter. An illustrative report is generated based on the gathered and processed data. This study specifically addresses the reliable assessment of SLA for both clients and service providers. Moreover, this study analyses the challenges associated with SLA monitoring and the repercussions of neglecting its assessment. This approach is particularly essential to organisations that use many cloud services from various vendors. The SLA Analyser was employed to monitor the availability of the cloud database services. In order to mitigate financial losses and uphold a positive reputation for consumer confidence, it is essential to validate the SLA.

1 INTRODUCTION

In recent years, Cloud Service has become a popular topic in the Information and communication technologies (ICT) domain. The term ”cloud services” refers to a wide range of services delivered on demand basis over the internet by the vendors to companies and customers. Many companies and institutions are moving in various ways to leverage these services. These cloud services are designed to provide its customers, an easy, scalable, cost effective access to resources, without being involved in the maintenance of internal infrastructure or hardware.

Cloud computing vendors and service providers manage cloud services. They are accessible to customers through provider servers. Service owners and operators must monitor cloud infrastructure components for faults, usage, and uninterrupted business operations. Data analysis in cloud-based service infrastructure relies on logs from system components. Logs can be used to assess the availability of cloud-hosted service infrastructures. Information on component availability aids organisations in making risk-based decisions about cloud vendors and components.

A cloud service level agreement (SLA) guarantees cloud providers meet enterprise-level requirements and deliver defined deliverables to customers. Quality of Service (QoS) may be measured in SLAs between vendors and organisations (customers). The SLA covers cloud infrastructure availability, defining the expected uptime and accessibility at the service provider and end-user level. The vendor must specify penalties, typically financial, for non-compliance with agreed-upon service levels (Hubballi et al., 2019).

The present state of affairs is characterised by SLA documents that are complex and open to multiple interpretations. It may provide specific and limited definitions for terms such as availability and security. Furthermore, service agreements often place distinct obligations on consumers to monitor modifications in service. The purpose of the study conducted by Badger et al. (2012) was to establish criteria for assessing agreements and deciding when to reassess service agreements. According to (Barros et al.,2015) when there is increased involvement of external service vendors, the customer’s control over the quality

Seid, E., Nazifa, M., Gupta, S., Popov, O. and Blix, F.
Security and SLA Monitoring for Cloud Services.
DOI: 10.5220/0012690800003687

In *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2024)*, pages 537-546
ISBN: 978-989-758-696-5; ISSN: 2184-4895

of service delivery decreases. Consequently, the customer must depend on the quality assurances established in accordance with the Service Level Agreements (SLAs).

Cloud computing providers delegate service violation provision to consumers, which is a major drawback (Barros et al.,2015). Cloud consumers struggle to identify SLA breaches due to their subjective and complex nature. Customers often learn about cloud application downtime through user complaints about accessibility. User complaints about service unavailability negatively impact the customer's business. Many cloud providers offer monitoring tools that allow clients to evaluate the availability of their services. However, these solutions are customised to specific providers and cannot be modified to accommodate customer requirements. Furthermore, the monitoring tools are customised to each provider, which means that the same platform cannot be used for numerous cloud providers.

There is a wide range of cloud monitoring tools accessible on the market. Cloud monitoring solutions facilitate the management and surveillance of cloud infrastructure, services, and applications.A plethora of cloud monitoring technologies are readily available in the market. Cloud monitoring solutions enable the oversight and control of cloud infrastructure, services, and applications. Several cloud monitoring systems are accessible, such Monitis, RevealCloud, and LogicMonitor (Al-hamazani et al., 2014; Ku c, 2023). However, (Dana et al. (2014) state that there is presently a deficiency in SLA-based cloud security monitoring services and solutions.

Service providers often utilise monitoring technologies to assess service characteristics and SLAs, although this can potentially induce bias. An impartial review is essential to guarantee compliance. Currently, consumers depend on suppliers' statistical statistics to authenticate SLA compliance. Therefore, it is crucial for SLA monitoring to be both dependable and impartial. This study presents a solution to the problem by presenting the SLA Analyser tool, which is designed to monitor the availability of cloud database services. Furthermore, users of cloud services use the cloud to host their applications, services, and other resources. Customers rely on the prompt availability of cloud services. Failure to do so could result in damage to their market reputation and business. It is crucial to monitor the availability of cloud services for both customers and suppliers and validate SLAs.

To verify service parameters against SLAs, SLAs must be simple, quantified, and easily understood (Frey et al., 2013). Studying SLA tracking is challenging due to its time-consuming nature and the need to validate quality metrics against agreed cloud service SLAs. This is especially challenging for organisations using multiple cloud services from various vendors. Thus, the research problem is broad, important, and difficult. Monitoring cloud service availability is essential in the ITC domain, despite its commonality. SLA Analyser enables cloud providers and customers to independently monitor service availability against SLA documents.

This research aims to monitor the availability of public cloud infrastructure components' SLA using a proposed tool. The proposed tool, SLA Analyzer, monitors cloud service availability. The tool consists of a core application that generates and collects data in the main registry database, and a compliance report generator that calculates cloud service availability based on previously collected data and compares it to the SLA availability parameter. A graphical report is created from collected and analysed data.

A service's downtime is when it's unavailable, while its uptime is when it's available for use. The SLA Analyzer provides cloud service downtime and uptime data. The data will be used for statistical analysis to determine the net availability of the cloud service. Downtime or uptime ratio determines availability (Oliveto et al., 1999). Calculated availability is compared to agreed-upon parameters in SLA documents between cloud service providers and customers. The study will present a tool known as SLA Analyzer that will autonomously analyse the parameters of cloud service availability. The objective of this study is to quantify the availability of SLA for cloud services specifically related to databases. The SLA Analyser tool uses data to assess and compute the availability of database services. The study aims to address the following research question (RQ)

- RQ1:How can SLA Analyzer be used to independently monitor the availability of cloud-based database-as-a-service (DBaaS) deployments?

The remaining parts of this paper are structured as follows. Section 2 provides the theoretical basis for our research, whereas Section 3 describes the approach and methods used in our study. Section 4 of the paper presents the SLA Analyser Architecture, while the fifth section focuses on the Experiment and result. Section 6 has discussions. Section 7 provides a conclusion, and also discusses potential areas for future research.

2 RESEARCH BASELINE

As managed services and cloud computing become more common, SLAs adapt to accommodate new methodologies. SLAs are used to negotiate computation and performance requirements between service providers and users. A service-level agreement should include an overview, service description, exclusions, performance, compensation, stakeholders, security, risk management, disaster recovery, tracking, reporting, review and change processes, termination, and signatures. In order to enforce a service-level agreement, it is crucial to comprehend the provider's delivery criteria. If the SLA is not satisfied, the client may be entitled to the contract compensation. SLAs monitor service provider performance using specific metrics and parameters. Parameters include availability, uptime, performance, data, security, privacy, hardware, and software requirements.

2.1 Cloud Service Availability

The availability and uptime characteristics measure the duration of services available to customers. In cloud services, uptime and availability are crucial characteristics. The availability of an application depends on the functionality of the underlying infrastructure. If there is a problem with the infrastructure, the application may cease to be available. Lack of accessibility and availability prevents the usage of digital applications. Key factors depend on the cloud service type: SaaS (Software as a service), IaaS (Infrastructure as a Service), or PaaS (Platform as a Service). The study 'Cloud security service level agreement: Representation and Measurement' conducted in 2019 found that there is a lack of standardised systems for defining and enforcing security SLAs in cloud computing (Hubballi et al., 2019).

Cloud service providers (CSPs) are required to offer assurances regarding the security and computational processes employed for essential applications. Customers usually engage in negotiations to establish SLA in order to enforce these responsibilities. Cloud computing platforms currently employ various tools or procedures provided by service providers to measure and enforce performance-related SLAs. Nevertheless, these SLAs generally fail to encompass security-related concerns and obstacles (Hubballi et al., 2019).

CSPs use security and openness standards such as the Cloud Control Matrix (CCM) developed by the Cloud Security Alliance and the NIST's SP 800-53. Security problems in cloud computing encompass the availability of the service, privacy of data, transparency, billing, and prevention of cyberattacks. Securing cloud services to encompass all areas of security is tough due to the heterogeneous composition of the cloud, consisting of many types of computer systems (Hubballi et al., 2019).

SLAs are commonly used to form and manage QoS agreements between clients and service providers. Kaaniche et al. (2017) found few SLA management systems that consider cloud security contexts. Kaaniche et al. (2017) found that operational performance management is often more sophisticated than security management in many systems. SLAs should clearly outline security duties such as confidentiality, integrity, and availability (CIA). Additionally, the study suggests considering the dynamic nature of cloud systems when creating security SLAs for monitoring. The study showed providers' difficulties providing reliable services. Current SLAs lack security management and tools for unbiased service comparisons. According to the article, there are no real-time tools to adequately characterise and manage security SLAs.(Kaaniche et al., 2017)

2.2 Cloud Security

A study on cloud security SLA adoption(Casola et al., 2015) found that cloud service providers (CSPs) typically provide opaque security. This implies that security methods are weak and inflexible to negotiation. This implies limited security feature options for clients. However, security should be considered with other crucial criteria when selecting a cloud service. The European Community has initiated work to standardise SLAs for cloud computing (Casola et al., 2015), and subgroups are addressing security challenges, however security is currently outdated.

(Toeroe and Tam et al., 2012) define availability as the percentage of time an application and its services are available within a certain timeframe. High availability (HA) is achieved when the service is unavailable for less than 5.25 minutes per year, guaranteeing at least 99.999 % availability. Achieving higher availability is a major challenge for cloud providers. A cloud provider should continuously monitor resources and deployed services to achieve high availability (Endo et al., 2016).

Availability is a key security component of CIA (Confidentiality, Integrity, Availability), ensuring system availability at agreed-upon times for designated individuals (Januzaj et al., 2015). We aim to monitor DBaaS availability in this study. Our unbiased tool verifies if agreed-upon Database cloud service availability is satisfied by several providers and alerts of SLA violations throughout the service lifecycle.

3 SLA ANALYSER

The Service Level Agreement Analyser, often known as the SLA Analyser, is a tool used for monitoring the availability of a service. This tool consists of two components: the Core Application and the Compliance Report Generator. The Core application periodically checks for the presence of a target database service and records the outcome in the main registry database. The primary registry database is located on the Core Aapplication. The Core Application establishes a connection with a specified database cloud provider and periodically verifies its availability. The Core application records the availability status of the target database service in its main registry database.

The Compliance Report Generator serves as the second module of the SLA Analyser tool. The Compliance Report Generator(CRG) assesses the accessibility of the target database cloud service by examining the data gathered in the primary registry database of the Core Application. CRG calculates the availability of the target database cloud service by using the uptime and downtime formula(as it can be seen sub section 5.1) within a defined time period. CRG afterwards compares the calculated availability with the availability parameter stated in the agreed Service Level Agreement (SLA) of the target database cloud service. An analytical assessment is presented in the form of a visual report. The compliance report features a graph where the x-axis denotes time and the y-axis represents availability. The SLA Analyser tool can check the accessibility of different database services, irrespective of the cloud service provider.

This study seeks to employ the SLA Analyzer to autonomously monitor the availability parameter of the SLA for cloud-based database-as-a-service. The research aim is accomplished by employing the use of an experiment-based research strategy. The SLA Analyser tool is used to monitor two target database cloud services during the experiment. Upon completion of the experiment, a report on SLA compliance is generated. This report can be used to identify any instances where the availability requirements outlined in the SLA documents for the target database cloud services have been violated.

3.1 Experimental Architecture

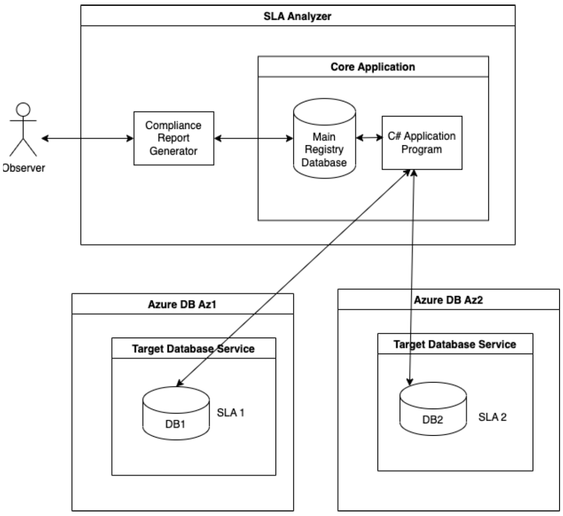

Figure 1: Architecture of SLA Analyser.

The experimental setup of the study is illustrated in Figure 1 (SLA Analyser Architecture). The architecture of the SLA analyser is described as follows. The core application comprises a C# application program and main registry database. The study uses a C# application program to develop an application that establishes a connection to a certain database cloud service by employing a database connection string. The connection string comprises essential parameters for establishing a connection between the applications and a database server. The configuration encompasses the server instance, database name, authentication details, and additional parameters required for communication with the database server.

After establishing the connection, the C# Application Programme verifies the availability of the target database cloud service. This check is conducted periodically at a predetermined frequency. The frequency at which the availability of the cloud service is monitored can be adjusted based on the specific monitoring needs. The C# Application Programme records the availability status of the target database service and writes it into the Main Registry Database. The Main Registry Database contains tables that store information pertaining to the cloud service entities that are being monitored. The database table's column names consist of the availability status (Status), timestamp (Timestamp), and specifics of the assessed cloud database (Slave identity country zone).

The Compliance Report Generator uses the data from the main registration database of the Core Application to determine the availability of the target database cloud service. The accessibility of the target database cloud service can be determined by calculating its uptime and downtime using a certain formula during a given time period. The computed availability is afterwards compared to the availability parameter specified in the agreed SLA of the target database cloud service. An analysis is conducted and a graphical report is produced as a result.

The target database service refers to the cloud database that is being monitored by the SLA Analyser tool. Two target Database Services were hosted on Azure for this experiment, each located in separate availability zones. Availability zones (AZs) are segregated data centres situated in distinct geographical regions where servers for public cloud services are established and managed. The knowledge of the availability zone of a cloud service is crucial, as SLA for cloud services differs depending on the availability zones in which the cloud services are hosted by the providers. The target Database services were supplied with a predetermined test data-load. The fixed data-load is read during the read operation performed by the C# Application Programme. Ensuring consistency throughout the read process is achieved by reading the same data load.

3.2 Experimental Scenarios

The SLA Analyser tool was specifically created to undergo testing with predetermined scenarios. These scenarios guarantee that the SLA Analyser fulfils its objective in accordance with the scope of this study. Below are four vital scenarios for SLA Analyser:
Scenario 1: SLA Analyser tool shall monitor the available database cloud service: Database cloud services will be monitored using SLA Analyser. To meet SLA requirements, the analyzer must connect to the database cloud services and successfully read fixed data stored there. For each successful read operation, the target database service stores a 'available' item in the main registry database as shown in Figure 1.
Scenario 2: SLA Analyser tool shall monitor the unavailable database cloud service: Requires SLA Analyser to detect unavailable database cloud services. SLA Analyser should track difficulty to connect or read fixed data stored on cloud services. To test the unavailable database scenario, we had to disable the database server, resulting in a loss of connectivity. Every failed connection to the target database service results in a 'unavailable' entry in the main registry database.
Scenario 3: SLA Analyser tool shall monitor more than one database cloud services: The SLA Analyser tool should connect to many cloud database services. Database cloud services can be hosted by many providers or in different availability zones.
Scenario 4: SLA Analyser tool shall generate SLA compliance reports for database cloud services: The Compliance Report Generator of SLA Analyser should use the dataset from the Core Application's main registration database to build availability plots. This figure demonstrates SLA compliance for cloud database services. In addition to functional criteria, the following availability analysis rules were used to determine the database cloud service availability status:

Rule 1: If the Core Application properly connects to and reads from the database service, the service can be marked accessible (Rule1). **Rule 2**: If the Core Application can successfully connect to the database service but fails to conduct a successful read operation, the database service can be deemed unavailable. **Rule 3**: In the event that the Core Application fails to establish a successful connection to the database service, the database service may be designated as unavailable. These rules were generated from standards for assessing cloud service availability. According to FISMA (Barker et al.,2003), 'availability' in cyber security refers to timely and dependable access and use of information or services by users. Accessing services does not guarantee availability. Rule 2 and Rule 3 were deemed inaccessible based on this understanding. A successful connection and read operation of the database cloud service by the tool resulted in the status available state in Rule 1.

4 EXPERIMENT AND RESULT

The SLA Analyser tool is used to monitor the availability parameter of SLA for cloud-based database-as-a-service during the study project. The SLA Analyser tool assesses the availability of cloud services by performing periodic read operations. The evaluation of database cloud services involves conducting a read operation. The evaluated database cloud services were furnished with a test data-load, which was read during the read operation performed by the SLA Analyser tool. The main registry database of the SLA Analyser tool was updated based on the findings of the read operation. The primary registry database is populated with entries in its table that store information pertaining to the monitored cloud service entity. The measured parameters consist of the availability status (Status), timestamp (Timestamp), and specifics of the assessed cloud database (Slave identity country zone), as depicted in Figure 2 of the Main Registry database table.

The Slave identity country zone records the name and availability zone of the cloud services that are currently underutilised. The availability status values obtained were categorised as either 'available' or 'unavailable'. The time at which this data was recorded was kept as a timestamp in the format of YYYY-MM-DD hh:mm:ss[.fractional seconds]. The availability was evaluated every five minutes for this study. The frequency was fixed throughout the experiment but adjustable. Users can vary cloud service availability monitoring frequency based on their needs and business justification. Mission-critical cloud customers can monitor service availability per second or minute, depending on their needs.

The availability score measures the proportion of 24-hour service availability. Each daily cycle adds several rows to the main register database based on monitoring frequency. If the frequency is 5 minutes, 288 rows will be generated. Daily availability was calculated using uptime and downtime. Uptime is when a service is available, while downtime is when it is not. The database cloud service's SLA availability metrics were then compared to each day's availability. Table 1 shows Azure DB Az1 data: The proposed tool collected data. The first column shows monitoring dates, while the second shows database cloud service availability requirements, which were 96.5%. The third column shows SLA Analyser-determined daily availability. Figure 5 shows a graph of the SLA compliance report based on the data table.

Table 1: Collected data through proposed tool.

Azure DB Az1		
Resources	**SLA**	**Compliance status**
May 10th	96.5000	97.14286
May 11th	96.5000	97.14286
May 12th	96.5000	94.89051
May 13th	96.5000	97.14286
May 14th	96.5000	97.14286
May 15th	96.5000	95.65217
May 16th	96.5000	97.11191
May 17th	96.5000	96.89922
May 18th	96.5000	94.89051
May 19th	96.5000	97.87234
May 20th	96.5000	97.14286

4.1 Data Analysis

Following the 11-day data collection period, which had a time difference of 5 minutes, the collected data was analysed using a one-sample proportion statistical test (z-test) in comparison to the SLA. The evaluation determines whether the uptime of the cloud database (DB) services in the sample meets or exceeds the agreed-upon availability percentage of the SLA. The test yields valuable information indicating that the tool's output is statistically significant within the given dataset. Through statistical analysis, the comparison between the uptime-downtime and agreed-upon availability percentages from the tool is reevaluated and confirmed.

Initially, data was imported into R-studio from a CSV file. Afterwards, the availability status has been transformed from ”available” to ”unavailable” using a binary conversion of 1 and 0 on the dataset. The steps for conducting a one-sample proportion test are as follows: Firstly, compute the sample percentage $(\hat{p})$ by counting the number of successes in the availability column and dividing it by the total number of observations. In step ii, the null hypothesis (H0) and alternative hypothesis (H1) are defined. The null hypothesis states that the availability percentage from the SLA is less than the agreed upon value, while the alternative hypothesis states that it is equal to or greater than the agreed upon value. In step iii, the standard error (SE) is computed for the sample proportion using the given equation.

$$SE = sqrt((\hat{p}) * (1 - (\hat{p}))/n)$$

Here, n represents the sample size and $(\hat{p})$ represents the sample proportion. The test statistics (z score) value is obtained using the following equation:

$$Z = ((\hat{p}) - p_o)/SE)$$

Out of a span of 11 days, 2 days were chosen at random for the analysis. The data from May 10th has been selected and employed in the test. The result indicates that the null hypothesis cannot be accepted and the sample proportion is much higher than the agreed-upon availability percentage of 0.965. The current service availability exceeds 96.5% as of May 10th, and the SLA has not been violated. The statistical test conducted on May 10th, as depicted in Figure 3, presents the outcomes of a one-sample proportion test. The one-sample proportion statistical test was also conducted using the data from May 12, 2023. The outcome indicates that the null hypothesis has not been rejected and the sample proportion is not higher than 0.965 (the agreed-upon percentage of availability). The service was unavailable for 96.5% of the day on May 12th. The availability has not met the promised level and the SLA has been violated. The use of a one-sample proportion statistical test confirms the statistical significance of the data gathered by the SLA Analyser tool.

4.2 Findings: Addressing Our Research Question

This study monitored database cloud service SLA availability using SLA Analyser. The SLA Analyser connected to the target database cloud services.

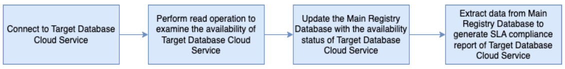
Connect to Target Database Cloud Service
Perform read operation to examine the availability of Target Database Cloud Service
Update the Main Registry Database with the availability status of Target Database Cloud Service
Extract data from Main Registry Database to generate SLA compliance report of Target Database Cloud Service

Figure 2: Workflow of SLA analyser.

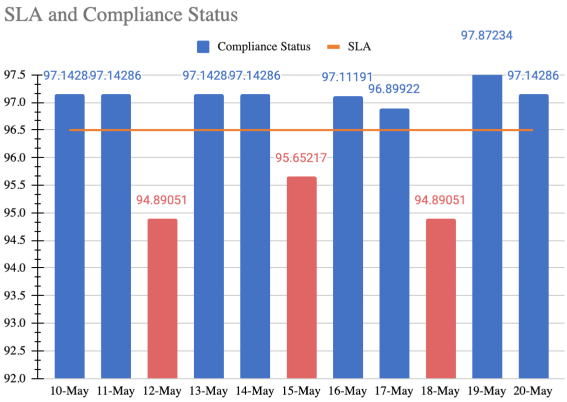

Figure 3: SLA Compliance Report.

After connecting, the SLA Analyser read the target database cloud services. SLA Analyser's primary registry database was updated with the target database cloud services' availability status after the read operation. SLA compliance reports use primary registration database data. The compliance report can detect occasions where target database cloud service SLA agreements have not satisfied availability standards. The SLA Analyser tool's operation is explained in Figure 4

As indicated, the tool was designed using availability analysis techniques. Database service availability was set to ”available.” if the database connection and read operation were successful. The database service was unavailable if the read operation failed after connecting to the database. The database service was unavailable if the database connection was not made. These criteria assessed target database cloud service availability. Based on 11-day availability calculations, a SLA compliance report graph was created. Monitoring dates are on the x-axis, and availability scores are on the y-axis. Customers and sellers' Service Level Agreement (SLA) was used to verify SLA compliance. The SLA Compliance Report for Azure DB Az1, the target database service, is shown in Figure 5.

The experiment had four main scenarios. The tool met and exceeded all test scenarios and quantified cloud-based database-as-a-service platform SLA availability parameters. Scenario 1 assessed the target database cloud services' availability by assessing the tool's ability to connect to and read from them. Scenario 2 assessed the target database cloud services' inaccessibility. Database services seldom become unavailable without external involvement. Perhaps they would descend once or twice a month. We purposely disabled the database server to test unavailability, creating a ”unavailable” record. The inability to connect to the database service caused the tool to throw an exception, reporting the service as down.

The SLA Analyser was tested by connecting to two Azure database services in different availability zones. Each database service monitored independently of experimental results. SLA Analyser monitors many cloud services. Scenario 4 was completed using the SLA Analyser primary registration database dataset. The data set was extracted using Excel to determine monitoring day availability using uptime and downtime. A plan was made based on daily availability. The plot used availability metrics from the approved (SLA) to analyse the database service's SLA compliance. Figure 5 shows the SLA Compliance Report.

5 DISCUSSION

The experiment and analysis provide the necessary data to solve this research challenge. The suggested SLA monitoring tool improves cloud service availability and SLA compliance. Companies that want to stay competitive and provide great customer service must prioritise service dependability and SLAs. This is critical given the shifting Cloud computing landscape and its impact on corporate processes. Recent research on SLA monitoring and cloud evaluation have stressed the importance of automated methods and real-time monitoring in this ever-changing environment.

The suggested tool monitors cloud-based database services using uptime and downtime. A tool was used to compare the 11-day service availability and unavailability record to the SLA availability percentage. The SLA Compliance Report shows that Azure DB failed to reach the guaranteed SLA % on May 12th, 15th, and 18th, 2023. Cloud service availability has dropped to 96.5% in recent days, which is below expectations. For the remaining days, the tool shows that services met the Service Level Agreement. The suggested tool monitored service availability against SLA. In table 2 and Figure 5, a one-sample % statistical test was used to reevaluate the indicated tool's data. Test results show statistical significance. By automatically assessing SLA, the SLA monitoring tool reduces human monitoring time and effort.

5.1 Novelty of the Proposed Tool

The results are thoroughly compared to existing research on the issue in this section. Undheim et al. (2011) did a key study on "Differentiated Availability in Cloud Computing SLAs." The study analysed cloud SLA availability and sought to simulate cloud data centres. Their analysis showed that SLAs should explicitly include key performance indicators (KPIs), but ours actively monitors those KPIs. This provides us track how well cloud service providers meet their availability promises. This helps us understand their performance and improve their SLA compliance.

In "Cloud Security Service Level Agreements: Representation and Measurement," Hubballi et al. (2019) defined SLAs and proposed a real-time audit method employing a trusted third-party auditor. We focus on monitoring the accessibility of standard service level agreements used by cloud providers and their clients, despite their success in generating and quantifying them. Our proposed tool ensures SLA compliance and uses an impartial and autonomous monitoring mechanism to avoid conflicts of interest. Independent service level agreement evaluations help build trust and transparency between cloud operators and clients. This provides constant and precise SLA compliance.

The 2013 Manuel et al. research, "Availability Management in Cloud Computing Based on the ISO/IEC 20000 Standard," addresses cloud computing availability management. They presented an ISO 20000-based framework for cloud service monitoring and management. The study advances availability management. Our system monitors cloud database-as-a-service availability. The proposed approach improves customer satisfaction by easily achieving industry standards and service level agreements to promote cloud service reliability.

Furthermore, Ameller et al. (2008) present "Service Level Agreement Monitoring Tool based on measures derived from ISO/IEC 9126-1-based service oriented quality model." Their research focuses on ISO 9126-1-compliant monitoring tools. Its main goal is to evaluate quality metrics. Only cloud-based database service accessibility and security protocols are monitored in the course of our study. This aids them by analysing quality measures. Our programme provides an all-encompassing approach for database performance evaluation and improvement. It emphasises availability, a key component of cloud architecture.

5.2 Related Work

Existing Tools. Regarding the available tools, cloud providers frequently provide monitoring tools like CloudMonitor, ServiceWatch, and SLA Tracker, which are proven to be useful in monitoring services within their particular ecosystems. These tools, provided by certain cloud providers, play a crucial role in guaranteeing service responsiveness and compliance with Service Level Agreements. Nevertheless, the proposed tool offers a chance for impartial and autonomous surveillance by guaranteeing the absence of any potential conflicts of interest or undue influence in the monitoring procedure. It is especially suitable for organisations with adaptable cloud environments due to its inherent flexibility and customisation capabilities. This solution provides flexibility, enabling businesses who utilise services from numerous cloud providers to monitor the availability of their entire cloud environment using a single integrated platform.

Conversely, the solutions offered by cloud suppliers are designed to be used only with a particular cloud provider. This thorough monitoring strategy improves a company's capacity to effectively manage its cloud infrastructure. To conclude, the suggested monitoring solution emphasises real-time monitoring of important performance indicators connected to cloud providers and clients' conventional service level agreements. This detailed monitoring approach provides businesses with valuable insights by actively monitoring SLAs and database-as-a-service availability. Our experiment helps companies understand how to deliver reliable cloud services that meet customer expectations. This technology can help cloud-using firms gain deeper insights into their cloud databases. Availability insights and SLA compliance data can help people choose the best cloud provider. Real-time monitoring helps organisations develop service level agreements faster.

Firms with sensitive data or regulatory compliance requirements benefit from the proposed tool's impartial and autonomous monitoring mechanism. Organisations can improve their competitiveness and meet legal and regulatory requirements by demonstrating SLA compliance through unbiased monitoring. In conclusion, the suggested SLA monitoring solution greatly improves cloud service availability monitoring. By monitoring availability and ensuring service level agreements, the app helps cloud service providers and organisations deliver high-quality cloud services. This research could improve cloud service reliability, customer satisfaction, and company success in a time when cloud computing is still changing business.

5.3 Threats to Validity

To confirm and ensure research accuracy and efficacy, multiple actions are taken. First, experiment-based testing was done to evaluate the SLA analyzer's correctness in gathering and creating database cloud service uptime and downtime statistics. The experiment tests whether the system can calculate and compare actual and SLA availability percentages. Determine if SLA was violated. Results were validated using statistical analysis. One-sample proportion test reevaluates data and verifies tool results are statistically relevant. The research also compares the suggested tool to market-available monitoring methods to evaluate its impact. This study offers impartial and objective monitoring, a versatile tool that can be adapted to the customer's business requirements, and the ability to monitor many cloud platforms with a single tool. Finally, a comprehensive literature review compared the new tool to past SLA monitoring research on cloud service accessibility. The review insightfully assesses the research's value. The proposed instrument's uniqueness is also emphasised. **Validity (internal and external):** The study has limitations. Student accounts initially purchased cloud services from cloud providers due to resource constraints. Purchase limits for student accounts vary by database size and choice. An interactive data visualisation tool like Power BI would have been best for SLA compliance reporting. It was not added into SLA Analyser because of the cost. Instead, Excel was used. Due to purchasing constraints, we chose Azure cloud services, which were free for students. All research was done on Azure. Execution is neutral and compatible with any cloud service. The suggested tool's proof-of-concept was conducted in a synthetic experimental environment. This was the best option for the task due to time restrictions. The ability to implement and repeat results may be limited in these scenarios.

6 CONCLUSION

This study evaluated using the SLA Analyzer tool to automatically monitor cloud-based database-as-a-service SLA availability. The research goal was attained by experimenting with scenarios. To ensure SLA compliance, the report emphasised autonomous cloud service monitoring. The results supported this study's goal and provided reliable SLA monitoring results. The SLA percentage did not always match service availability on some days, according to experiments. SLA breach was clear since promised services were not delivered.

Numerous enterprises and organisations are embracing client interest in cloud services, which the paper addresses. These entities are having trouble monitoring service availability. This effort was small-scale, hence its scientific impact was limited to monitoring cloud service availability. A tool that compares real service to stated SLA performed it. This study paved the way for further research on cloud computing SLA management that benefits customers and providers.

Future Work. A study on ”the Adoption of Security Service Level Agreements (SLAs) in the Cloud” found certain problems. Expressing security requirements accurately, measuring security, and monitoring and ensuring security are the primary challenges. These three reasons hinder cloud and security service level agreement adoption. The study focuses on monitoring and comparing security availability with the SLA availability %.

This study lays the framework for future research to improve the tool by adding parameters beyond availability to give a more comprehensive cloud service monitoring system. Consider studying secrecy and integrity to improve the research. Future research can also develop a precise way to determine the Key Performance Indicator (KPI) that precisely reflects Service Level Agreement confidentiality and integrity. Key Performance Indicators help measure and manage confidentiality and integrity. Furthermore, this study explored the database-as-a-service concept. Service level agreement monitoring might be studied in different cloud service models like infrastructure-as-a-service and platform-as-a-service. Future research could leverage this study's findings to address limits, improve the tool, and explore containers, IoT devices, servers, and other cloud service monitoring aspects.

REFERENCES

Alhamazani, K., Ranjan, R., Mitra, K. et al. An overview of the commercial cloud monitoring tools research dimensions, design issues, and state of the art. Computing 97, 357–377 (2015)

Badger, M. , Grance, T. , Patt-Corner, R. and Voas, J. (2012), Cloud Computing Synopsis and Recommendations, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD

Barker, W. (2003), Guideline for identifying an information system as a national security system:, , National Institute of Standards and Technology, Gaithersburg, MD

Ludwig, H., Stamou, K., Mohamed, M., Mandagere, N., Langston, B., Alatorre, G., Nakamura, H., Anya, O., & Keller, A. (2015). rSLA: Monitoring SLAs in Dynamic Service Environments. Lecture Notes in Computer Science, 139–153.

Begic, K. and Tanovic, A. (2012) ‘Improvement of implementation of ISO-IEC 20000 edition2 standard in IT systems of telecom operator through comparison with Itil V3 Best Practices’

Capel, M.; Aporta, O. and Pegalajar-Jiménez, M. (2020). Quality of Service in Cloud Computing Environments with Multitenant DBMS. In Proceedings of the 10th International Conference on Cloud Computing and Services Science

Casola, V., De Benedictis, A., Rak, M. (2015). On the Adoption of Security SLAs in the Cloud. In: Felici, M., Fernández-Gago, C. (eds) Accountability and Security in the Cloud. A4Cloud 2014. Lecture Notes in Computer Science(), vol 8937. Springer, Cham

V. Casola, A. De Benedictis and M. Rak, ”Security Monitoring in the Cloud: An SLA-Based Approach,” 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 2015, pp. 749-755

Cérin, C., Coti, C., Delort, P., Diaz, F., Gagnaire, M., Gaumer, Q. and Ville, A. (2013) Downtime Statistics of Current Cloud Solutions. International Working Group on Cloud Computing Resiliency, Tech.Rep.

Petcu, D. (2014, July). A taxonomy for sla-based monitoring of cloud security. In 2014 IEEE 38th Annual Computer Software and Applications Conference (pp. 640-641). IEEE.

Endo, P. T., Rodrigues, M., Gonçalves, G. E., Kelner, J., Sadok, D. H., & Curescu, C. (2016). High availability in clouds: systematic review and research challenges. Journal of Cloud Computing, 5(1), 1-15.

Al-Shammari, S., & Al-Yasiri, A. (2015, October). MonSLAR: a middleware for monitoring SLA for RESTFUL services in cloud computing. In 2015 IEEE 9th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Environments (MESOCA) (pp. 46-50). IEEE.

Frey, S., Reich, C., & Lüthje, C. (2013, September). Key performance indicators for cloud computing SLAs. In The fifth international conference on emerging network intelligence, EMERGING (pp. 60-64).

N. Hubballi, A. K. Patel, A. K. Meena and N. Tripathi, ”Cloud Security Service Level Agreements: Representation and Measurement,” IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 145-150

Januzaj, Y., Ajdari, J., & Selimi, B. (2015). DBMS as a Cloud service: Advantages and Disadvantages. Procedia-Social and Behavioral Sciences, 195, 1851-1859.

N. Kaaniche, M. Mohamed, M. Laurent and H. Ludwig, ”Security SLA Based Monitoring in Clouds,” 2017 IEEE International Conference on Edge Computing (EDGE), Honolulu, HI, USA, 2017, pp. 90-97

Kosinski, J., Nawrocki, P., Radziszowski, D., Zielinski, K., Zielinski, S., Przybylski, G., & Wnek, P. (2008, March). SLA monitoring and management framework for telecommunication services. In Fourth International Conference on Networking and Services (icns 2008) (pp. 170-175). IEEE.

Manuel, P. A trust model of cloud computing based on Quality of Service. Ann Oper Res 233, 281–292 (2015)

F. E. Oliveto, ”An algorithm to partition the operational availability parts of an optimal provisioning strategy,” Annual Reliability and Maintainability. Symposium. 1999 Proceedings (Cat. No.99CH36283), Washington, DC, USA, 1999, pp. 310-316

Sousa, F. R., Moreira, L. O., Santos, G. A., & Machado, J. C. (2012). Quality of Service for Database in the Cloud. CLOSER, 12, 595-601.

A. Taha, A. Zakaria, D. Kim and N. Suri, ”Decentralized Runtime Monitoring Approach Relying on the Ethereum Blockchain Infrastructure,” 2020 IEEE International Conference on Cloud Engineering (IC2E), Sydney, NSW, Australia, 2020, pp. 134-143

A. Undheim, A. Chilwan and P. Heegaard, ”Differentiated Availability in Cloud Computing SLAs,” 2011 IEEE/ACM 12th International Conference on Grid Computing, Lyon, France, 2011, pp. 129-136,

de Boer, F. S., Giachino, E., de Gouw, S., Hähnle, R., Johnsen, E. B., Laneve, C., ... & Zavattaro, G. (2019). Analysis of SLA Compliance in the Cloud–An Automated, Model-based Approach.

Toeroe, M., & Tam, F. (Eds.). (2012). Service availability: principles and practice. John Wiley & Sons.

Ameller, D., and Franch, X. (2008, February). Service level agreement monitor (SALMon). In Seventh International Conference on Composition-Based Software Systems (ICCBSS 2008) (pp. 224-227). IEEE.