Volume 9, Issue 4, April – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

# AI-Driven Proactive Cloud Application Data Access Security

Priyanka Neelakrishnan
Independent Researcher and Product Innovation Expert,
Coimbatore, India

**Abstract:- The widespread adoption of cloud applications, accelerated by remote work demands, introduces new security challenges. Traditional approaches struggle to keep pace with the growing volume of cloud applications, keeping track of their user activities and countering potential threats. This paper proposes a novel user access security system for cloud applications. The system leverages user activity tracking tied to user, device, and contextual identity data. By incorporating Identity Provider (IdP) information, Natural Language Processing (NLP), and Machine Learning algorithms (ML), the system builds user baselines and tracks deviations to bubble up critical deviations to the surface and proactively prevent further worsening in real-time, working in conjunction with security orchestration, automation, and response (SOAR) tools. Deviations from the baselines, which may indicate compromised accounts or malicious intent, trigger proactive interventions. This approach offers organizations superior visibility and control over their cloud applications, enabling proactive and real-time threat detection and data breach prevention. While real-time data collection from application vendors remains a challenge, near-real-time is made feasible today. The system can also effectively utilize IdP logs, activity logs from proxies, or firewalls. This research addresses the critical need for proactive security measures in the dynamic landscape of cloud application data security. The system will need a quarter (90 days) of learning time to ensure accurate detections based on historically gathered data and protect them for future baseline predictions on the user themselves and as well as on their peers. This approach ensures the detection is contextually aware of the organization as a whole. This research completely redefines traditional thinking with decentralized intelligence across the system that has a highly scalable microservice architecture. The proposed solution is a uniquely intelligent system where both human and artificial intelligence coexist, with the ultimate overriding control lying with humans (admin). This way, the outcomes at every stage are effective, making the overall detection and proactive security effective.**

***Keywords:-*** *Data Protection; User; Peers; Organization; Machine Learning; Aggregator; Cloud Application Security.*

## I. INTRODUCTION

In recent years, the explosion of cloud applications and their adoption by organizations for business continuityhas become evident. However, this trend also brings a dark side where organizations lack visibility into how data in these cloud applications is stored and accessed by their employees, particularly as remote work becomes more prevalent for various reasons. One challenge lies in visibility, while another lies in controlling access. Without adequate visibility, controlling access becomes impossible.

Another pain point that organizations face stems from the large number of incidents generated by their legacy security solutions. Incident remediators often struggle to triage these incidents, and the lack of evidential data further complicates forensic analysis. As a result, data breaches may go unnoticed and become difficult to prove.

Traditional cloud application data protection security solutions typically rely on security policies authored by cloud administrators, which specify various criteria. Incidents are generated when these criteria are violated. However, a significant flaw in this approach is that there is no one-size-fits-all policy, and it's challenging to add or remove inclusions and exclusions from already complex policies. Consequently, critical violations may go unnoticed, leading to data breaches. Moreover, the sheer volume of incidents generated in medium and large organizations on a daily basis often leaves them unserviced for months. Even when incidents are addressed, challenges such as insufficient forensic evidence, numerous low-priority incidents escalating to critical ones, and a lack of contextual understanding persist.

All these issues pose a serious threat to organizations, making it difficult for them to confidently allow their employees to use cloud applications for processing sensitive and confidential data.

The main objective of this paper is to provide guidance and demonstrate that it is possible to implement a robust cloud data security system that proactively protects organizational data in cloud applications while encouraging employee productivity.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

This paper aims to develop a novel system that leverages human and artificial intelligence for data aggregation, correlation, context and intent derivation, and consolidation of point solutions to effectively address the core purpose of cloud application data protection.

## II. LITERATURE AND BACKGROUND SURVEY

Insider threats and attacks are on the rise. Sixty-eight percent of organizations have observed an increase in insider threats over the past 12 months [1], and forty-nine percent of organizations can't detect these threats. Even if detected, it's often difficult, if not impossible, to prove due to a lack of proper forensics [2]. Compromised cloud accounts cost companies an average of $6.2 million each year and lead to 138 hours of application downtime [3]. Notably, sixty-two percent of data breaches are attributed to leveraged credentials, according to the Verizon Data Breach Investigation Report [4]. It takes an average of 287 days for an organization to identify a data breach, with the average cost amounting to $3.86 million [5]. Types of users that pose a risk include disgruntled employees, outgoing employees, accidental exposures, corporate spies, and fraudsters.

My research on the OpenDaylight Software Defined Network (SDN) controller, conducted in 2016 [6], aimed to improve the scalability of the architecture through microservices running on different instances of the controller. This research provided valuable insights for the current study. Based on the findings in SDN microservice scaling architecture, we could employ a user activity microservice for a specific user across cloud application instances. This approach allows us to holistically gather user activities across different applications, providing a sophisticated user data feed and an intelligent analytic analyzer that scales both horizontally and vertically. The novel software microservice-based architecture mentioned in the SDN research [6] significantly influenced the architecture of the proposed cloud AI-driven data security system.

Several real-world case studies prompted the need for this research, leading to the development of this paper.

In the General Electric's Malicious Insider Case of 2020, a couple of GE employees were convicted of stealing trade secrets to gain a business advantage [7]. Thousands of files were downloaded by the employees before leaving the organization, without the knowledge of the GE cybersecurity team. It took GE several years to discover and convict them [8], and even then, proving the case took years due to a lack of forensics.

The Marriott Data Breach Case in January 2020 involved hackers gaining access to a third-party application through compromised credentials [9], resulting in access to Marriott guest lists containing sensitive PII information [10]. Marriott was fined £18.4 million for non-compliance with GDPR requirements, and it took several months for Marriott to discover the data breach.

In the Twitter Bitcoin Scam of July 2020, hackers gained access to administrative tools via compromised credentials of Twitter employees and posted scam messages from 130 private and corporate high-profile Twitter accounts [11], resulting in the transfer of $180,000 in bitcoins to scamming accounts.

The Zola Hack in May 2022 involved hackers using an age-old attack technique known as credential stuffing to breach the popular wedding planning site, Zola [12]. This resulted in fraudulent activity tied to customer accounts [13], with approximately 3,000 accounts compromised. As part of their remediation efforts, Zola temporarily disabled mobile apps connected to the platform, causing business slowdowns and requiring urgent remediation efforts.

## III. EXISTING SYSTEM AND UNIQUENESS OF THE PROPOSED SYSTEM

➢ *Existing User Entity Behavioral Analytics (UEBA) Solutions in the Market and Academic Research [14] Lack in Four Critical High-Level Areas:*

- It's always hard to create a baseline due to data corruption and lack of user data and its aggregation. Even when this challenge is addressed, there are the next layer of challenges. The data feed is not rich enough to correlate the user activity across multiple applications and multiple instances of the same application. This is where my previous SDN research [6] helps our current research to consolidate the data by having a specific user data service run in different instances across applications. Artificial intelligence (AI) technologies like natural language processing and generative AI models are used to quickly connect and grasp the intent and context of the user holistically.
- The analytics engine is not sophisticated enough to accurately compare the user activity among themselves and across their peers at the same given time stamp. Here is where our proposed system is unique. It uses machine learning (ML) models to train the user data in relation to peer data to establish a baseline, along with attaching a baseline deviation score to each user action for predictions. The covalent machine learning model, which has the user and peer score attached, encompasses multiple inner models like probabilistic models and location models that vertically scale on-demand to effectively analyze and assign the activity deviation scores. Additionally, our proposed solution also incorporates feedback from the admin or traditional policy-based services to train the ML model to proactively adapt its detections.
- Once existing UEBA solutions provide anomalous scores, they do not limit and are mostly used for informational visibility purposes. Here, with our proposed system, we provide information for visibility and simultaneously take real-time action to adjust

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

privilege permissions for suspicious users and send notifications to the admin and suspicious end-users via email and real-time system-generated "on-the-fly Policy" logged in the existing policy lists. When the notification reaches the admin in real-time, they have the option to override the system-provided "on-the-fly Policy" back to its previous state. This approach allows malicious users to be prevented from certain access or activities without blocking productivity. In the future, suspicious end-users and their managers could also be added to the notification service, and the manager could be given a justification option submitted to the admin to allow for one of several scenarios in a decentralized manner, saving them triaging time. This approach eliminates the burden on the admin while allowing them to retain overall approval/disapproval authority.

- In a traditional system, there is only one analytic engine that is intelligent with a basic ML model or rule-based model. This engine forms the core of the UEBA system. However, in our proposed system, the intelligence of the detection engine is decentralized, making every service from the ground up autonomous to enable smart work for a fully intelligent system.

Overall, we have established that the proposed solution is one-of-a-kind and has been proposed for the first time.

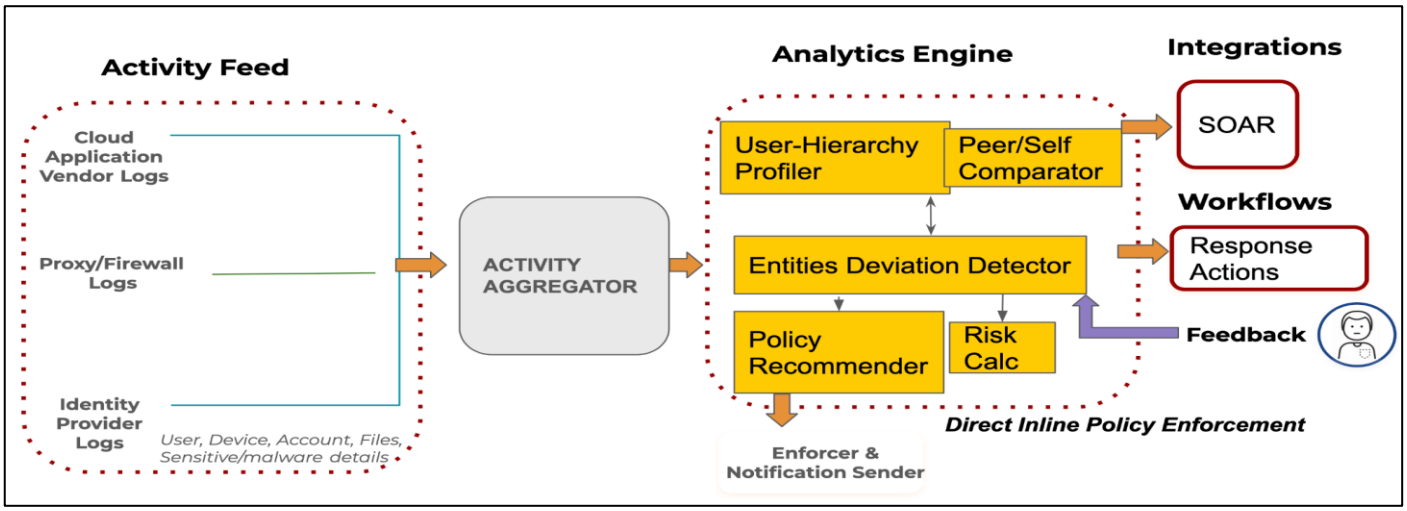



Fig 1: AI-Driven Data Access Security System

## IV. PROPOSED SYSTEM ARCHITECTURE

The proposed system is architecturally classified into four horizontal planes. In the proposed model, the intelligence of the data processor is decentralized across all the planes, unlike traditional single intelligent UEBA analytic engines. This way, the system becomes fully autonomous and ready for smart work from the ground up.

- Activity feeder plane
- Aggregator plane
- Analytics engine plane
- Action driver plane.

There are several services running in each of these planes that scale both vertically and horizontally on-demand to avoid performance degradation during load. The services themselves shut down and turn on as per the servicing application and user traffic data. All of the microservices in the system scale horizontally and vertically on-demand.

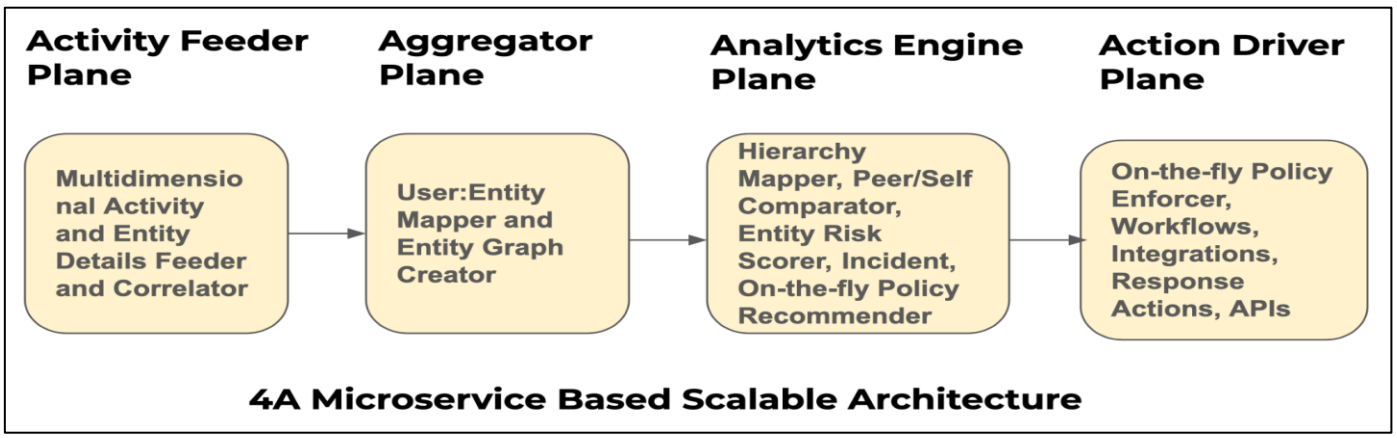



Fig 2: Automatic System Architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

*A. Activity Feeder Plane*

The activity feeder plane is responsible for collecting and providing a rich data feed of the user, device, application, identity provider services, proxy or firewall, and cloud application vendor logs to the aggregator in their respective formats. Each entity has a service of its own that scales, for example: user service, application service. Inside that parent service, there are child services to support multi-tenancy, such as device service, cloud Azure service, Okta service, proxy service, file manager service, file activity type service, resource creator tracker service, sensitive data snippet service, and malware file identifier service. There is a common "Time manager service" based on a large language model (LLM) and natural language processing (NLP) that collects data from each service to associate the outputs together based on the timestamp and funnel them to the Activity aggregator service.

*B. Activity Aggregator Plane*

The activity aggregator plane is responsible for the overall mapping to draw the user 360 associations. Key mapper microservices are run in this plane, including user:device mapper, user:application mapper and its child service user:app instance mapper, user:location mapper, user:sensitive data snippet mapper, user: malware file mapper, user:file activity type mapper, and user:resource creator tracker mapper. There is a common "Job manager service" that unifies the details from the output of each of the services to create a user and entity 360 graph with all the user activities and their associated entities aggregated.

*C. Analytics Engine Plane*

The analytics engine plane is responsible for creating a holistic user profile with hierarchy and peer profile mapper. Services like comparator, active directory hierarchy collector, deviation score assigner, further probability predictor, user graph enhancer, feedback collector, feedback disperser, on-the-fly policy enforcer, notifier, and admin on-the-fly policy overrider are included in this plane. The analytics engine plane outputs the user risk score, entity risk score, on-the-fly policy recommendations, notifications, and a forensics trail with the incident log. The entity risk score here refers to application risk scores, file risk scores, file activity type risk scores, device risk scores, department/division risk score, role-based risk scores, and region risk scores.

*D. Action Driver Plane*

The action driver plane is responsible for taking actions after the detailed visibility provided by the analytics engine plane. The services in this plane include on-the-fly policy service, incident forensic viewer, and external integrations like security orchestration, automation and response (SOAR) system or just APIs. Bi-directional communication is involved in case of response actions and workflows. In the future, there is potential for generating reports and having them accessible via APIs in this plane. This plane is also responsible for notifying suspicious end users, their managers and admins, and managing justification approval workflows.

## V. METHODOLOGY

The solution runs for a solid 90 days (typically from the beginning of the quarter), collecting all the activities surrounding the entities. This ensures that unique activities occurring at the end of the quarter are not missed.

In the first stage, which involves services in the activity feeder plane, smart microservices are trained to collect all the activities by tracking every entity along with the corresponding timestamps. The entities of interest include:

- User
- Files/Folders
- Application
- Application Instances
- Sensitive Data Snippets
- Malware Details
- Account Details, Including Service Accounts
- Identity Provider Logs
- Identity Provider Sync (Azure Ad, Okta)
- Device Details
- All Possible Logs From Cloud Application Vendors And Proxies.

The primary focus in this stage is the user and the user's interaction with all related entities. Every activity related to the user is thoroughly captured for processing. Smart AI technologies then act on this data and create time-based event correlations.

In the second stage, the aggregator plane receives the time-correlated event logs for the entities and begins creating the user:entity mapper in the respective microservices. The result of this processing is to create a mapper table for user interaction and to follow the data in addition to the user. A consolidated user and entity graph is created as the output, enabling the system to track data from its origination. This operation enhances forensics and enables proactive security.

In the third stage, the analytics engine plane receives the entity graphs and uses AD sync information to finalize the user profile with respect to their position in the organization. User role, department, region, group, and peer information, along with their corresponding activities at the same given time, are compared. This results in:

- Granular user profile
- User and entity risk scores, comparing the user to themselves, peers, and entities
- Evidence content for forensics
- Incidents with severity
- On-the-fly policy recommendations.

Feedback from humans (admins) is analyzed by the feedback analyzer to ensure the system's accuracy and practicality. The merge of human and system intelligence ensures control over scoring and detection by humans

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

(admins). Risk is calculated based on deviations detected in a user/entity's normal behavior pattern. An overall risk score, its corresponding range, and rank are computed for a user/entity based on various types of suspicious activity incidents.

➢ *The User/Entity Risk Model Includes:*

- Risk Range: Critical, High, Medium, Low, Info level
- User/Entity Risk Score: (0-100)%
- Risk Rank: user rank/number of employees in the organization
- Peer Risk Score: (0-100)%.

Risk scores are computed in a human-understandable percentage format (0-100)%, with risk range categorization for plain English interpretation.

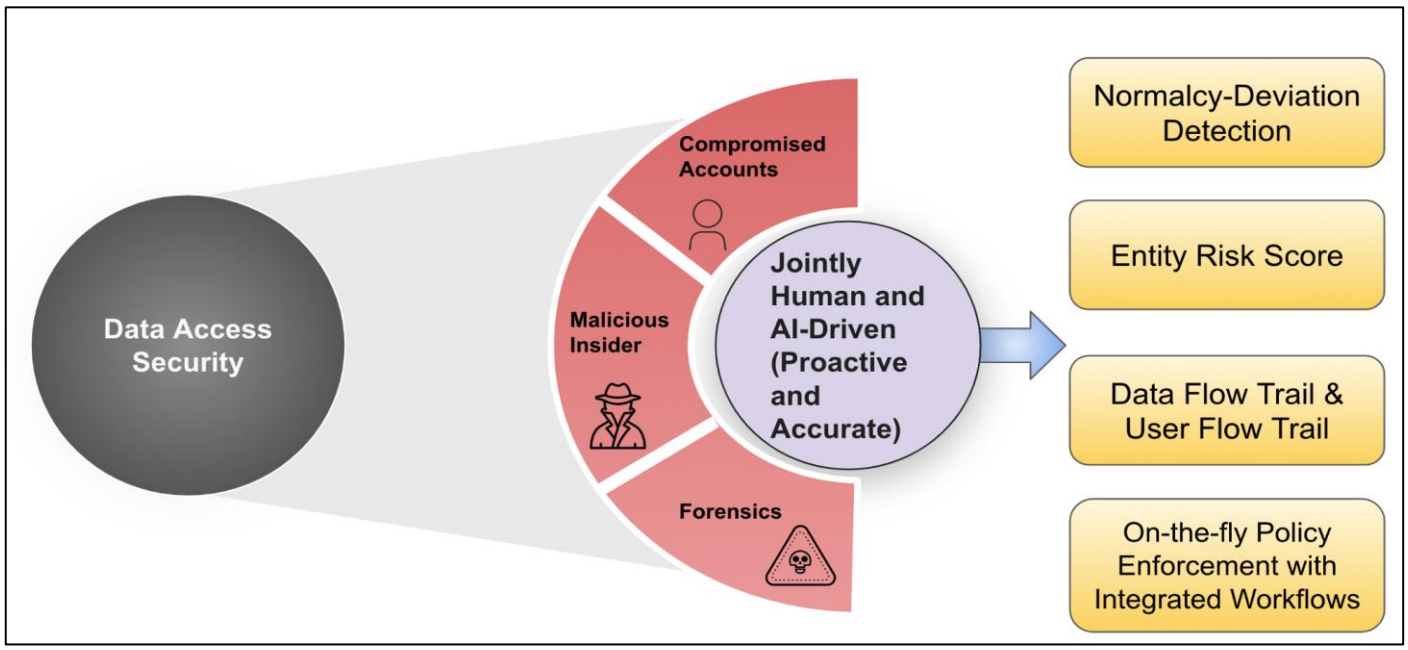



Fig 3: Key Outcomes from Analytics Engine Plane

In the fourth stage, the action driver plane is responsible for taking control actions based on the visibility and recommendations provided by the analytics engine plane. This is where the response actions, involving write-to-left communication in the system, are initiated. For instance, once a policy is enforced, the notification of the incident is sent to the suspicious end user, their manager, with the option to provide justification, and the admin to approve or revoke the on-the-fly policy in real-time.

➢ *Here are Some of the Key Use Cases the System Effectively Addresses.*

- Potential Attacker Identification - As a cloud admin, I'd like to detect and prevent potential attacks to ensure our organization's data in the cloud remains secure.
- User Access Privilege Misuse Identification - As a cloud admin, I'd like to identify and stop unnecessary privileges given to certain users and restore them to their peer norms.
- Malicious insider stealing data from multiple corporate applications - An employee exfiltrates data by downloading a large number of files from Google Drive and Box, later uploading them to their personal Google Drive from a managed device.
- Admin gets notified of suspicious user activities - By having both the employee's profile and their group, the normalcy-deviation detector (without any policies) tracks activities across corporate applications and flags the user as suspicious, thereby identifying malicious insiders.
- Multiple devices using the same credentials to access corporate apps - Several employees from the same department and region access Salesforce corporate applications using the credentials of the same local account.
- Manager gets notified of compromised account - Having device-to-user mapping, the normalcy-deviation detector (without any preset policies) tracks Salesforce application access from different devices using the same local account and flags this as a compromised account. The manager of the group gets notified, necessitating them to deprovision the account to mitigate potential risks.
- Malicious data accesses go undetected - Employees use their valid credentials to exfiltrate data; ex-employees

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

still use unprovisioned accounts to gain access; attackers use valid user accounts to access corporate applications.

- Visibility to admin - Risk score-based top risky users - ML-driven analytics engine tracks user activities across all SaaS applications. Based on this, every user in the organization receives a risk score indicating their risk to the organization. The admin gains visibility on top risky users, and policy recommendations are provided to monitor the risky users accessing applications, which the admin can enforce in a single click.
- Remote employee accesses corporate data - An employee accesses corporate applications from a new remote location using their managed device.
- Instant incident remediation with SOAR - The behavioral analytics engine flags the user as suspicious. SaaS security directly integrated with SOAR automatically executes a playbook to notify both the employee and their manager about this incident. The manager remediates the incident by providing a response action as a false positive with justification that the user has moved to this new remote location.
- Malware attacker goes unrestrained - An employee continuously uploads malware files to a corporate application. The system immediately blocks the attacker and enables the admin for future decisions. The analytics engine has already flagged this user as “high” risk. Additionally, the engine notifies this specific user uploading malware content to the corporate application, makes a policy recommendation, and enforces blocking the user from further accessing that corporate app. The admin reviews this enforcement and allows or revokes this policy in a single click.

## VI. IMPLEMENTATION AND RESULTS

The overall system implementation is done using the Java programming language, and machine learning models, largelanguage models, and natural language processing are used across the system, working and interacting along with the databases and the microservices. These models utilize a range of methodologies starting with probability distribution, neural networks, and feedback correlator, and subsequent decorrelator to ensure the models are more robust and accurate. Following are the key scenarios for testing:

*A. Compromised Accounts (Credential Theft):*

- Local Accounts - Several employees from the same department and region access the Salesforce corporate application using the credentials of the same local account. Leaving loose ends would mean the employee, even after leaving the organization, could access that local account with the known shared credentials.
- Is Uma really Uma? - Uma usually accesses the Box application from San Jose, California, between the hours of 8 am and 6 pm. A hacker, who claims to be Uma, with her stolen credentials accesses the same Box application from a different location (never accessed by Uma from this location based on her past history) at an unusual time.

*B. Privilege Misuse (Privileged User Threats):*

- Activity Type - Losh, who is part of the HR organization, usually can view the salary data of all employees. She also has the additional privilege to copy. Losh copies the salary information of select employees in the Sales organization, differing from the behavior of her peers.
- Application Access - Neela from the engineering division has access to all corporate applications in the organization. One fine day, Neela accesses the Salesforce application to view the quarterly report, differing from her peers in the engineering department.

*C. Data Exfiltration (Data Theft):*

Bulk Activity - Pranesh has tendered his resignation. Now, Pranesh downloads marketing documents from different corporate applications, which is unusual behavior compared to his baseline behavior. He intends to use this information in his next job.

*D. Sensitive Data Exfiltration (Data Breaches):*

- Extensive Sensitive Data Access -Viji, who is a Bank manager, downloads all customer PII data from corporate GDrive.
- Broader Sensitive Data Access - Perumal is an employee in the HR department who, as part of his job duties, had to access employees' SSN. Suddenly, we see Perumal accessing the source code and HIPAA content. This is a deviation from his usual sensitive content access, which is SSN.

The system creates entity details, which are the outcomes of the analytics engine plane. Figure 4 illustrates the fundamentals of user details, which also stack ranks the entity with respect to their peers. Figure 5 showcases how the incidents change over time as the system learns and adapts the detection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

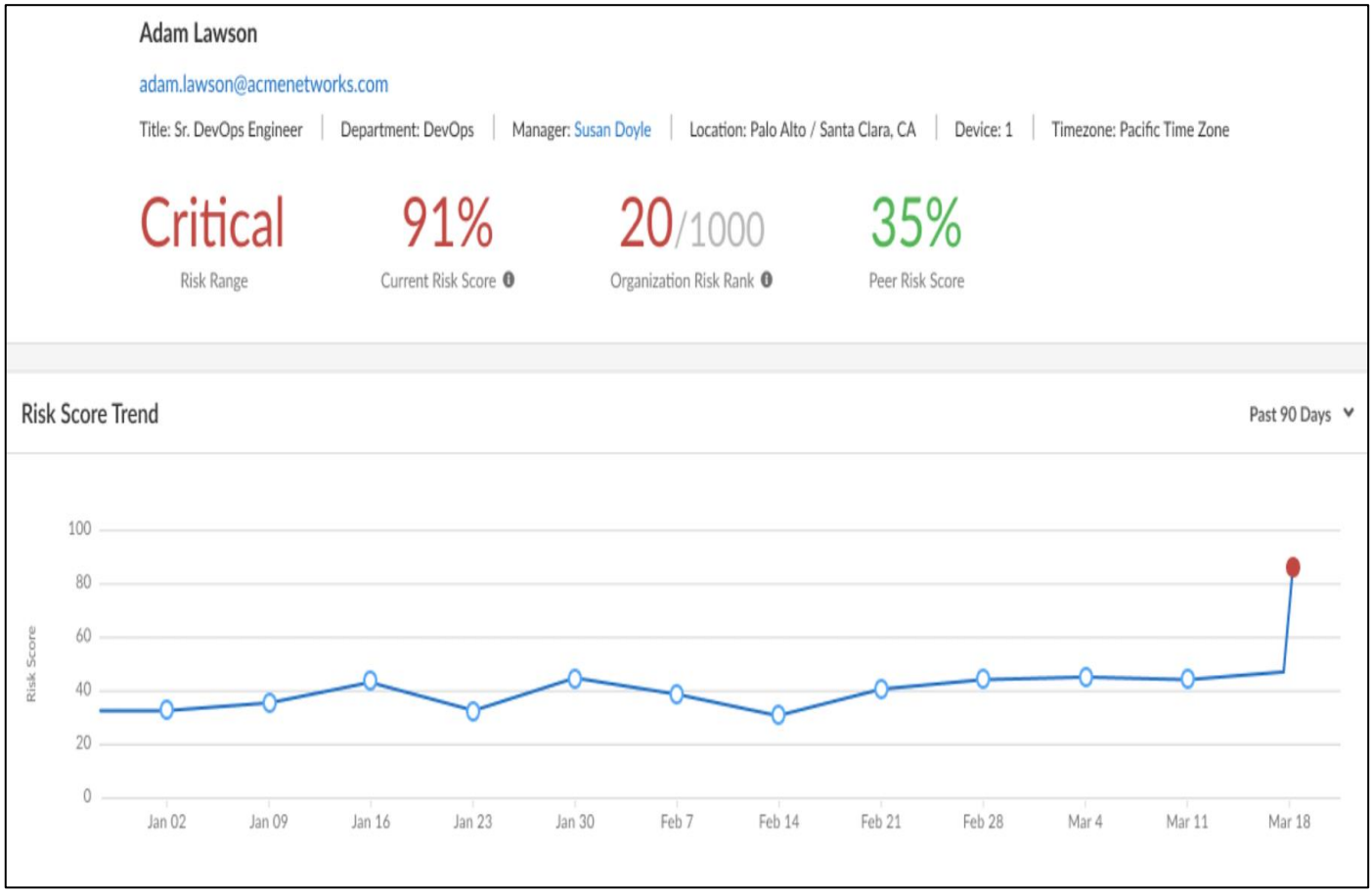



Fig 4: User/Entity Details

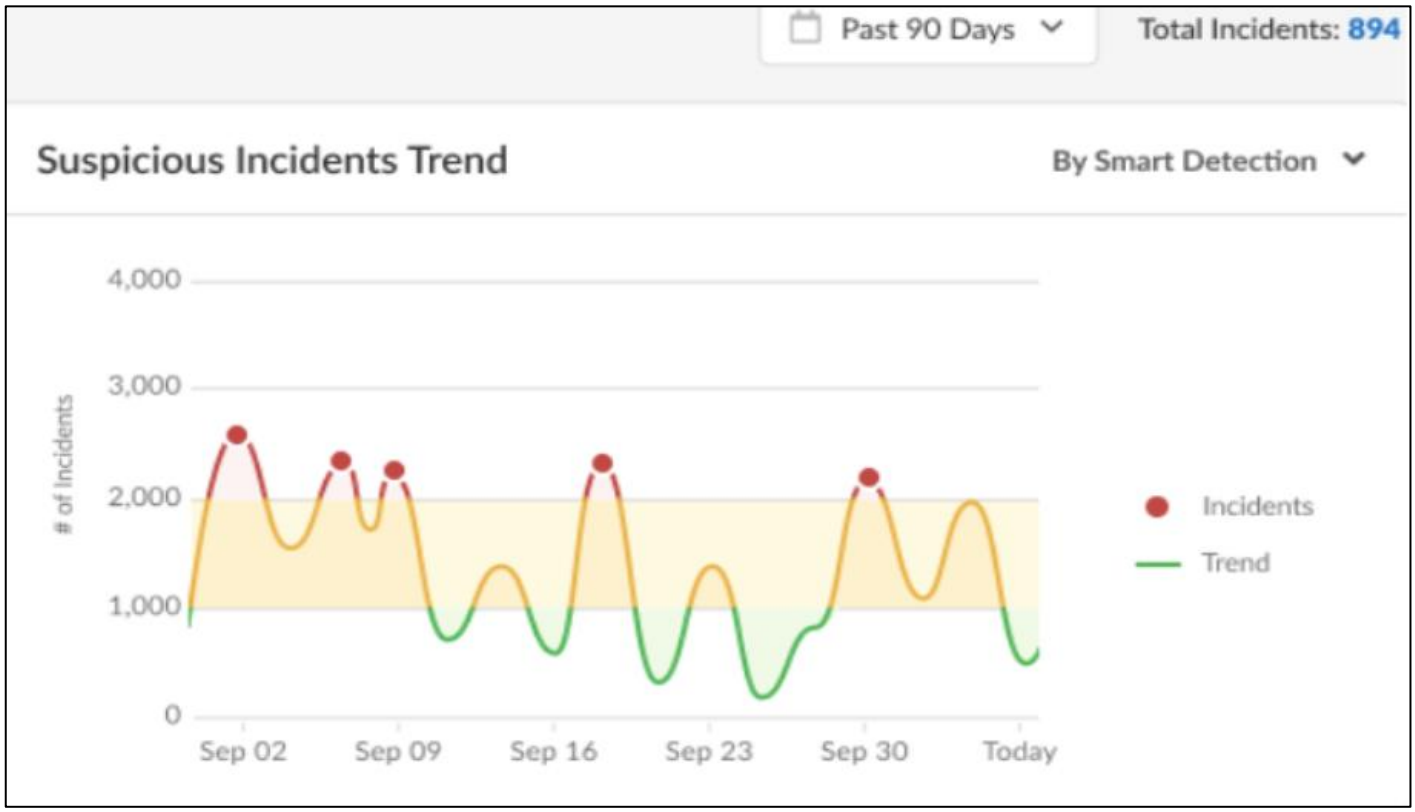
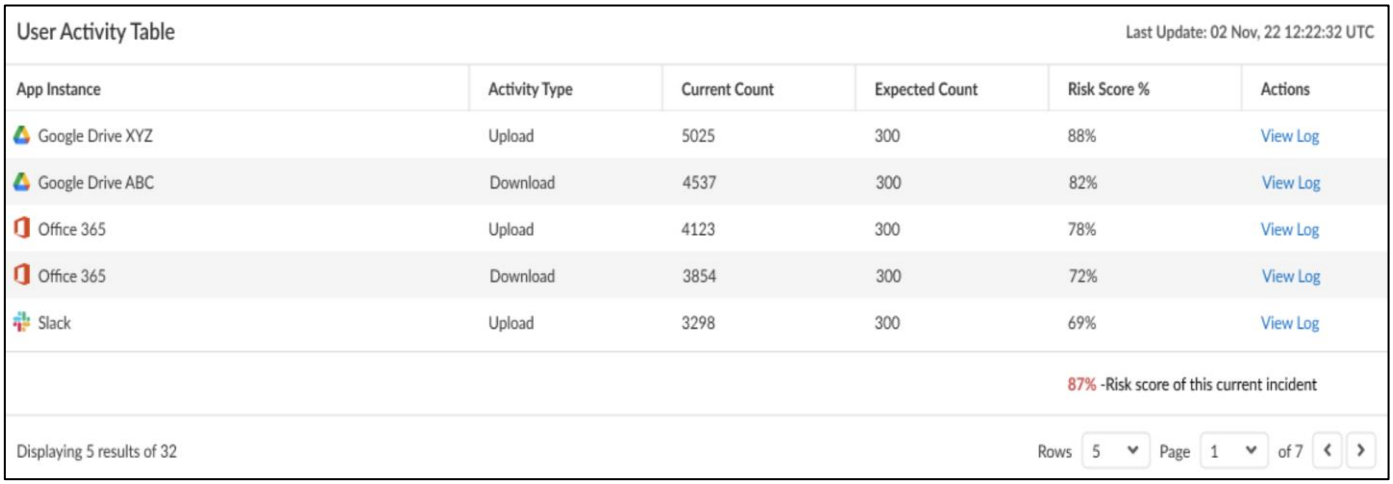



Fig 5: Incident Trend over a Time Period

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

➢ *Key Outcomes of the System are as Follows:*

- File Count Deviation - Data Exfiltration/Suspicious Data Access (Volume Deviation) - App Instance Name, Activity Type, Current File Counts, Expected Value, Risk Score, View Log.



User Activity Table — Last Update: 02 Nov, 22 12:22:32 UTC

| App Instance | Activity Type | Current Count | Expected Count | Risk Score % | Actions |
|---|---|---|---|---|---|
| Google Drive XYZ | Upload | 5025 | 300 | 88% | View Log |
| Google Drive ABC | Download | 4537 | 300 | 82% | View Log |
| Office 365 | Upload | 4123 | 300 | 78% | View Log |
| Office 365 | Download | 3854 | 300 | 72% | View Log |
| Slack | Upload | 3298 | 300 | 69% | View Log |

87% -Risk score of this current incident

Displaying 5 results of 32 Rows 5 Page 1 of 7

Fig 6: User Activity Table for Data Access

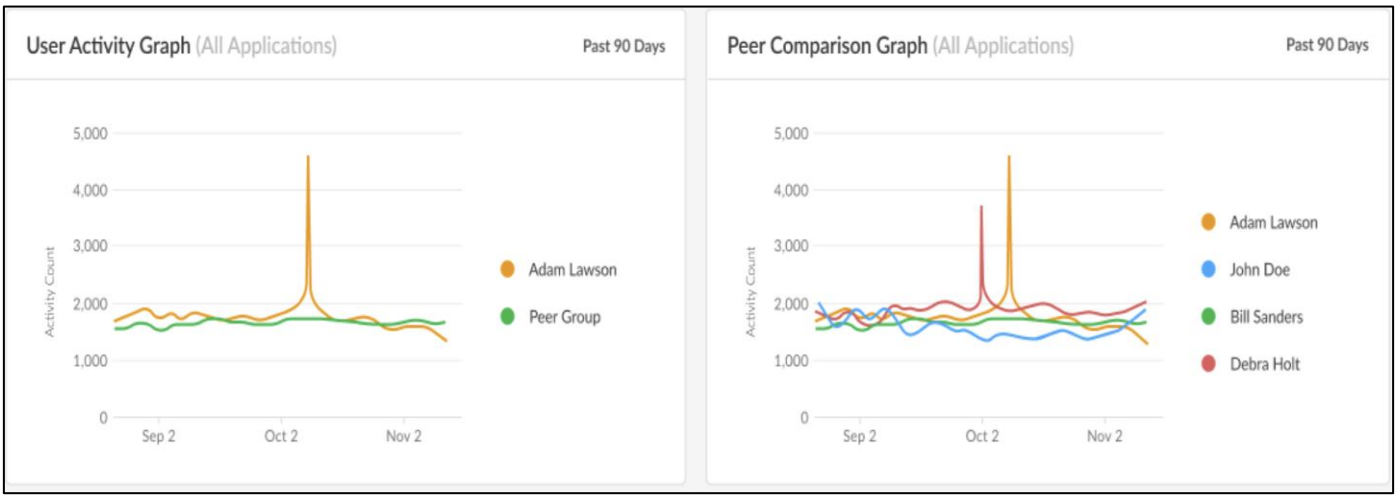
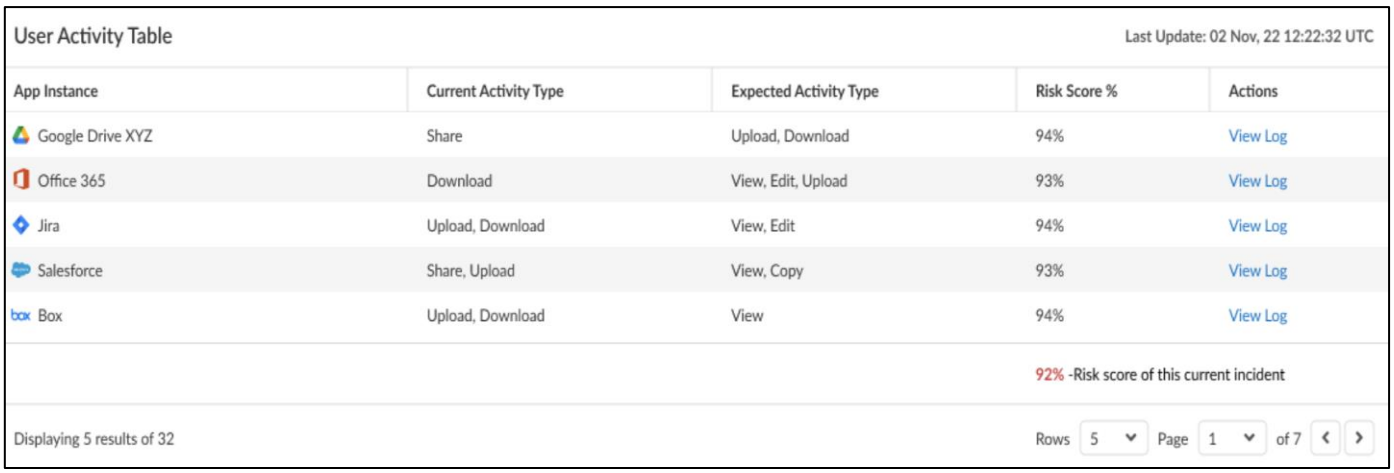



Fig 7: User and Peer Comparison Graphs for Data Access

- File Activity Type Deviation - Privilege Misuse/Suspicious Activity Type Access and Suspicious Application Access (Activity Type Deviation, Applications Deviation) - App Instance Name, Current Activity Types/Applications Value, Expected Value, Risk Score.



User Activity Table — Last Update: 02 Nov, 22 12:22:32 UTC

| App Instance | Current Activity Type | Expected Activity Type | Risk Score % | Actions |
|---|---|---|---|---|
| Google Drive XYZ | Share | Upload, Download | 94% | View Log |
| Office 365 | Download | View, Edit, Upload | 93% | View Log |
| Jira | Upload, Download | View, Edit | 94% | View Log |
| Salesforce | Share, Upload | View, Copy | 93% | View Log |
| Box | Upload, Download | View | 94% | View Log |

92% -Risk score of this current incident

Displaying 5 results of 32 Rows 5 Page 1 of 7

Fig 8: User Activity Table for Activity Type Access

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

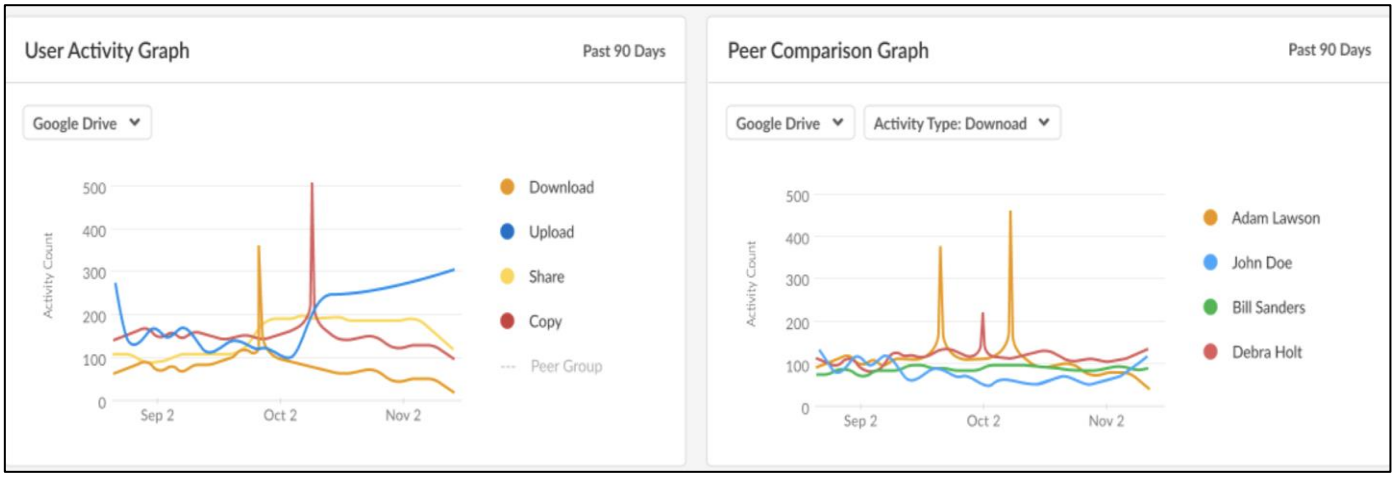



Fig 9: User and Peer Comparison Graphs for Activity Type Access

- Application Access Deviation - Privilege Misuse/Suspicious Activity Type Access and Suspicious Application Access (Activity Type Deviation, Applications Deviation) - App Instance Name, Current Activity Types/Applications Value, Expected Value, Risk Score.

User Activity Table — Last Update: 02 Nov, 22 12:22:32 UTC

| Application | Current App Instance | Expected App Instance | Risk Score % | Actions |
|---|---|---|---|---|
| Google Drive | Google Drive abc | Google Drive xyz | 94% | View Log |
| Office 365 abc | Office 365 abc | Office 365 xyz | 93% | View Log |
| Jira 12 | Jira 123 | Jira xyz | 94% | View Log |
| Salesforce 2 | Salesforce abc | Salesforce xyz | 93% | View Log |
| Box 2 | Box jkl | Box xyz | 94% | View Log |

92% -Risk score of this current incident

Displaying 5 results of 32 Rows 5 Page 1 of 7

Fig 10: User Activity Table for Application Access

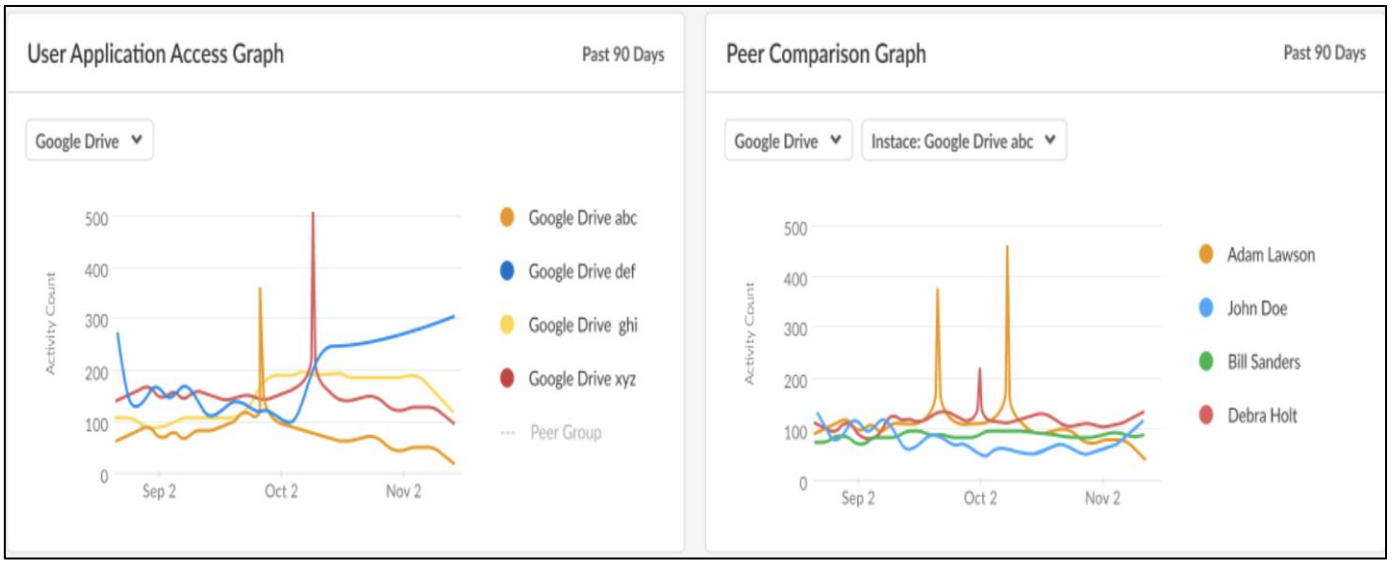



Fig 11: User and Peer Comparison Graphs for Application Access

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

- Location and Time Deviation - Compromised Account/Suspicious Logins (Time Deviation, Location Deviation, Device Deviation) - App Instance Name, Current Value (Time, Location, Device), Expected Value, Risk Score, View Logs.

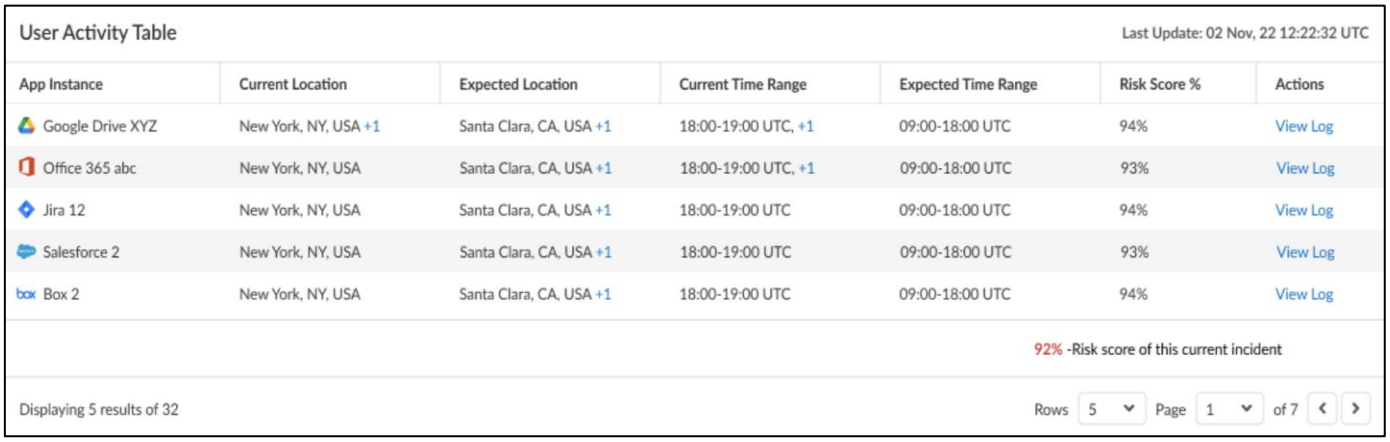



Fig 12: User Activity Table for Time and Location Access

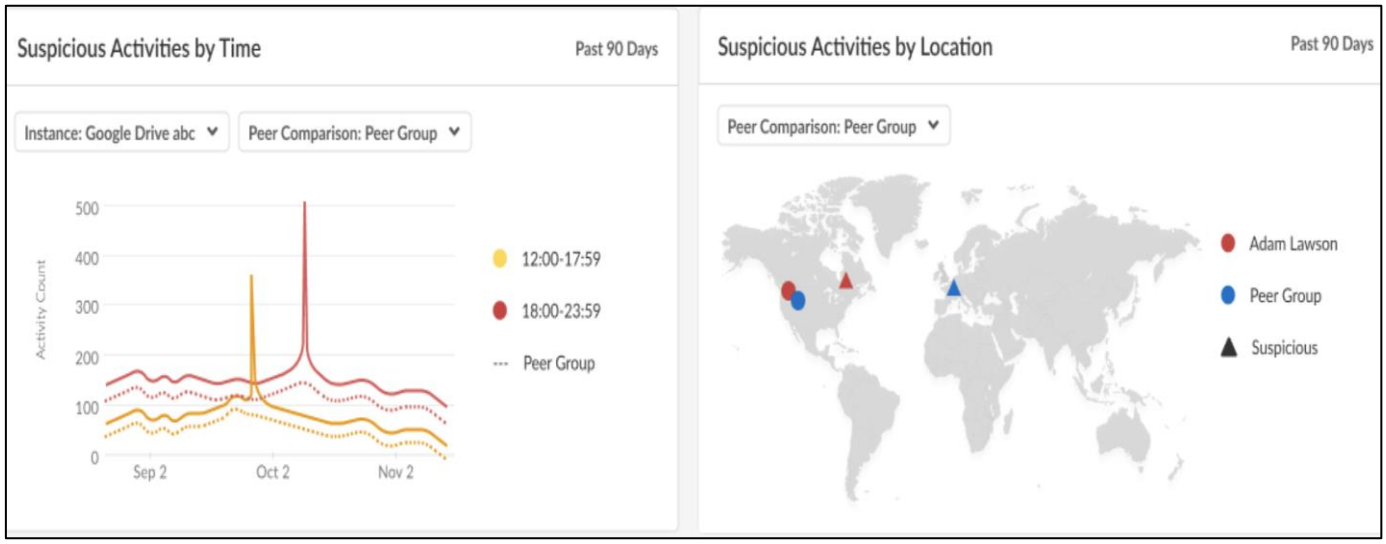



Fig 13: User and Peer Comparison Graphs for Time and Location Access

- Sensitive Data Access Deviation - Sensitive Data Exfiltration/Suspicious Sensitive Content Access (Data Patterns and Profiles) - App Instance Name, Activity Type, Current Value (Files/Messages/Entity), Expected Value, Risk Score, View Log (this will include Time, Location, File/Entity Name, Sensitive Data Content).

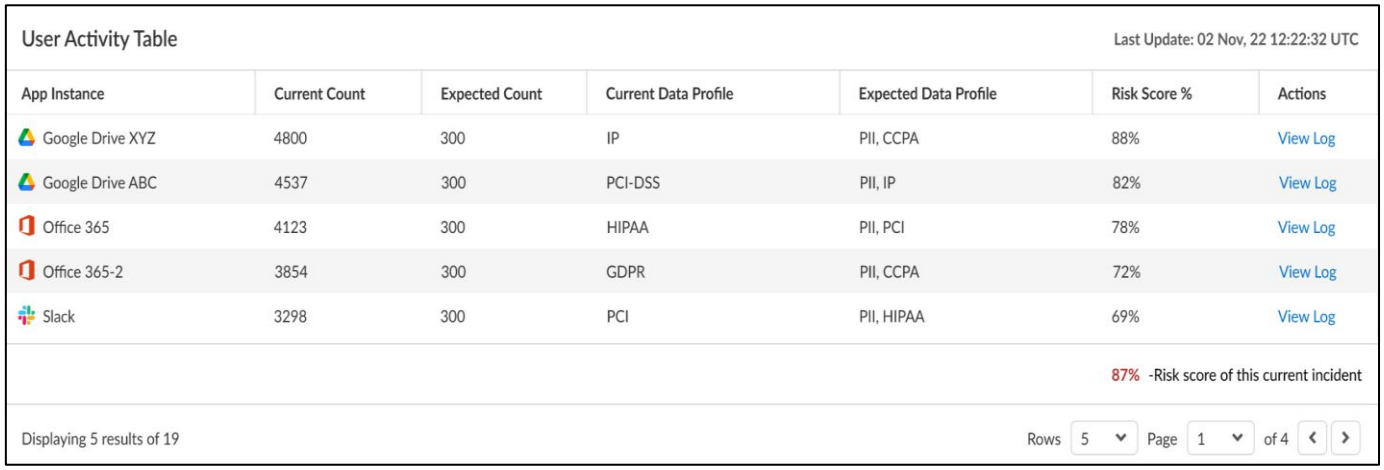



Fig 14: User Activity Table for Sensitive Data Access

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

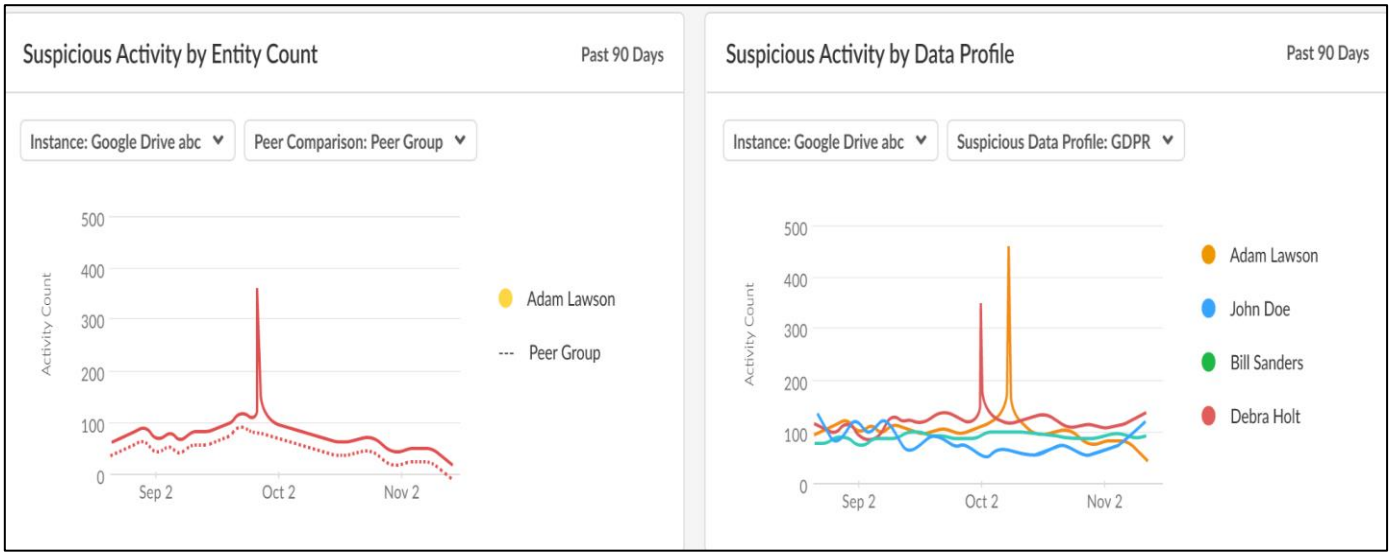



Fig 15: User and Peer Comparison Graphs for Sensitive Data Access

## VII. CONCLUSION

In summary, the findings of this research emphasize the importance of implementing robust security protocols to protect organizational data within cloud environments. Through an in-depth examination of various threat scenarios, we have underscored the critical need for proactive detection and mitigation strategies to safeguard against potential breaches.

Our proposed system, leveraging advanced technologies including machine learning models, large language models, and natural language processing, offers a comprehensive approach to identifying and addressing security risks. By harnessing these methodologies, we enhance the accuracy and efficiency of threat detection, enabling organizations to respond swiftly and effectively to potential security incidents.

Moreover, the system's capability to analyze user behavior, application access patterns, and data activity deviations provides administrators with valuable insights into potential security vulnerabilities. By stack-ranking entities and providing risk scores, administrators can prioritize remediation efforts and allocate resources more efficiently, thereby strengthening the organization's overall security posture.

In conclusion, this research highlights the effectiveness of an integrated approach to cloud data security, combining advanced technologies with proactive monitoring and response mechanisms. By adopting such strategies, organizations can fortify their defenses against emerging threats and mitigate the risks associated with sensitive data access and exfiltration, thus safeguarding the integrity and confidentiality of their valuable assets.

## REFERENCES

[1]. Cybersecurity Insiders, “Insider Threat Report [Gurucul],” [Online]. Available at: https://www.cybersecurity-insiders.com/wp-content/uploads/2021/06/2021-Insider-Threat-Report-Gurucul-Final-dd8f5a75.pdf. [Accessed: May-2022].

[2]. Pulse and Code 42 Survey report. “Pulse Survey: 47% of Organizations Don’t Properly Monitor Insider Risk Indicators,” [Online]. Available at: https://www.code42.com/resources/infographics/pulse-survey-forty-seven-percent-of-organizations-dont-properly-monitor-insider-risk-indicators. [Accessed: May-2022].

[3]. Ponemon LLC Research report, “The Cost of Cloud Compromise and Shadow IT,” [Online]. Available at: https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-us-ar-cost-of-cloud-compromise-and-shadow-IT.pdf. [Accessed: May-2022].

[4]. Verizon business, “2022 Data Breach Investigations Report (DBIR),” [Online]. Available at: https://www.verizon.com/business/resources/reports/dbir/. [Accessed: May-2022].

[5]. IBM Security, “Cost of a Data Breach Report,”[Online]. Available at: https://www.ibm.com/downloads/cas/RZAX14GX [Accessed: May-2022].

[6]. Priyanka Neelakrishnan, “Enhancing Scalability and Performance in Software-Defined Networks: An OpenDaylight (ODL) Case Study,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[7]. “Famous Insider Threat Cases,” [Online]. Available at: https://gurucul.com/blog/famous-insider-threat-cases. [Accessed: June-2022].

[8]. “Trade Secret Theft,” [Online]. Available at: https://www.fbi.gov/news/stories/two-guilty-in-theft-of-trade-secrets-from-ge-072920. [Accessed: June-2022].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR957

[9]. "Real Life Data Breaches caused by Insider Threats," [Online]. Available at: https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches. [Accessed: June-2022].
[10]. "Marriott International Notifies Guests of Property System Incident," [Online]. Available at: https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident. [Accessed: June-2022].
[11]. "2020 Twitter account Hijacking," [Online]. Available at: https://en.wikipedia.org/wiki/2020_Twitter_account_hijacking. [Accessed: June-2022].
[12]. "Credential Stuffing," [Online]. Available at: https://en.wikipedia.org/wiki/Credential_stuffing. [Accessed: June-2022].
[13]. "Wedding Registry site Zola says Customer Accounts were Hacked," [Online]. Available at: https://www.nydailynews.com/2022/05/23/wedding-registry-site-zola-says-customer-accounts-were-hacked/. [Accessed: June-2022].
[14]. JagreetKaur; Kuldeep Kaur; Surya Kant; Sourav Das,"UEBA with Log Analytics," IEEE 3rd International Conference on Computing, Analytics and Networks (ICAN), 2023.

**PRIYANKA NEELAKRISHNAN**, was born on December 20, 1990. She holds a Bachelor of Engineering degree in Electronics and Communication Engineering from Anna University, Chennai, Tamil Nadu, India (2012); a Master of Science degree in Electrical Engineering with a focus on Computer Networks and Network Security from San Jose State University, San Jose, California, United States (2016); and a Master of Business Administration degree in General Management from San Jose State University, San Jose, California, United States (2020). Currently, Priyanka works as a Product Line Manager, Independent Researcher, and Product Innovator, specializing in driving product innovation and development. Previously, she has held positions as a Senior Product Manager and Senior Software Development Engineer at reputable cybersecurity firms.

Priyanka Neelakrishnan is also an accomplished author, having penned the book titled "Problem Pioneering: A Product Manager's Guide to Crafting Compelling Solutions". She is currently in the process of writing another book focusing on cybersecurity.