Industry Perception of Security Challenges with Identity Access Management Solutions

Abhishek Pratap Singh
Department of Informatics
King's College London
London, UK
abhishek.p.singh@kcl.ac.uk

Ievgeniia Kuzminykh
Department of Informatics
King's College London
London, UK
ievgeniia.kuzminykh@kcl.ac.uk

Bogdan Ghita
School of Engineering, Computing and Mathematics
University of Plymouth
Plymouth, UK
bogdan.ghita@plymouth.ac.uk

***Abstract*— Identity Access Management (IAM) is an area posing significant challenges, particularly in the context of remote connectivity and distributed or cloud-based systems. A wide range of technical solutions have been proposed by prior research, but the implementation and integration of these solutions in the commercial sector represent steps that significantly hamper their acceptance. The study aims to outline the current perception and security issues associated with Identity Access Management (IAM) solutions from the perspective of the beneficiaries. The analysis relies on a series of interviews with 45 cyber security professionals from different organisations all over the world. The particular focus of the study is represented by the challenges and vulnerabilities of on-premises and cloud-based IAM deployment models. As highlighted by the interviewees, cloud IAM solutions and on premises IAM solutions are affected by different issues. The main challenges for cloud based IAM solutions were Default configurations, Poor management of Non-Human Identities such as Service accounts, Poor certificate management, Poor access review, Poor API configuration and limited Log analysis. In contrast, the challenges for on premise solutions were Multi Factor Authentication, insecure Default configurations, Lack of skillsets required to manage IAM solution securely, Poor password policies, Unpatched vulnerabilities, and compromise of Single-Sign on leading to compromise of multiple entities. The study also determined that, regardless the evolving functionality of cloud based IAM solutions, 41% of respondents believe that the on premise solutions more secure than the cloud-based ones. As pointed out by the respondents, cloud IAM may potentially expose organisations to a wider range of vulnerabilities due to the complexity of the underlying solutions, challenges with managing permissions, and compliance to dynamic IAM policies.**

Keywords*— *Identity Access Management, IAM, On Premise, Cloud, Access Control, Vulnerability, Authentication, Authorisation, CISO

I. INTRODUCTION

Identity and Access Management (IAM) is pivotal in safeguarding digital and at times physical identities. IAM solution is being extensively used in a typical on-premises environment where deploying organisations own everything including user administration, cost of software, underlying support infrastructure along with security aspects such as vulnerability and patch management, penetration testing, etc.

On the other side, in a cloud-based IAM model such as Infrastructure as a server (IaaS), Software as a Service (SaaS) it's been taken care of by Cloud service provider (CSP).

In the realm of cybersecurity, IAM stands as a critical cornerstone. Simultaneously, cloud computing has emerged as a transformative model for delivering IT services via the Internet, offering scalability, flexibility, and cost efficiency. However, this paradigm shift brings various security challenges, particularly within IAM.

A study [1] shows that Cloud IAM solutions occupy 42% of the IAM market with expected growth of 18.3% between 2022 and 2032, and sales of cloud IAM are expected to reach US$ 25,539.2 million by 2032.

Checkpoint cloud security report 2023 [2] indicates that around 24% organisations have faced public cloud related incidents. The previous Checkpoint report in 2022 [3] showed that 15% of all cloud incidents were linked to compromising of IAM; report also states that 72% of respondents are using Microsoft Azure, 69% are using Amazon Web Services (AWS) and 34% are using Google Cloud Platform (GCP) as their IaaS providers, yet 54% of this audience conceded to the fact that for Cloud security they rely on independent security service provider. Despite highlighting the overall concerning picture, neither of the two reports details specific incidents or concerns related to the cloud based IAMs.

Given the increasingly distributed range of technical solutions for IAM, coupled with the seamless interconnectivity of systems in such environments, organisations are (justifiably) concerned when required to deploy more flexible IAM, potentially as a cloud service rather than a controlled on-premises solution. Therefore, the aim of this study is to explore the security concerns and weaknesses of cloud and on premise solutions for access management from the perspective of their beneficiaries – the companies requiring such implementations.

II. Background and Related Works

In order to understand the current level of threat posed by the IAM vulnerabilities and weaknesses, this section discusses a series of specific security breaches, based on their public reporting. This review represents the foundation for investigating the attack vectors attackers in the past and overview the related studies highlighting the challenges with the IAM systems.

A study by the monitoring company ManageEngine [4], which focused on cyber incidents linked due to IAM solutions failure over last decade, described an incident where hackers breached the Deloitte global email server infrastructure via an administrator account which was protected by a single password without any multi-factor authentication (MFA). In a similar case, the online shopping giant eBay and the major home improvement retailer HomeDepot became victims of data exfiltration as credential of small group of employees were compromised. According to the Checkpoint reports [2, 3] the account compromise happens to compose 29% in 2022 and 16% in 2023 of all security incidents related to public cloud.

The study of Gofman and Dahan [5] found common weaknesses in the IAM model of top three players of cloud industry AWS, Google Cloud Platform (GCP) and Azure linked to dangerous permissions categorised under Assignment, Code Execution, Grants and Delegation and New Credentials.

The study [6] discussed the authentication challenges with cloud based IAMs related to multi-factor authentication (MFA) and single sign-on (SSO). MFA, a robust security measure, necessitates users to provide multiple forms of authentication to access a system or resource. It is a powerful defense against various authentication attacks, including phishing and password breaches. However, implementing and managing MFA in cloud environments can be complicated. A notable challenge is the disparity in MFA support across different cloud providers. Some providers may not offer all MFA methods, making it challenging for organisations to choose and enforce MFA consistently, especially for users utilizing diverse devices and applications.

Another study [7] discussed the challenges related to the policies and rules that dictate user permissions to cloud resources, a fundamental aspect of IAM. IAM policies are an essential security measure, as they help ensure users only have access to the resources they need. However, IAM policies can also be challenging to create, manage and understand.

While there are many studies that investigate the security of IAMs separately, on premises [8, 9] or in the cloud [10 - 12], the comparison analysis of two IAM deployment models is not widely covered in the literature. The observational analysis of existing studies was performed in [13] to compare two models in terms of cost effectiveness, ease of management, scalability and agility, constant updates, and compliance. Another study [14] as based on the surveys of professionals to get insights on usage of IAM solutions in the companies. While study tackled such questions as outsourcing of IAM vs Internal management, size of IAM team and compliance with zero trust principles, it had only 3 questions out of 8 related to IAM and they were mostly focused on collecting the statistical data.

In our study we focus on getting deeper insight through the professional experience on the usage of IAMs by companies, potential vulnerabilities and security challenges.

III. Methodology

A. Research Questions

Based on the aim of this study related to exploring security concerns and weaknesses of cloud solutions for access management, we pose the following research questions:

RQ1: What are the key challenges and vulnerabilities associated with cloud based IAMs?

RQ2: On-Premises versus Cloud, which IAM model is more secure?

RQ2 is centred on end-user experience and perception, the outcome of RQ1 will be taken as a basis for survey on perception of security by professionals.

B. Data Collection

In order to collect the data, we interviewed the cyber security professionals of leading organisations to learn from their day-to-day experience more about security weaknesses and challenges witnessed during different phases of deployment of on premises and cloud based IAM solutions.

First tour of questions was targeted to collect information about expertise of respondents, companies they work at, their domain the size and location. The distribution of respondents in terms of expertise and industry sector they represent are shown in Fig.1, the majority of respondents are holding the position of Chief Information Security Officer (CISO) and IT Security Administrator among the rest are Chief Technology Officer (CTO) and Directors.

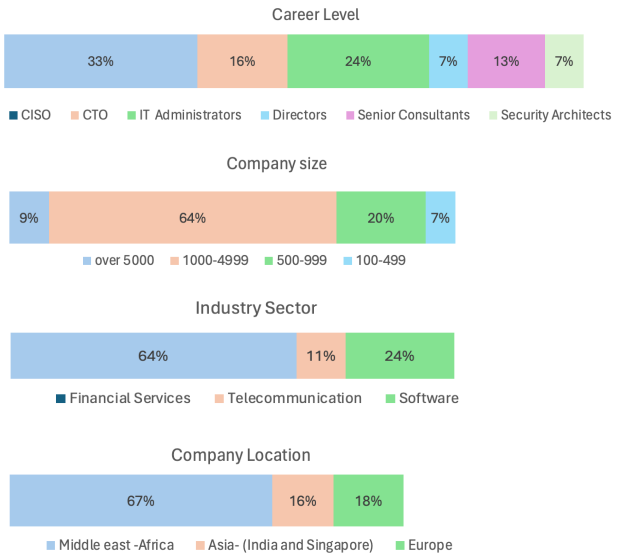

Fig. 1. Respondents data

Most respondents (78%) with more than 15 years' experience relevant to information security domain. Size reflects a number of employees in the company. The participants encompass a spectrum of technical executives and IT security practitioners, providing a well-rounded representation of organisations of diverse sizes across three industries, namely, Finance (64%), Telecom (11%), and Software production (24%).

The following set of questions were asked to respondents of different organisations working at different geographic locations and industries with the help of online collaborations tool MS teams:

- What factors influenced your organisation's decision to choose between on-premised and cloud-based IAM solutions, and how do these decisions align with your security strategy?
- What motivated your organisation's shift to cloud based IAM solutions?
- In your experience which IAM deployment model is more secure?
- As CISO, what key security challenges have you faced with IAM solutions be it on premised or cloud based?
- How has cloud based IAM impacted your organisation's security? Have you suffered a security breach in recent past?
- How does your organisation ensure compliance with regulations while using cloud based IAM, and what challenges have you encountered?
- Does your organisation deal with multiple cloud service providers?

Responses from the participants were further analysed with the help of content analysis tool Lexalytics to get a quantitative view of subject in scope.

The interviews and surveys were conducted in the period of November-December 2023. The participants were provided with written assurance to not to disclose their names at any point in time that indicates they volunteered for the survey who have different characteristic from those who denied for survey. The outcome of the survey might change with the target set of participants having different experiences and exposure.

IV. Results and Analysis

The survey identified top six challenges related to on-premises IAM deployment model illustrated on Fig.2. The challenges reported by interviewees were not having the MFA, insecure Default configurations, Lack of skillsets required to manage IAM solution securely, Poor password policies, Unpatched vulnerabilities, and compromise of Single-Sign on (SSO) leading to compromise of multiple entities.

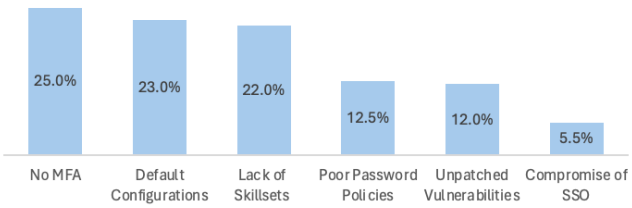

Fig. 2. Challenges with on-premise IAM solutions.

In case of cloud based IAM solutions, Default configurations, Poor management of Non- Human Identities such as Service accounts, SaaS applications, services and APIs, Poor certificate management, Poor access review, Poor API configuration and limited Log analysis with multi-cloud were among top six challenges and illustrated on Fig.3.

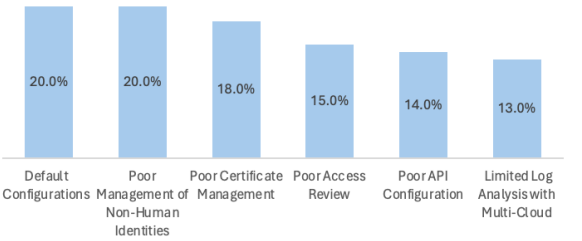

Fig. 3. Key weaknesses with cloud based IAMs.

The analysis revealed that 76% of organisations use more than two cloud service providers (CSP).

The survey results showed that 53.4% of the security professionals believe that cloud based IAM solutions are more secure in comparison to 41% who believe on premises IAM solutions are secure (Fig.4). Such a high percentage in supporting the on-premises solutions could be explained by the growing threat landscape with integration of IAM into cloud [15, 16]. Although on premise IAMs face their own challenges regarding threats and vulnerabilities, their impact is relatively small. Threats and vulnerabilities affecting cloud based IAMs have a broader reach, and the impact could be significant. In addition, given that many organisations use several CSPs, this requires an IAM solution supporting multiple cloud environments, creating a local identity for each of the application that makes it very difficult to keep track of all the entities and identities who have access.

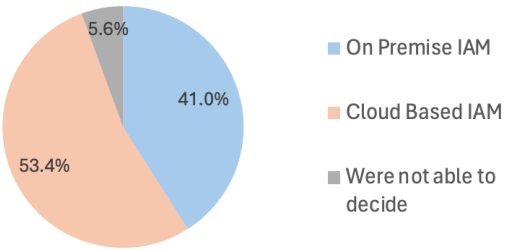

Fig. 4. Security comparison of on premise and cloud based IAM solutions.

In addition, the analysis of interviews allowed to reveal the risks associated with IAM vulnerabilities in cloud environments that we categorised in several groups such as Data Breaches and Unauthorized Access, Financial Losses, Reputational Damage, and Compliance and Regulatory Issues.

A. Data Breaches and Unauthorized Access

IAM vulnerabilities within cloud environments can have wide and severe consequences, impacting an organisation's data integrity, financial stability, reputation, and compliance to regulatory standards. One of the most pivotal outcomes of these IAM vulnerabilities resides in the data breaches. Data breaches involve unauthorized attackers getting access to confidential information [17]. These incidents can result in the disclosure or thief of customer data, substantial financial setbacks, and significant damage to the organisation's reputation. Unauthorised access into cloud resources gives attackers to steal data, disrupt operations, or launch an attack on other systems.

A data breach can result in significant financial losses. The financial burden extends far beyond immediate expenditures, as organisations may face long-term financial consequences in the form of lost business loss, decreased revenue, and legal liability. Moreover, data breaches can potentially result in fines and penalties from regulators. For instance, the European Union's General Data Protection Regulation (GDPR) empowers government agencies to impose fines of up to 4% of a company's global annual turnover or €20 million, against organisation that fails to fulfil the obligations to protect, securely store and process personal data.

B. Financial Losses

IAM vulnerabilities, when exploited, can lead to significant financial losses [18]. Beyond the direct costs associated with addressing the security incident, organisations must consider the expenses related to investigating the breach, implementing security improvements, and notifying affected customers. The organisations may be held financially responsible for any damages incurred by customers or third parties due to the breach. In addition, the organisations may face indirect financial consequences, such as decreased revenue and increased insurance premiums. Customers may lose confidence in a company that has experienced a data breach, leading to reduced business, lost sales, and long-term financial impact.

C. Reputational Damage

IAM vulnerabilities and subsequent data breaches can cause serious reputational damage to organisation [19]. Customer trust is of utmost importance in business, and data breach incidents undermine trust. Customers may view such organisations as unreliable or negligent, which can result in a loss of business, decreased market share, and a damaged brand image. Media coverage of data breaches can exacerbate reputational damage: negative headlines and news stories can spread quickly, reaching a broad audience, and further tarnishing an organisation's reputation. Restoring trust and credibility can be a long and challenging process, often requiring significant investments in public relations and marketing efforts.

D. Compliance and Regulatory Issues

The participants highlighted that the organisations are subject to strict regulatory obligations in regards to data security. The consequences of failure to comply with these mandates could be extremely serious. To clarify, consider the healthcare sector's obligation to comply with the Health Insurance Portability and Accountability Act (HIPAA), a directive that places a particular emphasis on protecting patient's health information with significant fines in case of uncomplying. Furthermore, the organisations that fail to comply regulatory benchmarks may find their ability to engage with specific government entities or other organisations severely limited, thus, in turn, limiting their market influence and potential prospects. IAM vulnerabilities in cloud environments present a combination of challenges, including data breaches, financial downturns, reputation damage, and non-compliance. Analysing the potential impact of these IAM vulnerabilities using the security risk management methods [20] highlights the importance of implementing robust security protocols and best practices. This approach is necessary to strengthen the protection of sensitive data and maintain the trust by customers and stakeholders.

V. Discussion

From the analysis conducted in the previous paragraphs, we summarize the following findings with regards to the research questions.

RQ1: What are the key challenges and vulnerabilities associated with cloud based IAMs?

The results of the survey showed that set of IAM challenges discussed by security professionals for on premise and cloud IAM solutions differs significantly. The on premise IAM deployment experiences the lack of skilled personal to skills to deploy and manage a hardware and associated software and tools. Interestingly, that the respondents in our study did not identify it as challenge for cloud solutions in contrast to the survey from Checkpoint which states that the lack of skill is the biggest challenge (58%) in managing the solutions across all cloud environments [2, 3]. None of the respondents reported the challenge with IAM related to the cost and support from the executives/investments, while the report from the Cyber Risk Alliance from March 2024 [21] reported both economic and technical barriers with adopting of IAM in general. It is obvious, that there is an economical challenge associated with cost of deployment and human resource required to manage the IAM, but our report showed that once the IAM solution is deployed other security challenges came onto the first place. All highlighted in the survey challenges are related to technical or configuration difficulties and can pose the potential vulnerabilities. Default configuration, SSL certificate management, API between company side and cloud solution, access method using MFA or SSO were reported as the areas of most concern for organisations with IAM solution.

Interpreting the research findings, it becomes apparent that IAM vulnerabilities within cloud ecosystems pose an acute predicament for organisations. The research study showed that organisations encounter not only technical issues with IAM within cloud environments, but also are imposed to set of vulnerabilities related to unauthorised access, reputational damage and compliance with regulations. Cloud service providers offer an extensive spectrum of permissions, thereby putting organisations in the position to deal with the implementation of various authentication and authorisation protocols to access the cloud which might create vulnerabilities related to misconfiguration of such protocol and requires additional work resources. The extensive capabilities of cloud settings offer many options, creating additional layer of complexity to IAM implementation. Moreover, the task of managing the permissions becomes a huge barrier. Organisations are faced with the challenges of managing multiple credentials required for various cloud services which have been already flagged by many resources [15 22, 23] including the Cloud Security Alliance IAM Working Group as one of the main challenges, thereby amplifying the vulnerability surface. Dynamic IAM policies represent a persistent challenge. The ever-evolving nature of cloud environments requires constant monitoring and adjustments to keep IAM policies and configurations up to date. Failure to do so leaves organisations vulnerable to security breaches, financial losses, reputational damage, and compliance issues.

RQ2: On-Premises versus Cloud, which IAM model is more secure?

Determining a concrete answer to RQ2 is difficult based on the limited sample size during survey. The outcome of surveys might vary with increased population. The current opinions have been divided nearly equally between on-premises (41%) and cloud solutions (53%), that could be explained the growing security threat landscape when moving to cloud environment and associated complexity of managing the multiple cloud platforms, applications and accounts. According to Forrester report [24], only 12% of organisations are fully encompassed identity management in the cloud environment.

VI. Conclusions

In summary, this study has highlighted the significant challenges and vulnerabilities related to Identity and Access Management (IAM) both on premise and in cloud settings. The research identified complexities in cloud permission models, the necessity for various methods of authentication and authorization, challenges in managing credentials, and the dynamic nature of IAM policies as primary obstacles for wider adoption of cloud based IAM solutions.

Future research in this field should investigate specific strategies and tools for mitigating IAM vulnerabilities. Additionally, exploring the evolving landscape of cloud security threats and IAM solutions is vital. The potential impact of emerging technologies like artificial intelligence and blockchain on IAM in cloud environments should also be explored. Furthermore, studying the human element in IAM vulnerabilities, including user behaviour and awareness, is a promising avenue for future research. As the cloud landscape evolves, research efforts must stay current to protect organisations from the persistent threat of IAM vulnerabilities.

References

[1] S.Saha, “Cloud IAM Market,” Future Market Insights report, REP-GB-15034, June 2022.

[2] Checkpoint, “Cloud Security Report. How organizations are leveraging cloud security strategies, technologies, and tools for operational excellence,” Cybersecurity Insiders, 2023.

[3] Checkpoint, “Cloud Security Report,” Cybersecurity Insiders, 2022.

[4] Manageengine AD360, " Three major identity security failures of the last decade," Accessed: Apr, 5, 2024. [Online]. Available: https://download.manageengine.com/active-directory-360/data-breaches-due-to-poor-iam-strategy.pdf.

[5] I. Gofman, N.Dahan, "IAM the one Who Knocks," BlackHat USA, August 6-11, 2022. [Online]. Available: https://i.blackhat.com/USA-22/Wednesday/US-22-Gofman-IAM-The-One-Who-Knocks.pdf.

[6] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574-588, 2018, doi: 10.1016/j.jestch.2018.05.010.

[7] C. Nobles, "Investigating Cloud Computing Misconfiguration Errors using the Human Factors Analysis and Classification System," *Scientific Bulletin,* vol. 27, no. 1, pp. 59-66, Jun. 2022, doi: 10.2478/bsaft-2022-0007.

[8] C. Singh, R. Thakkar, and J. Warraich, “IAM Identity Access Management - Importance in Maintaining Security Systems within Organizations,” *European Journal of Engineering and Technology Research*, vol. 8, no. 4, pp. 30-38, 2023. doi:https://doi.org/10.24018/ejeng.2023.8.4.3074.

[9] A. Cameron, and G. Williamson, “Introduction to IAM Architecture (v2),” *IDPro Body of Knowledge,* vol. 1, no. 6, 2020, doi: 10.55621/idpro.38.

[10] D. H. Sharmaa, C. A. Dhoteb, M. M. Poteyc, “Identity and Access Management as Security-as-a-Service from Clouds,” *Procedia Computer Science*, vol. 79, no. 2016, pp. 170 – 174, 2016, doi: 10.1016/j.procs.2016.03.117.

[11] I. A. Mohammed, “Cloud Identity And Access Management – A Model Proposal,” *Int. J. Innovations in Engineering Research And Technology* (IJIERT), vol. 6, no. 10, pp.1-8, 2019.

[12] A. Sandesh, P. Hrishitva, H. Sanwal, “Data Security in Cloud: A Review,” Asian J. *Advances in Research*, vol. 5, no. 1, pp. 1099-1106.

[13] L. F. Plá, N. Shashidhar, and C. Varol, "On-Premises Versus SECaaS Security Models," in *Proc. 8th Int. Symp. Digital Forensics and Sec. (ISDFS*), Beirut, Lebanon, 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116453.

[14] A. Liveretos, I. Draganov, “Identity & Access Management (IAM) and Customer IAM (CIAM): a Pulse Survey of Several Global Corporations Over Their Current Usage and Exploitation of Automated IAM and CIAM Solutions,” *Int. J. Computers,* vol. 7, pp. 95-103.

[15] A. Nachmany, S. Kulkarni, “Navigating the Top 10 Challenges in Cloud Identity and Access Management,” IAM Working Group, Cloud Security Alliance, June 2023.

[16] “Cloud Migration Optimizes Identity and Access Management," Forrester Consulting report, November 2023.

[17] R. Janakiraman, J. H. Lim, and R. Rishika, "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer," *Journal of Marketing*, vol. 82, no. 2, pp. 85-105, 2018, doi: 10.1509/jm.16.0124.

[18] “Cost of a Data Breach Report 2023,” IBM Security report, USA, July 2023.

[19] B. Wolford, "What are the GDPR Fines?," GDPR.eu, Sep. 2023, [Online]. Available: https://gdpr.eu/fines/.

[20] I. Kuzminykh, B. Ghita, V. Sokolov, T. Bakhshi, “Information Security Risk Assessment,” *Encyclopedia*, vol. 1, no. 3, pp. 602-617, 2021, doi:10.3390/encyclopedia1030050.

[21] “Navigating the identity security minefield: Practitioners share lessons learned so others can move forward,” CyberRisk Alliance report, March 2024, [Online]. Available: https://www.cyberriskalliance.com/press-release/cra-cbir-identity.

[22] Strata Identity Orchestration, “Complexity is the enemy of securing identity,” State of Multi-Cloud report 2023.

[23] I. Kuzminykh, B. Ghita, J. Such, “The Challenges with Internet of Things Security for Business,” in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Y. Koucheryavy, S. Balandin, S. Andreev, Eds., NEW2AN ruSMART 2021, LNCS, vol. 13158, Springer, Cham, doi:10.1007/978-3-030-97777-1_5.

[24] "Identity and Access Management Market Insights, 2022," Forrester Research, Inc., January 12, 2023.