Evaluation of Security and Privacy Risks, and Solutions in Web and Cloud Applications using Web Services

Lakshika Paiva,
Faculty of Engineering, University of Ottawa
lpaiv023@uottawa.ca

Dr. Imran Ahamed,
Faculty of Engineering, University of Ottawa
iahmad3@uottawa.ca

ABSTRACT

This research paper explores the pervasive risks concerning security and privacy within web and cloud applications. Examining prevalent issues in these digital landscapes, it scrutinizes risks in customer-side issues in cloud, misuse of sensitive user data and third-party infrastructure dependencies. Addressing these challenges, the paper investigates cutting-edge solutions, encompassing cloud security assessment tools, privacy policies, and resilient websites. It delves into the imperative need for proactive improvement strategies of the evaluated solutions and strategies and emphasizes the significance of comprehensive security solutions. By analyzing existing threats and innovative solutions, this study makes a significant contribution to fortify the resilience of web and cloud applications, safeguarding stakeholders against potential security breaches and privacy concerns.

I. INTRODUCTION AND PROBLEM

The surge in cloud technology adoption among enterprises, driven by its promise of innovation, agility, and competitive advantages, has fundamentally reshaped modern business landscapes. Web services often constitute an indispensable foundational element within these applications, serving as integral infrastructural pillars for their operational framework and interconnectivity. Notably, individuals possessing limited technical acumen have adeptly used these web and cloud applications, underscoring their seamless integration into daily routines.

However, this transition to web and cloud services brings forth intricate challenges in security and privacy with significant consequences. Research shows evidence that a notable concern stems from insufficient knowledge and losing control of large-scale deployments like Amazon Web Services (AWS) [1]. In addition, securing cloud operations [1] [2] can become complex with application vulnerabilities and customer side issues such as service misconfigurations and data breaches [2]. Moreover, the reliance on third-party services exposes websites to shared risks from attacks like the Mirai incident, increase the risk of service disruption [3], and risk personal data [4]. Despite existing solutions for cloud security, user privacy and security vulnerabilities, the evolving landscape of web and cloud applications demands for more research to improved approaches that encompass tactical security dimensions.

A. The Need and Research Questions

The serious consequences of security threats and attacks, operational security concerns and privacy policy violations in web and cloud brings forth a critical need to ensure the security and privacy of these applications. As a result, various research underscores the need to investigate these issues to develop a better understanding. Moreover, studies emphasize the lack of in-depth research on security issues of cloud operations due to new and complex requirements and lack of specific techniques for the cloud. Further, the scarcity of knowledge concerning these specific security attacks, third party risks, and issues in privacy policies, warrant a deeper investigation into these threats and strategies to mitigate them [3] [4].

Although there are several solutions available such as security vulnerability detection, security checks, modeling languages, redundancy solutions, and privacy and compliance policies, research emphasizes that these solutions are not sufficiently cloud centric and holistic, and many did not account for tactical security dimensions. As a result, research underscores the need to evaluate existing solutions and proactive strategies and their suitability to solve security and privacy issues that can guide improved solutions in future. Hence, this study aims to investigate the key issues and existing solutions of security and privacy to guide organizations, and accordingly sets forth the following research questions for investigation.

RQ1: What are the security and privacy risks of web and cloud applications?

RQ2: What are the solutions that address security and privacy risks of web and cloud applications?

B. Significance of this research

This research holds substantial significance for both industry and academia. The study enables industry stakeholders to comprehend the intricate security and privacy risks within web and cloud applications often involving web services, enhancing their ability to ensure user trust. Moreover, the study offers a repository of solutions and approaches, empowering industries to implement effective strategies, bolstering their security frameworks. Academically, this research contributes a comprehensive understanding of the evolving security landscape in web and cloud, guiding future research endeavors. Ultimately, the outcomes benefit industries by fostering resilient security and privacy measures and advancing academic knowledge, ensuring safer, more trustworthy web and cloud-based environments for all stakeholders.

II. METHODS

Five relevant research papers were used in this literature review. These were selected by assessing and evaluating nine research papers made available for the Web Services research project component. Suitable papers were selected by assessing the content and recurrence of themes and concepts in 'security and privacy', 'web services' and 'cloud technologies' and other sub concepts with similar variations.

III. LITERATURE REVIEW

This section critically evaluates the literature related to the research questions on security and privacy issues and their solutions and presents the evaluation in a concept-centric manner.

A. RQ1: The security and privacy risks in web and cloud applications

The literature identifies several security and privacy risks in web and cloud applications. The three primary issues revolve around risks in customer-side issues in cloud security, risks of third-party dependencies and hidden privacy risks (Table I) are critically evaluated in this section.

TABLE I
CONCEPT MATRIX FOR SECURITY AND PRIVACY RISKS

Articles	Concepts		
	Risks in customer- side issues in cloud security	Risks of Third-party service dependencies	Hidden privacy risks that harvest user information
Assessing discrepancies between network traffic & privacy policies of public sector web se… [4]		✓	✓
Automated Security Assessments of Amazon Web Services Environments [2]	✓		
Security and Cost Optimization Auditing for Amazon Web Services [1]	✓		
Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Se… [5]			✓
Analyzing Third Party Service Dependencies in Modern Web Services… [3]		✓	

1) Risks in customer-side issues in cloud security

Majority of the literature presents risks in customer side issues in cloud security [1] [2] owing to operational aspects. Supporting this, Gartner predicts that by 2025, 99% of all cloud breaches will be customer side lapses [6]. Consequences are severe as users can lose control of the cloud infrastructure [1] and face security incidents.

In the cloud, risks arise from customer-side issues due to insufficient knowledge in operating cloud services, difficulty in management of cloud services [1], service misconfigurations, data breaches and insecure changes [2], identity and access management problems, and account hijacking [7]. Moreover, research claims that "a crux with customer-side cloud security is combinations of traditional security vulnerabilities enhanced with cloud-native attacker tactics" [2], which cause security breaches that can lead to vulnerability chains [2] causing catastrophic impact on cloud deployments such as the Tesla [8] and Uber breaches [9].

Similarly, new, and complex requirements of infrastructure and working conditions [1] also add to cloud security concerns as users lack the knowledge to manage such scale and evolving complexity. As a result, many users are concerned if their services are secure [2]. While these top five issues are synonymous with the Cloud Security Alliance top five threats, a key limitation is that the findings are mostly discussed in the perspective of AWS cloud.

Although migrating to the cloud is a very common trend, customer-side mistakes commonly arise from lack of knowledge among users. The issues mainly point to operational aspects and complexity in managing cloud deployments which may give rise to security incidents. Further, a key finding is that vulnerability chains are often under analyzed and need more attention.

2) Hidden privacy risks that harvest user private information

Literature points to hidden security risks which are not apparent to users, such as discrepancies in privacy policies, and phishing in the Dark Web, which in turn harvests users' privacy-sensitive information.

Privacy risks which exploit personal information are often hidden in functions within online applications, like third party analytics services which process user information with privacy policies in place, guaranteeing anonymity. However, a study analyzing such network traffic data claims that there are discrepancies in privacy policies and actual data transmitted, and those policies lack transparency and clarity [4]. Moreover, although these data like IP, browser, operating system, and viewed contents when acting alone are not personally identifiable, by combining these data the system formed a user-identifiable digital fingerprint [4]. As a result, user privacy and anonymity are abused without user knowledge and consent.

Similarly, the concept of anonymity in the Dark Web is exploited by phishing websites or hidden web services [5]. However, the approach to gathering personal data is different compared to third parties because users are deliberately deceived in the Dark Web. Delving into details, legitimate and phishing websites on the Dark Web are visually and functionally identical, but their databases are different, which helps to harvest users' personal and payment information easily. Oftentimes, attackers diligently spread fake information on the Dark Web to gain higher popularity [5], which makes phishing websites to mislead users easily.

However, the study [4] on network traffic covered only clearly detectable personal data, so encrypted data may have gone undetected. In the Dark Web study [5], the approach had limitations, for instance websites were compared manually and the analysis was incomplete because many domains were unclassified.

In summary, hidden risks in these websites abused user anonymity in a different manner, but it confirms the privacy risk to users' sensitive information. Further, both occurrences claim to lack in-depth research work, however, they cause a significant impact on the privacy of individuals.

3) Risks in Third Party Service dependencies

Much of the literature focuses on the use of third-party service dependencies which give rise to security and privacy risks such as leaking of sensitive personal data [4], and shared risks such as security attacks like Distributed Denial of Service (DDoS) attacks and Certificate Revocation Errors [3] on dependent websites.

Third party dependencies can cause a variety of security and privacy risks. While third-party analytics service dependencies dealing with large amounts of data can cause user privacy violations [4], infrastructure level third party dependencies cause system unavailability [3] resulting from DDoS attacks. A significant privacy risk is presented by a study in the Finnish public sector, demonstrating how anonymous user information like IP, browser, operating system, and viewed contents were leaked outside the actual web service by 90% of its services. In turn they were effectively used in combination to profile and identify a user (i.e. digital fingerprint) [4]. While it highlights a deviation from normal personal data like name and date of birth, it is an approach equally harmful to user privacy. However, this research only covers the clearly detectable personal data, and not encrypted data.

Comparatively, a study on infrastructure level dependencies emphasizes that the top 100,000 websites critically depend on three provider types, Domain Name Systems (DNS), Content Delivery Networks (CDN) and Certificate Authorities (CA), and the use of these third-party services is highly concentrated among the top three providers and has the potential to make 50-70% websites unavailable [3] from a security attack, which is a significant impact. Notably, the study further found that indirect dependencies amplify provider concentration and impact [3]. However, the study focuses only on dependencies on landing pages, and disregards region-specific dependency structures, dependencies between web-services and lacks measuring physical and network infrastructure dependencies.

Overall, third-party dependencies cause notable security and privacy risks. A relatively overlooked phenomenon emerges which is, forming a digital fingerprint of a person using non-identifiable but personal digital information. This is executed by third parties without the user's knowledge and consent, although privacy policies assure user anonymity. These issues are significant and need immediate attention.

In summary of this section, it is notable that key risks of security and privacy include customer-side issues in the cloud, dependency on third party services and hidden user privacy risks in web and cloud applications. They all cause significant security incidents to users and developers and importantly most concerns lack research as they are emerging topics in the web and cloud landscape.

B. RQ2: Solutions that address security and privacy in web and cloud applications

The literature presents solutions that address security and privacy risks in web and cloud applications including cloud security assessment tools, privacy policies and resilient and redundant websites. In this review, we evaluate three existing solutions (Table II) that emerged from the research.

TABLE II
CONCEPT MATRIX FOR SECURITY AND PRIVACY SOLUTIONS

Articles	Concepts		
	Cloud security assessment tools	Improved privacy policies	Website resiliency and redundancy
Assessing discrepancies between network traffic & privacy policies of public sector web se… [4]		✓	
Automated Security Assessments of Amazon Web Services Environments [2]	✓		
Security and Cost Optimization Auditing for Amazon Web Services [1]	✓		
Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services… [5]		✓	
Analyzing Third Party Service Dependencies in Modern Web Services… [3]			✓

1) Cloud security assessment and auditing tools

Much of the literature presents cloud security assessment or auditing tools that perform audits, security checks and apply compliance using third party tools [1] and domain specific modeling languages [2].

There are several security assessment-tools for cloud environments. The popular Dome9 tool applies rules of leading security organizations such as CIS and PCI DSS to audit cloud security, however the cost is significant for large businesses [1]. To overcome costs, this study designs a similar tool with security audit functions for AWS where users can detect vulnerabilities and compliance policies [1]. The tool is free and requires updates with new developments. Similarly, another study evaluates several automated security assessment tools for AWS, both open source and commercial, but these tools often focus on general network security [2]. Equally, AWS itself provides numerous security services for EC2 and vulnerability assessments [2] however, security incidents occur regardless of the large selection of services and tools.

Contrastingly, another research looks at a different approach with cloud modeling languages but states they account for applications security but not tactics and techniques or focused on strategic and requirements [2]. Despite its richness, cloud modeling work serves a different purpose to modeling threats. As a result, the

research proposes a domain-specific modeling language (DSL) focusing on automatic assessment of AWS by simulating attacks and distinguishes itself by not relying on users to model attacks and threats themselves [2]. The language is advanced in the sense it can reason out security by constructing and traversing attack graphs. A major drawback is, when attacker tactics change the environment, the attack graphs could change to reflect that after computation [2] and it could not always simulate tactics.

In summary, there is a lack of specialized but holistic security assessment methods for cloud, and none of the existing solutions and tools capture the structural relationships and chains of vulnerabilities in cloud environments. A differentiated approach to security assessment tools is emerging with DSL enhancing the automatic security assessments with representation of attacker behaviors with security attack-defense graphs.

2) Improved policies and techniques for protecting user privacy

The literature presents several approaches to safeguard privacy and sensitive information of users through the means of privacy policies, and other procedures.

Privacy policies are beneficial in informing users what information is collected and how it is used by websites and their third parties, however there are several drawbacks. A study on network traffic to third parties claims that privacy policies had discrepancies with reality, and lacked transparency and clarity, and importantly missed who processed personal data [4]. Moreover, they use technical jargon which is incomprehensible by non-technical users and suffer from extensive scopes and vague expressions [4]. Although there are regulations like GDPR and authorized bodies like the European Commission to give clarity on personal data, in the actual implementation process developers lack understanding and web service maintainers struggle to write clear and concise privacy policies [4]. Notably, this study was limited to detectable personal data, and client side, and lacked legal analysis of privacy policies. However, privacy policies were understudied in evaluated research.

In comparison, another study proposed a traditional phishing mitigation technique to secure sensitive user information, that is to “use a completely random onion domain so that its visitors give up on memorizing the domain and use a bookmark instead” [5], however this research did not propose newer or other policies on protecting personal data in the Dark Web from a user or development perspective.

Overall, privacy policies and phishing mitigation techniques were found to protect personal data. However, these approaches either had significant issues, or lacked detail. Furthermore, the objective of privacy policies was only achieved partially, and they can improve in transparency, clarity, and simplicity.

3) More resilient and redundant websites

Few of the literature highlights the need to build more resilient and redundant websites to reduce risks of potential unavailability caused by security attacks on dependent third-party services [3].

Third-party services like analytics, DNS and CDN offer better quality of service and higher capacity, which smaller websites cannot afford on their own [3]. However large-scale security risks like DDoS attacks on third parties may lead to prolonged unavailability like the Mirai incident. Research shows evidence that use of third-party services is highly concentrated among the top three providers and has the potential to make 50-70% websites unavailable [3] during a security incident. As a result, websites need to build more resilience and redundancy, especially those which use infrastructure level dependencies such as DNS, CDN and CA [3]. Although many of these party providers have multiple points of presence [3], they are not immune to security attacks, errors, and failures. Furthermore, website providers need to understand the indirect dependencies of third-party services they use as they may be indirectly exposed to security threats. For instance, if a website uses multiple CDN providers but those CDNs use the same DNS provider. Similarly, if indirect dependencies of a website are also redundantly provisioned, it makes the website less prone to outages [3].

All in all, the trend towards the use of third-party services is increasing [3] irrespective of security threats, hence resiliency and redundancy in websites are critical to implement in websites, especially if third-party services are involved. Unfortunately, this area lacked research for comparison with wider research.

In conclusion of this section, there are several solutions proposed to reduce risks of security and privacy issues including implementing cloud security assessment tools with more specialization and holistic approach, improved privacy policies to secure user data, and building resiliency and redundancy in websites.

IV. DISCUSSION AND FINDINGS

In this section, we discuss the key findings, implications, and gaps in research, and conclude on the study.

RQ1: What are the security and privacy risks of web and cloud applications?

The literature highlights risks from customer-side issues in the cloud, dependency on third-party services and hidden privacy risks that harvest users' private information as key security and privacy risks in web and cloud applications that can lead to security incidents that lead to catastrophic consequences. Some of these include losing control of a cloud deployment, unavailability of services and abuse of user anonymity on the web leading to collection of user-sensitive information without consent, respectively.

4) Hidden privacy risks that harvest user private information

RQ2: What are the solutions that address security and privacy risks of web and cloud applications?

Literature evaluation of security and privacy solutions provide valuable insights. There are many solutions proposed to proactively reduce these risks, including cloud security assessment tools, improved privacy policies and building resiliency and redundancy in websites relying on third-party services. It was clear that cloud security assessment tools evaluated were primarily geared towards AWS, and only a few solutions were applicable across other cloud providers. Moreover, privacy policies of web and cloud applications demonstrate a need for significant improvement in terms of comprehensiveness and simplicity, especially for non-technical users. Adding to that, the process of writing privacy policies highlights the need to align them with the actual implementation and focus on non-harmful usage of personal data. Furthermore, resiliency and redundancy are most applicable for web and cloud applications using third-party infrastructure services and needs more visibility into indirect dependencies of third parties to avoid unforeseen security and privacy risks.

Combined implications

Primarily, the security and privacy risks identified in RQ1 can be addressed by applying the solutions discussed in RQ2, with major or minor improvements. First, the risks from customer-side security issues occurring due to insufficient knowledge and difficulty in operation of cloud services can be overcome by using a cloud security assessment tool like the DSL which helps to monitor threats and identify potential attack-defense paths, proactively. Importantly, web and cloud applications should evaluate and select the most appropriate solution or a combination of approaches for their websites to monitor and manage security risks proactively. Second, although anonymous user data sent to third-party analytics are converted into a digital fingerprint of the user, these actions can be governed with modified and improved privacy policies with the combination of privacy regulations and frameworks like GDPR, improved developer understanding on implementation and the help of policy writers and web service maintainers. Third, the risk of third-party infrastructure level service dependencies can be mitigated by implementing more resilient and redundant web and cloud applications.

There was little to no discussion on significant solutions proposed from a developer or user perspective to handle phishing attacks in the Dark Web or combat abuse of user anonymity, hence this needs more research.

Web Services was a common theme in most of the literature. Research shows the widespread adoption of web services in the Government, public sector, and private companies. They offer benefits to stakeholders by introducing scalability, interoperability, and ease of maintenance especially in cloud environments.

More and more websites are migrating to the cloud irrespective of security and privacy risks including vulnerability chains, complexity, or lack of knowledge about the cloud due to its benefits and efficiencies. Government, public sector, and private enterprises need to equally be aware of the variety of risks and take the right path to adoption and maintenance of cloud applications and minimize security and privacy risks.

Gaps and limitations

Although security risks are a key theme in the study, security incidents causing vulnerability chains in the cloud environment lack in-depth research and specialized solutions in the studies. There is a clear need to understand the excessive use of analytics by third parties and its impact on user privacy however, there is lack of research coverage on this area.

As for limitations, the studies discussing security assessment solutions for AWS cloud-based requirements, gave very little consideration to other popular cloud platforms like Azure and Google Cloud or smaller cloud providers. Moreover, the studies analyzing user-sensitive information and privacy concerns did not consider sharing user data beyond geographical locations (such as out of Europe) and relevant regulations.

V. CONCLUSION AND FUTURE RESEARCH

In conclusion, the study presents a set of security and privacy risks like customer-side issues, hidden privacy risks that harvest user information and risks in third party dependencies, that can be mitigated using solutions such as cloud security assessment tools, privacy policies and resilient and redundant websites as evaluated in this study. The findings from this research guide the direction and security strategies, tactics and operations of Government, public sectors, and private enterprises to build more robust and resilient security and privacy frameworks that safeguard users as well as organizations.

As recommendations, future research can focus on designing solutions to combat security vulnerability chains in cloud environments addressing its complex needs. Moreover, privacy policy research can assess the legal framework under which anonymous user data can be combined to form users' digital fingerprints. Further, research studies can center on developing comprehensive third-party dependency structures, empowering website administrators to make informed decisions when selecting new service providers.

VI. REFERENCES

References of selected papers:

[1] A. Q. Huy and P. D. Hung, "Security and Cost Optimization Auditing for Amazon Web Services," in *Proceedings of the 2nd International Conference on Software Engineering and Information Management*, in ICSIM '19. New York, NY, USA: Association for Computing Machinery, Jan. 2019, pp. 44–48. doi: 10.1145/3305160.3305181.

[2] V. Engström, P. Johnson, R. Lagerström, E. Ringdahl, and M. Wällstedt, "Automated Security Assessments of Amazon Web Services Environments," *ACM Trans. Priv. Secur.*, vol. 26, no. 2, p. 20:1-20:31, Mar. 2023, doi: 10.1145/3570903.

[3] A. Kashaf, V. Sekar, and Y. Agarwal, "Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?," in *Proceedings of the ACM Internet Measurement Conference*, in IMC '20. New York, NY, USA: Association for Computing Machinery, Oct. 2020, pp. 634–647. doi: 10.1145/3419394.3423664.

[4] T. Heino, R. Carlsson, S. Rauti, and V. Leppänen, "Assessing discrepancies between network traffic and privacy policies of public sector web services," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, in ARES '22. New York, NY, USA: Association for Computing Machinery, Aug. 2022, pp. 1–6. doi: 10.1145/3538969.3539003.

[5] C. Yoon, K. Kim, Y. Kim, S. Shin, and S. Son, "Doppelgängers on the Dark Web: A Large-scale Assessment on Phishing Hidden Web Services," in *The World Wide Web Conference*, in WWW '19. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 2225–2235. doi: 10.1145/3308558.3313551.

References of 'cited works of other authors' taken from within, the above papers:

[6] K. Panetta, "Is The Cloud Secure," Gartner. Accessed: Nov. 27, 2023. [Online]. Available: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

[7] Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven | CSA," 2019. Accessed: Nov. 26, 2023. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

[8] R. Browne, "Hackers hijack Tesla's cloud system to mine cryptocurrency," *CNBC*, 2018. [Online]. Available: https://www.cnbc.com/2018/02/21/hackers-hijack-teslas-cloud-system-to-mine-cryptocurrency-redlock.html

[9] D. Lee, "Uber concealed huge data breach," *British Broadcasting Corporation*, 2017. Accessed: Nov. 26, 2023. [Online]. Available: https://www.bbc.com/news/technology-42075306