IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Cloud Security Penetration Testing Using Prowler

Mohammadkaif Aatar[1], Mohammadarsh Khan[2], Bankar Prashant[3], Prof.S.S.Dale[4], Dr. V. S. Ranmalkar[5], Dr. P. M. Patil[6]
Department of Computer Applications (MCA)[1-6]
Adsul's Technical Campus, Chas, Ahilyanagar

Abstract: *Cloud platforms now host the applications, databases, storage and business services on which many organizations depend. Cloud infrastructure offers scalability and flexibility, but improperly configured security controls can introduce risks such as unauthorized access and data exposure. Misconfiguration, rather than software defects alone, is a frequent cause of such weaknesses. This research proposes a cloud security assessment framework for Amazon Web Services (AWS) built around Prowler, an open-source cloud security assessment tool. The framework is demonstrated in a controlled AWS test environment in which a configuration weakness is deliberately introduced, detected through automated checks, validated manually through the AWS Management Console, analyzed for potential impact, and addressed through remediation guided by established cloud security best practices. The study emphasizes the importance and practical feasibility of evaluating cloud security before configuration weaknesses contribute to security incidents. It is a limited proof of concept: it does not establish the security of any complete cloud account, and its observations are qualitative.*

Keywords: AWS Security, Cloud Security Assessment, Prowler, Security Misconfiguration, Identity and Access Management, Least Privilege, Cloud Security Posture

I. INTRODUCTION

Applications, databases, business services and sensitive information are increasingly hosted on cloud platforms. NIST defines cloud computing as a model for on-demand network access to a shared pool of configurable computing resources [1]. Because the provider and the customer share security responsibilities, customers remain responsible for securing what they configure, including identities, permissions, data and network settings [2], [12].

Cloud security misconfigurations may arise from excessive Identity and Access Management (IAM) permissions, incorrect access-control configurations, inadequate identity security controls, insecure storage or network configurations, inadequate security monitoring, and failure to follow cloud security best practices. The Cloud Security Alliance has listed misconfiguration and inadequate change control among the top threats to cloud computing [8]. Reviewing such settings by hand is slow and difficult to repeat consistently.

Automated assessment tools help customers inspect cloud configuration repeatedly and consistently. Prowler is an open-source tool that evaluates cloud accounts against a library of security checks [6]. This research examines how Prowler can be used within a controlled AWS environment to identify potential configuration weaknesses, support security review, and guide remediation according to established best practices, with the aim of demonstrating the importance and practical feasibility of cloud security testing.

II. LITERATURE REVIEW

NIST's definition of cloud computing [1] and its guidelines on public cloud security and privacy [2] establish the vocabulary of service and deployment models and stress that customers must evaluate and manage the risks of outsourced resources. Surveys of cloud security issues [11] and of security assurance in the cloud [10] review threats and controls and motivate continuous, evidence-based assessment rather than one-time review.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 7, October 2026 Impact Factor: 8.2

For identity and access management, AWS documents security best practices that include applying least-privilege permissions, requiring multi-factor authentication, and preferring temporary credentials [4]. Least privilege has long been recognized as a design principle for protection mechanisms [7] and appears as a control family in NIST SP 800-53 [3]. The AWS Well-Architected Framework Security Pillar encourages the use of detective controls [5].

These sources define good practice, but they are general by nature. They do not by themselves show a small team how a configuration weakness appears in an assessment tool's output, how that output can be confirmed against the cloud console, and how the result maps to remediation. A further limitation is that an automated tool reports only on the conditions its checks cover [6]. This research addresses that gap with a compact, reproducible assessment workflow and does not claim to improve on existing tools.

III. PROBLEM STATEMENT

Cloud environments can contain misconfigured permissions and security controls that increase the risk of unauthorized access, data exposure and excessive privilege. Manual configuration review is time-consuming and hard to repeat, and security teams need a structured way to assess configuration before weaknesses are exploited. This study asks a deliberately narrow question: can an automated assessment tool such as Prowler, in a controlled AWS test environment, identify a deliberately introduced configuration weakness, and can that finding be confirmed manually and used to guide remediation? The study does not attempt to solve cloud security in general or to assess a complete production account.

IV. OBJECTIVES

The primary objectives of this research are:

- To investigate the importance and practical feasibility of AWS cloud security assessment.
- To establish a controlled AWS environment for security testing.
- To introduce a selected security misconfiguration in that environment.
- To use Prowler to identify the misconfiguration through automated security checks.
- To validate the automated finding manually through the AWS Management Console.
- To analyze the potential security impact of the weakness.
- To recommend remediation aligned with cloud security best practices.
- To evaluate remediation through a subsequent assessment.
- To identify limitations and possible extensions of the framework.

V. RESEARCH METHODOLOGY

The proposed methodology consists of the following phases:

Phase 1: AWS Test Environment Preparation. Prepare an isolated AWS account used only for the experiment, together with the AWS Management Console and Prowler.

Phase 2: Controlled Misconfiguration. Introduce a known, deliberately selected configuration weakness. A known weakness provides ground truth against which detection can be judged.

Phase 3: Automated Assessment. Run Prowler against the environment to execute its security checks.

Phase 4: Finding Identification. Inspect the output for failed checks and record the affected resources.

Phase 5: Manual Validation. Confirm in the AWS Management Console that the reported condition genuinely exists.

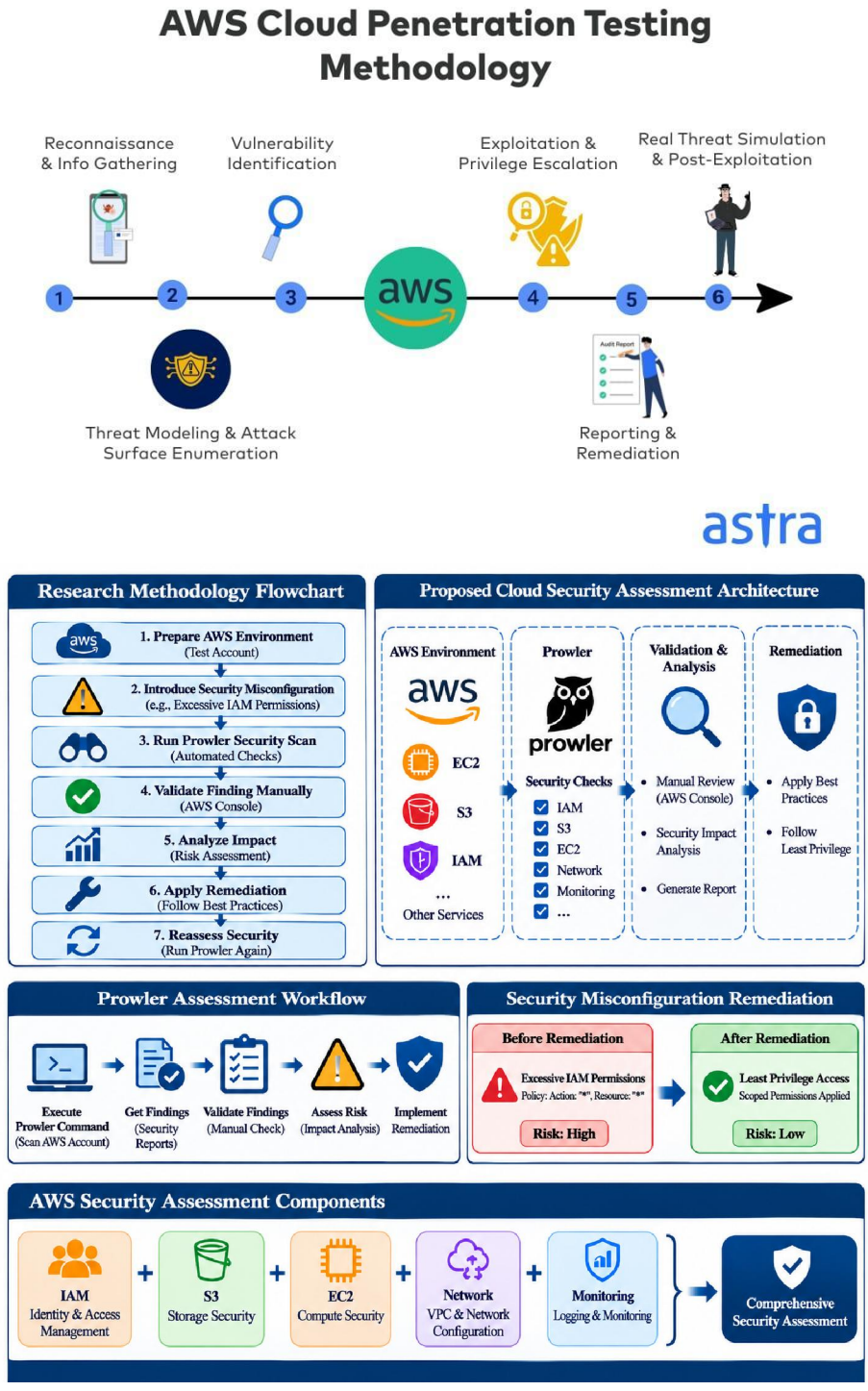
Phase 6: Risk Analysis. Reason about the potential security impact of the confirmed condition against established principles such as least privilege.

Phase 7: Remediation Recommendation. Recommend corrective action based on cloud security best practices.

Phase 8: Re-assessment. Repeat the assessment after remediation and compare the outcome with the earlier result.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

VI. PROPOSED CLOUD SECURITY ASSESSMENT FRAMEWORK



Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

The proposed framework consists of the following stages:

AWS Test Environment
↓
Controlled Misconfiguration
↓
Automated Assessment (Prowler)
↓
Finding Identification
↓
Manual Validation (AWS Management Console)
↓
Security Risk Analysis
↓
Remediation Recommendation
↓
Re-assessment
↓
Security Assessment Report

The framework begins with an isolated environment in which a known weakness is introduced. Prowler executes automated checks, and failed checks are recorded with the affected resources. Each finding is confirmed manually in the console so that the reported condition is verified rather than assumed. The confirmed finding is analyzed for potential impact, remediation is recommended according to best practices, and a repeat assessment compares results before and after remediation. The final report documents scope, evidence, limitations and actions.

VII. SAMPLE CLOUD ENVIRONMENT DESCRIPTION

This research uses a small, controlled AWS environment designed for learning and demonstration rather than production use. The environment represents areas commonly examined in cloud security reviews:

- Identity and access management (users, permissions and policies)
- Access-control configuration
- Identity security controls such as multi-factor authentication and credential management
- Storage configuration
- Network configuration
- Security monitoring and logging

These areas provide a suitable basis for evaluating how automated checks report configuration weaknesses. The specific configuration, resources and account details of the laboratory environment are intentionally not disclosed in this paper.

VIII. TOOLS AND TECHNIQUES EVALUATED

The following approaches are considered in this study:

Manual AWS Configuration Review. A reviewer inspects settings directly in the AWS Management Console. This gives direct validation but is slow and hard to repeat.

Automated Assessment with Prowler. Prowler runs a library of security checks and reports results per check [6]. It is repeatable but reports only on the conditions its checks cover.

Prowler with Manual Validation (this study). Automated detection is combined with console confirmation of each finding, giving both repeatable detection and verified evidence.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Assessment, Remediation and Re-assessment. The assessment is repeated after remediation to allow a before-and-after comparison.

IX. EXPERIMENTAL SETUP

Platform and Tools

Amazon Web Services: controlled test account

Prowler: open-source cloud security assessment tool

AWS Management Console: manual validation of findings

Evidence Collected

Assessment output from Prowler

Console evidence confirming the validated condition

Evaluation Criteria

Because this is a limited proof of concept, evaluation is qualitative and uses the following criteria:

Detection: whether the deliberately introduced weakness was reported by the automated assessment.

Validation: whether the manual console check confirmed the reported condition.

Impact Analysis: whether the potential consequences were identified and explained. Remediation Guidance: whether the recommended action follows established best practice.

Repeatability: how easily the assessment can be re-run and compared.

X. RESULTS AND DISCUSSION

The framework was exercised in a controlled AWS environment. The automated assessment reported the deliberately introduced weakness, and manual inspection in the AWS Management Console confirmed that the reported condition was present. The agreement between the automated output and the console supports the practical feasibility of this approach for the tested case.

The potential consequences of this class of weakness are discussed as risks, not as incidents: configuration weaknesses can enlarge the impact of a credential compromise, permit unintended access, or expose data. In a laboratory account the practical exposure is small, but the same condition in a production account would be of higher concern.

Remediation is recommended in line with AWS guidance, which advises granting only the permissions required for a task, enabling multi-factor authentication and preferring temporary credentials [4]. A repeat assessment should then be run and compared with the earlier result, together with a console check.

Limitations. Only one misconfiguration was examined, and only a small set of checks was considered. Passing checks do not show that an account is secure, and not every AWS control was tested. No detection rate, timing or other quantitative measure was collected, and the findings should not be generalized beyond the controlled environment.

XI. CONCLUSION

This research motivated cloud security assessment as cloud platforms carry more of an organization's workloads, and it demonstrated a Prowler-based assessment workflow in a controlled AWS environment. Automated checks identified a deliberately introduced weakness, and manual validation confirmed it, showing that automated detection and console verification can be combined into a practical, repeatable review process. The study supports the feasibility of automated cloud security assessment for the tested case. It does not show that an environment is fully secure or that other misconfigurations would be found.

Future Work

Future research can extend this work by:

Performing and reporting remediation with a verified re-assessment.

Assessing storage configurations, network exposure and security groups.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 7, October 2026
Impact Factor: 8.2

Adding multi-factor authentication, credential and access-key checks.
Verifying logging and encryption-related checks.
Running repeated, scheduled assessments with historical scan comparison.
Automating report generation.
Extending the framework to additional accounts and environments and integrating it with cloud security posture management workflows.

REFERENCES

1. P. Mell and T. Grance, "The NIST definition of cloud computing," NIST, Gaithersburg, MD,USA, SP 800-145, Sep. 2011.
2. W. Jansen and T. Grance, "Guidelines on security and privacy in public cloudcomputing," NIST, SP 800-144, Dec. 2011.
3. Joint Task Force, "Security and privacy controls for information systems andorganizations," NIST, SP 800-53 Rev. 5, Sep. 2020.
4. Amazon Web Services, "Security best practices in IAM," AWS IAM User Guide.[Online]. Available: https://docs.aws.amazon.com/IAM/latest/UserGuide/bestpractices.html
5. Amazon Web Services, "AWS Well-Architected Framework: Security Pillar." [Online]. Available: https://docs.aws.amazon.com/wellarchitected/latest/securitypillar/welcome.html
6. Prowler, "Prowler Documentation." [Online]. Available: https://docs.prowler.com
7. J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems,"Proc. IEEE, vol. 63, no. 9, pp. 1278-1308, Sep. 1975.
8. Cloud Security Alliance, "Top threats to cloud computing: Pandemic Eleven," 2022.
9. OWASP Foundation, "Web Security Testing Guide (WSTG)." [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/
10. D. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From security to assurance in the cloud: A survey," ACM Comput. Surv., vol. 48, no. 1, Art. 2, 2015.
11. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models ofcloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, 2011.
12. Amazon Web Services, "Shared responsibility model." [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/