JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Simulation of Attacks on Cloud Environments: A Comprehensive Review and Framework

[1]**Ms. Vaishnavi Sunil Patil,** [2]**Prof. Y.B.Jadhao**
[1]Student, CSE Department, Padm. Dr. V.B. Kolte,College of Engineering, Malkapur
[2]Assistant Professor, CSE Department, Padm. Dr. V.B. Kolte,College of Engineering, Malkapur

Abstract: Cloud computing has revolutionized IT infrastructure, offering on-demand access to computing resources. However, cloud environments are susceptible to various security threats. This paper presents a comprehensive review of simulation techniques for evaluating the impact of attacks on cloud environments. We discuss different attack types, simulation tools, and key metrics for assessing security posture. Additionally, we propose a comprehensive framework for simulating attacks on cloud environments, combining existing approaches and addressing their limitations. This framework can guide researchers and practitioners in designing and conducting effective simulations to strengthen cloud security.

Keywords: Cloud Security, Simulation, Attacks, Security Assessment, Framework

I. INTRODUCTION

Cloud computing has emerged as a dominant paradigm in IT infrastructure, providing on-demand access to resources like virtual machines, storage, and software. Organizations leverage cloud services for scalability, cost-effectiveness, and ease of management. However, cloud environments are inherently more complex than traditional on-premise deployments, introducing new security challenges. It offers numerous advantages, but it also introduces new security risks. One significant threat is brute-force attacks, where attackers systematically try various login credentials (passwords, usernames) to gain unauthorized access to accounts. Cloud environments are particularly vulnerable due to:

- **Centralized Storage:** Sensitive data, including credentials, is often stored centrally in the cloud, making it a prime target for attackers.
- **Increased Attack Surface:** Cloud environments offer multiple access points (web interfaces, APIs), expanding the attack surface for brute-force attempts.
- **Remote Access:** Cloud resources can be accessed from anywhere, potentially opening up additional avenues for attackers to exploit weak security practices.

Cloud computing has revolutionized financial services, enabling efficient and scalable platforms for credit card processing. However, transitioning sensitive financial data and operations to the cloud introduces new security concerns. One significant challenge arises from credit card faults, encompassing:

- **Intentional Attacks:** Malicious actors might exploit vulnerabilities in cloud infrastructure or applications to manipulate or steal credit card data. Examples include injection attacks, man-in-the-middle attacks, and data breaches.
- **System Malfunctions:** Hardware or software failures, such as disk errors, network outages, or software bugs, can lead to unintended data loss, corruption, or unauthorized access.

II. LITERATURE SURVEY

Credit card fraud detection has drawn a lot of research interest and a number of techniques, with special emphasis on data mining, have been suggested. Gosh and Reilly [1] have developed fraud detection system with neural network. Their system is trained on large sample of labeled credit card account transactions. These transactions contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and non receive issue(NRI) fraud.

E. Aleskerov et al. [2] present CARDWATCH, a database mining system used for credit card fraud detection. The system is based on a neural learning module and provides an interface to variety of commercial databases.

Dorronsoro et al. [3] have suggested two particular characteristics regarding fraud detection- a very limited time span for decisions and a large number of credit card operations to be processed. They have separated fraudulent operations from the normal ones by using Fisher's discriminant analysis. Syeda et al. [4] have used parallel granular neural network for improving the speed of data mining and knowledge discovery in credit card fraud detection. A complete system has been implemented for this purpose.

Chan et al. [5] have divided a large set of transactions into smaller subsets and then apply distributed data mining for building models of user behavior. The resultant base models are then combined to generate a meta-classifier for improving detection accuracy. Chiu and Tsai [7] consider web services for data exchange among banks. A fraud pattern mining (FPM) algorithm has been developed for mining fraud association rules which give information regarding the new fraud patterns to prevent attacks.

III. ATTACK TYPES ON CLOUD ENVIRONMENTS

Cloud environments are vulnerable to a wide range of attack vectors, including:

- **Denial-of-Service (DoS) Attacks:** These attacks aim to disrupt normal service by overwhelming resources, causing service unavailability. Examples include Distributed DoS (DDoS) attacks that flood the cloud with malicious traffic.
- **Injection Attacks:** Malicious code is injected into user input or system vulnerabilities, allowing attackers to gain unauthorized access or manipulate data. Examples include SQL injection and cross-site scripting (XSS).
- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept communication channels to steal sensitive information or manipulate data in transit.
- **Data Breaches:** Attackers gain unauthorized access to sensitive data stored in the cloud, compromising confidentiality and integrity.
- **Privilege Escalation:** Attackers exploit vulnerabilities to gain higher privileges within the cloud environment, potentially leading to complete system control.

A. *Simulating attacks on cloud environments offers numerous benefits, including:*

- **Evaluating the effectiveness of security controls:** Simulations can help assess the ability of existing security measures to detect and mitigate various attacks.
- **Identifying potential vulnerabilities:** Simulated attacks can uncover weaknesses in system design or configuration before they are exploited by real attackers.
- **Validating security policies and procedures:** Simulations can test the effectiveness of security policies and procedures to ensure they are adequate and actionable during an attack.

B. Several simulation techniques are employed to assess security posture in cloud environments:

- **Network simulations:** These techniques reproduce network behavior and traffic patterns to analyze the impact of DoS attacks, network intrusion attempts, and other network-based threats. Popular tools include CloudSim and CloudAnalyst.
- **Workload simulations:** These techniques mimic user behavior and resource utilization to evaluate the performance of cloud systems under stress or attack scenarios. Tools like GridSim and iFogSim can be used for workload simulations.
- **Vulnerability scanning simulations:** These simulations scan cloud environments for known vulnerabilities and assess their potential impact on security. Tools like OpenVAS and Nessus are commonly used for vulnerability scanning simulations.

IV. RESEARCH OBJECTIVES

- ***To demonstrate the generation of credit card number and its comprise result for attacks***
- ***To simulate the attacks through multiple profile***
- ***To identify the difference of previous, comprise of card numbers and current***
- ***To generate the comprise numbers and stored for record in cloud through encryption process***

A. Algorithm used (Random Forest Algorithm)

Random Forest is a supervised machine learning algorithm that uses a group of decision tree models for classification and making predictions. Each decision tree is a weak learner because they have a low predictive power. It is based on ensemble learning, which uses many decision tree classifiers to classify a problem and improve the accuracy of the model. As a result, the random forest employs a bagging method to generate a forest of decision trees.

Step 1: (DATA PREPARATION)

Credit card information has been sent to the server over the network. The information is a 46 digit string formed by concatenates some values such as Credit card number, card verification value and expiry date of the card. For the purpose of security, the information has been encrypted before sent to server over the network. The encryption technique used for securing the cipher text is Caesar cipher. Caesar cipher has been used with shift value of three. Original string of 46 digits has been converted into encrypted string of same length. For the purpose of security of

Credit card application, some of the network attacks have been examined. An attack has been examined on the credit card information being sent over the network.

Step 2: IMPLEMENT RF CLASSIFIER

Random forest classifier creates a set of decision trees from a randomly selected subset of the training set. It is a set of decision trees (DT) from a randomly selected subset of the training set and then It collects the votes from different decision trees to decide the final prediction

Step 3: TRAINING AND TESTING FOR MODEL CREATION

The selected ML algorithm learns how to make predictions or categorize data using the training set. In this phase, the model refines its internal settings to best match the training set of data.

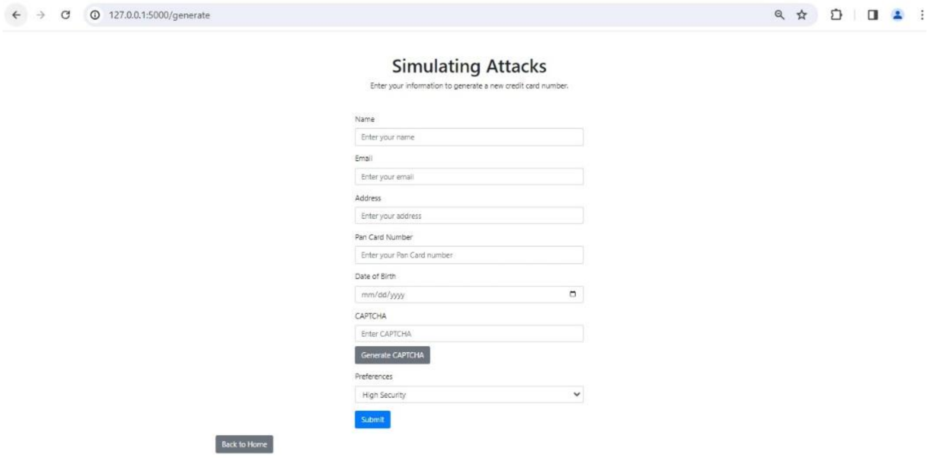
Finding the optimal values for hyperparameters (parameters that govern the learning process) that are not learned from the data is known as "hyperparameter tuning." In order to enhance the performance of the model, we are experimenting with various hyperparameter settings using the validation set.

Step 4: IMPLEMENT ENHANCED RF CLASSIFIER

In this step, we will prepare the data by standardizing it, separating features from labels, and then splitting it into training and validation sets for machine learning model development and evaluation.

Step 5: TEST RESULT WITH DIFFERENT METRICS

This stage allows us to identify the comprise value of credit card and stored on cloud so as to maintain the records for future references



127.0.0.1:5000/generate

Simulating Attacks

Enter your information to generate a new credit card number.

Name: Enter your name

Email: Enter your email

Address: Enter your address

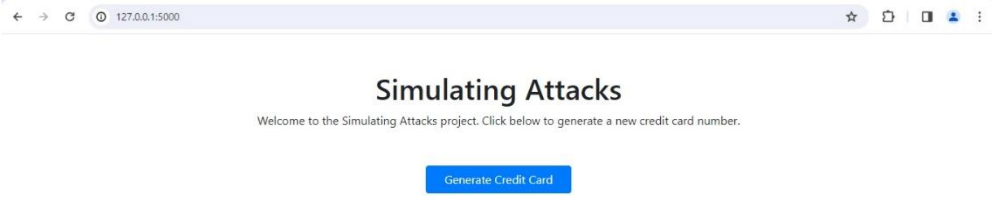
Pan Card Number: Enter your Pan Card number

Date of Birth: mm/dd/yyyy

CAPTCHA: Enter CAPTCHA

Preferences: High Security

Fig. 1 Profile creation page

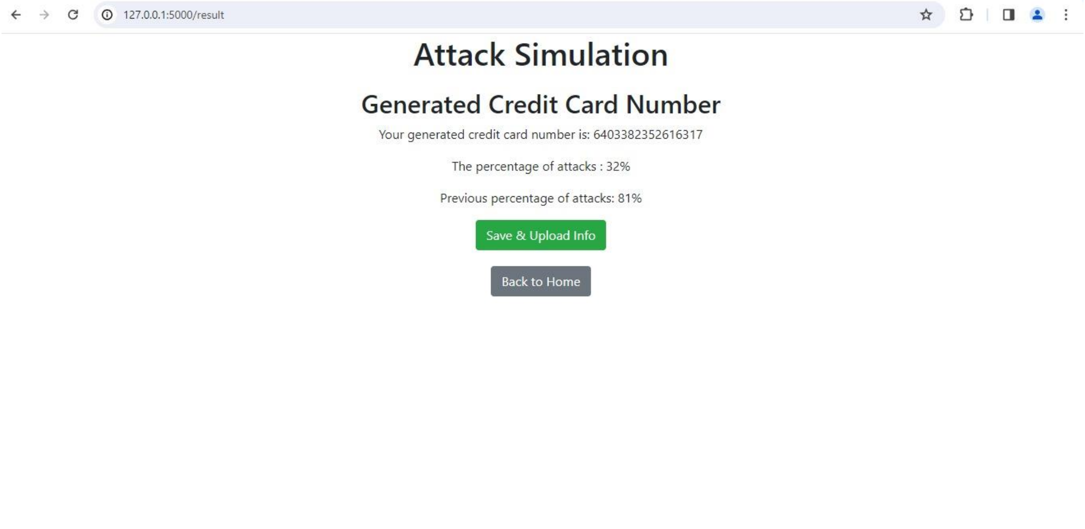


127.0.0.1:5000

Simulating Attacks

Welcome to the Simulating Attacks project. Click below to generate a new credit card number.

Fig. 2 Dashboard after profile creation



127.0.0.1:5000/result

Attack Simulation

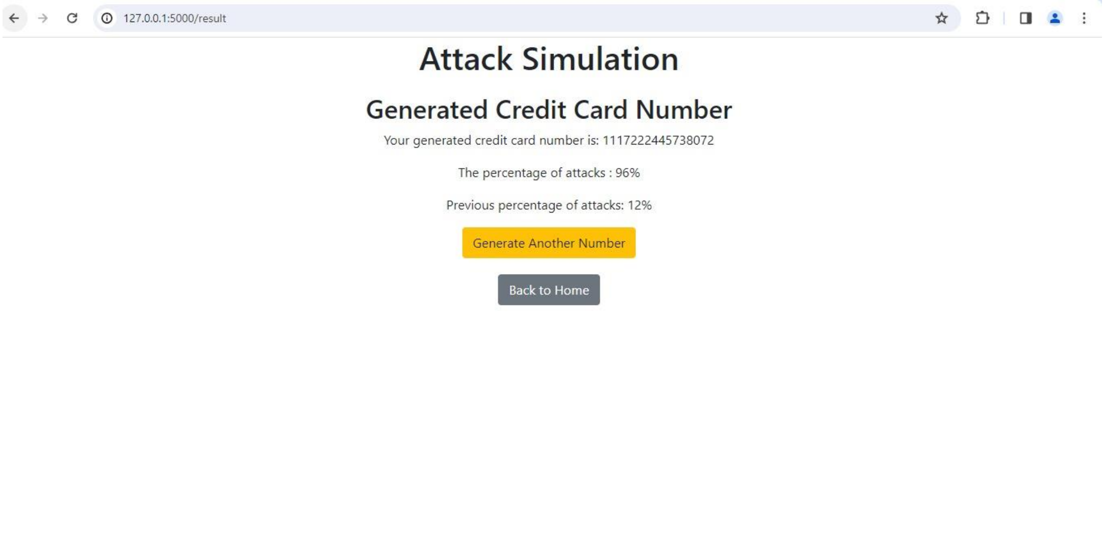
Generated Credit Card Number

Your generated credit card number is: 6403382352616317

The percentage of attacks : 32%

Previous percentage of attacks: 81%

Fig. 3 Generating credit card numbers to check attacks



127.0.0.1:5000/result

Attack Simulation

Generated Credit Card Number

Your generated credit card number is: 1117222445738072

The percentage of attacks : 96%

Previous percentage of attacks: 12%

Fig. 4 Result showing attacks on generated numbers

V. CONCLUSION AND FUTURE SCOPE

Simulating attacks on cloud environments offers a valuable and proactive approach to strengthening security posture. By emulating real-world attack scenarios, organizations can gain crucial insights into vulnerabilities, assess the effectiveness of existing security controls, and identify areas for improvement. This allows for:

- Proactive identification and mitigation of vulnerabilities: Before attackers exploit them, simulations can unveil weaknesses in security configurations, access controls, and system design, allowing for timely mitigation efforts.
- Improved understanding of attacker behavior: By analyzing simulated attack behavior, organizations can gain valuable insights into attacker tactics and motivations, enabling them to develop more targeted and effective defense strategies.
- Validation of security controls: Simulations offer a safe and controlled environment to test the efficacy of implemented security controls, ensuring they can efficiently detect and respond to potential threats.
- Informed decision-making: By providing empirical data on the impact of different attacks and the effectiveness of security measures, simulations empower organizations to make informed decisions regarding security investments and resource allocation.

However, it's crucial to acknowledge the limitations of simulations. They cannot perfectly replicate the real world and may not capture the full spectrum of potential attack methods. Additionally, the effectiveness of simulations heavily relies on the quality of attack scenarios and the accuracy of simulated environments.

Despite these limitations, simulations remain a powerful tool in the cloud security arsenal. By incorporating them into a comprehensive security strategy alongside other security practices, organizations can significantly enhance their preparedness against cyber threats and ensure the continued resilience of their cloud environments.

The future of simulating attacks on cloud environments holds immense potential for enhancing security posture and proactive risk management. Here are some key trends and directions we can expect to see:

- Increased Sophistication and Integration
- Enhanced Automation and Continuous Assessment
- Focus on Specific Attack Types and Cloud Services
- Increased Collaboration and Standardization
- Ethical Considerations and Transparency

By embracing these advancements and fostering responsible practices, simulation will play a crucial role in proactively strengthening cloud security and empowering organizations to stay ahead of evolving threats.

REFERENCES

[1] Sumathy, K. L., and M. Chidambaram. "Text mining: concepts, applications, tools, and issuesan overview." International Journal of Computer Applications 80, no. 4 (2013). pg. 23

[2] Aggarwal, Charu C., and Haixun Wang. "Text mining in social networks." In Social network data analytics, pp. 353-378. Springer, Boston, MA, 2011.

[3] Mostafa, Mohamed M. "More than words: Social networks' text mining for consumer brand sentiments." Expert Systems with Applications 40, no. 10 (2013): 4241-4251.

[4] Netzer, Oded, Ronen Feldman, Jacob Goldenberg, and Moshe Fresko. "Mine your own business: Market-structure surveillance through text mining." Marketing Science 31, no. 3 (2012): 521-543.

[5] Fuller, Christie M., David P. Biros, and Dursun Delen. "An investigation of data and text mining methods for real-world deception detection." Expert Systems with Applications 38, no. 7 (2011): 8392- 8398.

[6] Othman, Rohana, Nooraslinda Abdul Aris, Ainun Mardziyah, Norhasliza Zainan, and Noralina Md Amin. "Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions." Procedia Economics and Finance 28 (2015): 59-67.

[7] Dong, Wei, Shaoyi Liao, and Liang Liang. "Financial Statement Fraud Detection using Text Mining: A Systemic Functional Linguistics Theory Perspective." In PACIS, p. 188. 2016.

[8] Fu, Kang, Dawei Cheng, Yi Tu, and Liqing Zhang. "Credit card fraud detection using convolutional neural networks." In International Conference on Neural Information Processing, pp. 483-490. Springer, Cham, 2016.

[9] Rawte, Vipula, and G. Anuradha. "Fraud detection in health insurance using data mining techniques." In Communication, Information & Computing Technology (ICCICT), 2015 International Conference on, pp. 1-5. IEEE, 2015.

[10] Dilla, William N., and Robyn L. Raschke. "Data visualization for fraud detection: Practice implications and a call for future research." International Journal of Accounting Information Systems 16 (2015): 1-22.

[11] Kanapickienė, Rasa, and Živilė Grundienė. "The model of fraud detection in financial statements by means of financial ratios." Procedia-Social and Behavioral Sciences 213 (2015): 321-327.

[12] West, Jarrod, and Maumita Bhattacharya. "Some Experimental Issues in Financial Fraud Mining." In ICCS, pp. 1734-1744. 2016.

[13] Kim, Yeonkook J., Bok Baik, and Sungzoon Cho. "Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning." Expert systems with applications 62 (2016): 32-43. pg. 24

[14] Olszewski, Dominik. "Fraud detection using self-organizing map visualizing the user profiles." Knowledge-Based Systems 70 (2014): 324-334.

[15] Albrecht, Chad, Daniel Holland, Ricardo Malagueño, Simon Dolan, and Shay Tzafrir. "The role of power in financial statement fraud schemes." Journal of Business Ethics 131, no. 4 (2015): 803-813.

[16] West, Jarrod, Maumita Bhattacharya, and Rafiqul Islam. "Intelligent financial fraud detection practices: an investigation." In International Conference on Security and Privacy in Communication Systems, pp. 186-203. Springer, Cham, 2014.