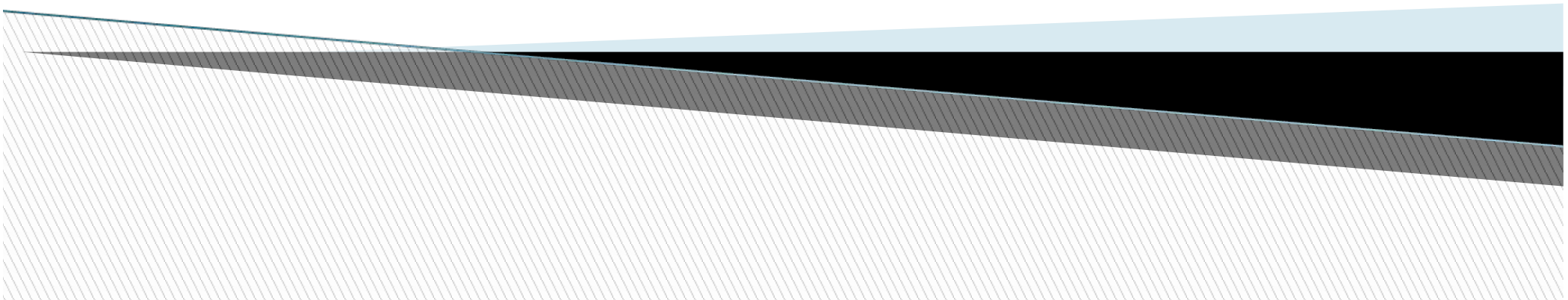
Enhancing Cloud Data Security with ECC-SVM: A Machine Learning-Driven Framework for Encryption and Threat Detection

Presented By:



CONTENTS

Abstract

- This study presents a comprehensive data security framework for cloud environments using Elliptic Curve Cryptography (ECC) combined with Support Vector Machine (SVM) techniques, referred to as ECC-SVM. The framework aims to ensure both data confidentiality and robust threat detection, essential for securing cloud-based applications and sensitive data. ECC provides a lightweight yet highly secure encryption solution, ideal for cloud systems where resource efficiency and strong security are paramount. Meanwhile, the SVM component leverages machine learning to monitor network traffic in real-time, identifying potential threats based on patterns learned from previous data. Through encryption and continuous threat monitoring, the ECC-SVM framework offers a dual-layered security approach that adapts to evolving security needs.

Continue..

- Performance analysis was conducted using five datasets (DS1 to DS5), focusing on key metrics: accuracy and precision.

- Results indicate that the ECC-SVM model demonstrates exceptionally high performance, achieving 100% accuracy on datasets DS2, DS3, and DS5, while maintaining precision scores between 98% and 99% across all datasets.

- This strong performance in both metrics highlights ECC-SVM's effectiveness in reliably classifying and encrypting data while minimizing false positives and false negatives, essential for ensuring data protection in cloud environments.

Introduction

- In the contemporary digital landscape, cloud computing has emerged as a pivotal technology, offering unparalleled benefits in terms of scalability, cost-efficiency, and accessibility. Organizations across various sectors increasingly rely on cloud services to store, manage, and process vast amounts of data.

- However, this migration to the cloud brings significant security challenges.

- Ensuring the confidentiality, integrity, and availability of data in cloud environments is paramount, as data breaches can lead to severe financial losses, reputational damage, and legal consequences [1-4]. To address these concerns, robust data security mechanisms are essential [5-7].

Continue..

- Encryption is a fundamental strategy for securing data, rendering it unintelligible to unauthorized users. Among the myriads of encryption algorithms available, the advanced encryption standard (AES) and Rivest cipher (RC6) stand out due to their robustness and efficiency [8-10].

- AES, a symmetric encryption algorithm, is renowned for its speed and security. It utilizes fixed block sizes and key lengths, making it suitable for encrypting large amounts of data efficiently [11, 12]. On the other hand, RC6, an evolution of the RC5 algorithm, offers flexibility in key length and block size, and its design simplicity enhances both its security and efficiency [11, 12].

- Combining AES and RC6 provides a multi-layered encryption approach, significantly complicating the decryption process for potential attackers.

Literature Survey

- Rajasekar et al. [36] suggested that the cloud computing boosts business scalability, flexibility, and affordability but raises security concerns due to centralized interactions. Integrating Distributed Ledger Technology (DLT), like blockchain, enhances cloud security by decentralizing data protection and enforcing transparent security policies. DLT also strengthens identity management, secure data sharing, and regulatory compliance, reducing trust and privacy risks in cloud ecosystems for resilient, stable performance.

- Kiran et al. [37] emphasized that cloud transformation is a crucial strategy for organizations aiming to leverage cloud computing's scalability, flexibility, and cost-efficiency. However, as IT infrastructure, applications, and data migrate to the cloud, security becomes a paramount concern, requiring strong identity management, encryption, and compliance. Balancing transformation with security is vital, given challenges like cost management, performance reliability, and vendor lock-in.

Objectives

1. To analyze and compare the security challenges in public and private cloud environments, identifying potential vulnerabilities and evaluating existing security measures in both settings.
2. To assess the performance of various encryption and security mechanisms, including a comparative analysis of previous methods, to determine their effectiveness and efficiency in cloud environments.
3. To design and implement a comprehensive data security framework for cloud environments, integrating elliptic curve cryptography (ECC) and support vector machine (SVM) techniques, combining encryption and machine learning to enhance security and breach detection capabilities.

Proposed Method

- The ECC-SVM Data Security Framework algorithm is designed to provide robust security for data in cloud environments by combining Elliptic Curve Cryptography (ECC) for encryption and Support Vector Machine (SVM) for detecting security threats.

- This approach leverages ECC's efficient encryption to protect data confidentiality and SVM's machine learning capabilities to monitor and identify patterns indicative of potential threats.

Continue..

- The first step involves setting up the parameters required for both ECC and the SVM model. ECC is a cryptographic method that relies on elliptic curves, which are mathematical structures enabling secure key generation.

- Along with ECC, the SVM model is initialized. SVM is a machine learning model trained to detect and classify potential threats by learning patterns from past data. This trained model serves as a monitoring tool, identifying suspicious activity or unauthorized access attempts by analyzing network traffic.

- In this step, ECC is applied to encrypt the data before it is stored in the cloud. Encryption is essential because it ensures that even if unauthorized individuals access the data, they cannot read or understand it without the appropriate decryption keys. For each data file or packet, ECC is used to convert the information into a secure, encrypted format.

Continue..

- Once data is encrypted and stored, the next focus is on monitoring network activity to detect any potential threats. This monitoring is necessary because encrypted data still needs protection from unauthorized access attempts and network-based attacks. The algorithm monitors network traffic related to the data, extracting specific features like data size, frequency, and the source and destination of the data packets.

- Given that cyber threats evolve, the algorithm includes a regular update process for the SVM model to ensure it can adapt to new types of threats. This step collects fresh network data and labels it according to observed behaviors, allowing the SVM model to be retrained on new patterns and anomalies.

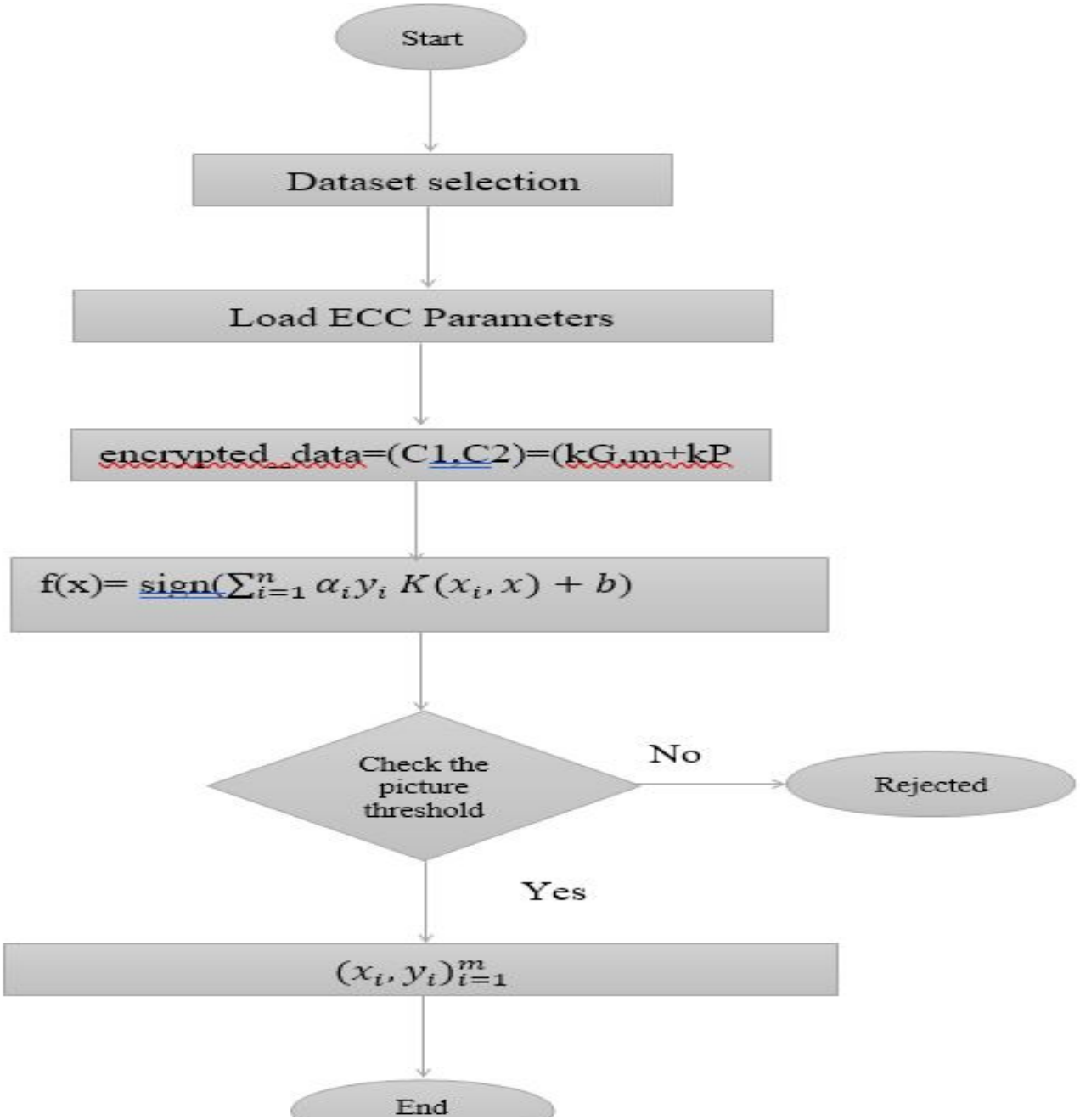
Continue..

- The final step of the algorithm involves maintaining logs and generating reports to ensure transparency and accountability.

- Every encryption event, threat detection instance, and security action is logged, creating a detailed record of the system's security activities.

- This logging is essential for auditing purposes and allows security teams to trace actions and detect patterns that may not be immediately evident.

Flow Chart


Start
Dataset selection
Load ECC Parameters
encrypted_data=(C1,C2)=(kG,m+kP
f(x)= sign($\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + b$)
Check the picture threshold
No
Rejected
Yes
$(x_i, y_i)_{i=1}^{m}$
End

Algorithm

- **ECC-SVM Data Security Framework for Cloud Environments**

- **Inputs:**
  - Data to be secured in the cloud
  - Parameters for Elliptic Curve Cryptography (ECC) encryption
  - Trained Support Vector Machine (SVM) model for threat detection
- **Outputs:**
  - Encrypted data for secure cloud storage
  - Threat detection status for potential security events

- **Steps**

1. **Initialize Encryption and Detection Parameters**
    1. Load necessary ECC encryption parameters.
    2. Load the trained SVM model for threat detection.
2. **Prepare Data for Encryption**
    1. Convert each data packet or file to a suitable format for encryption.
3. **Encrypt Data with ECC**
    1. Select a random value for the encryption process.
    2. Perform ECC encryption, resulting in a secure ciphertext.
    3. Store the encrypted data in secure cloud storage.

Continue..

4. **Monitor Network Traffic**
   Continuously observe incoming and outgoing network traffic related to the encrypted data.
5. **Extract Features for Threat Analysis**
   Identify and extract key features from network traffic data to analyze for security risks.
6. **Classify Data with SVM**
   Use the SVM model to classify traffic data based on extracted features.
   Determine threat status based on classification results.
7. **Update SVM Model Periodically**
   Collect new network data and label it with any new threat patterns.
   Retrain the SVM model using updated data to adapt to evolving threats.
8. **Deploy the Updated SVM Model**
   Replace the old SVM model with the newly trained model to maintain detection accuracy.
9. **Log Encryption and Detection Events**
   Record details of each encryption event and threat detection outcome for future reference.
10. **Generate Security Reports**
    Produce regular reports summarizing encryption activities, threats detected, and system performance.

Result and Validation

Data keys and other information

File name	User name	Server name	Open status	RC6 Key	AES key
c3.txt	user123456	server4	no	mV9IcB5Qh4	174e9
c5.txt	user12345	server4	no	tU6CrH2Qi2	17768
eee.txt	amit2	server4	yes	tL5BfF5Bf6	17d50
c1.txt	user123456	server4	yes	jI4FpB5Ub4	17e47
c4.txt	user123456	server4	no	rM0AqD5Cb6	fffe86aa
ff.txt	amit2	server4	no	rS7LdD1Fh6	fffe8e18
aba.txt	nehagupta	server4	yes	pY3EuI1Gi4	fffe8da8
c4.txt	shirsthi	server4	no	oX3VzJ8Yc9	fffe8cfa

Continue..

Encryption (E) and decryption (D) time in MS

File name	Status	E-RC6 Time in ms	D-RC6 Time in ms	E-AES Time in ms	D-AES Time in ms	status
c3.txt	attack	20372	20094	193	0	Attack
c5.txt	attack	31751	31155	401	0	attack
eee.txt	safe	5	5	25	3	safe
c1.txt	safe	7136	7008	233	247	safe
c4.txt	attack	27514	27102	472	0	attack
ff.txt	attack	1252	1244	32	0	attack

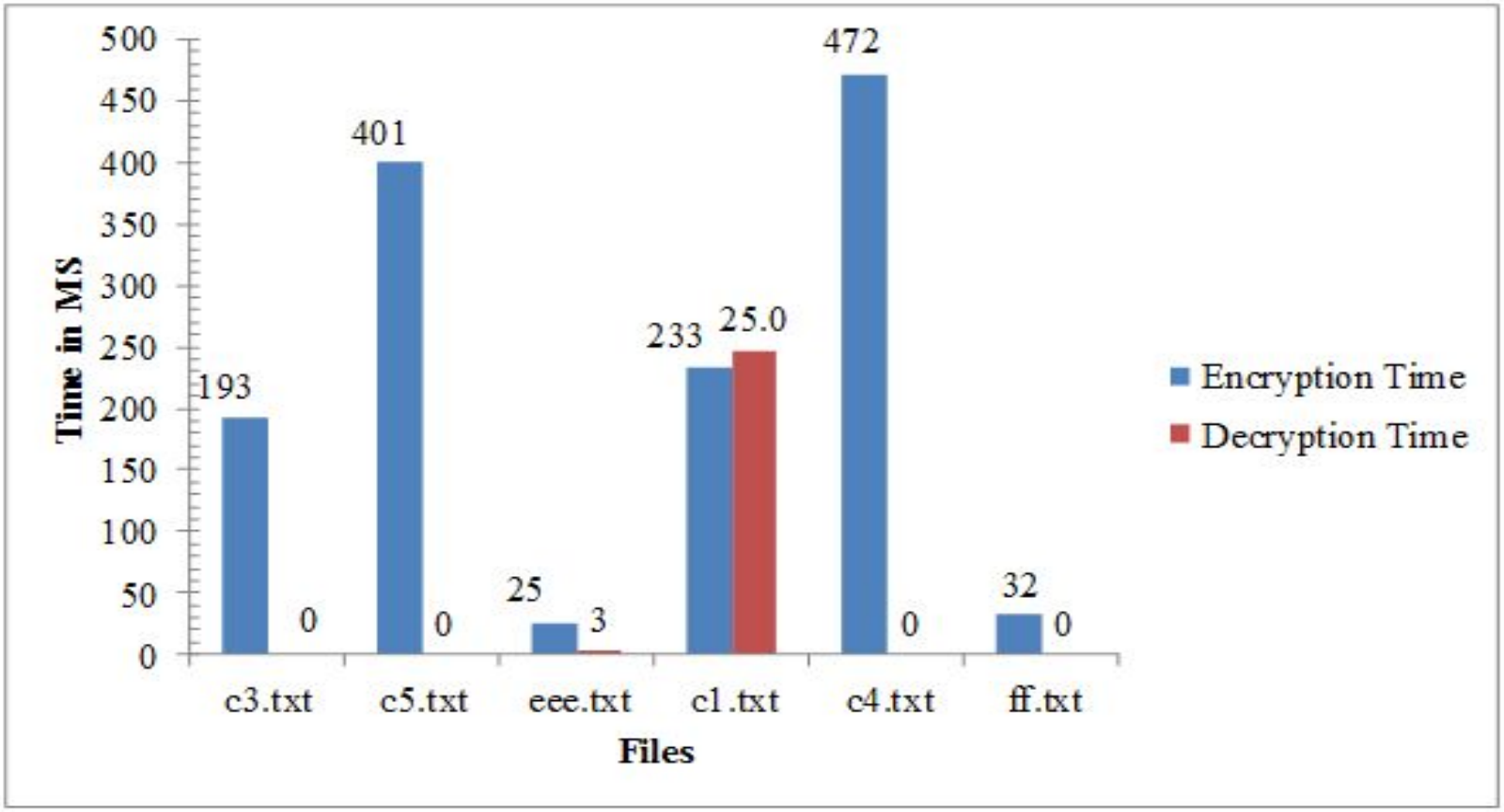
Continue..

Communication Load

User name	File name	Rendering time	Notification time	Margin in MS
U1	ff.txt	January 03 20:03:47 IST 2018	January 03 20:03:47 IST 2018	29
U2	c3.txt	January 22:23:28 IST 2018	January 03 22:23:28 IST 2018	86
U3	c4.txt	January 16:44:12 IST 2018	January 03 16:44:12 IST 2018	48
U4	c5.txt	January 16:53:54 IST 2018	January 03 16:53:54 IST 2018	75
U5	c1.txt	January 20:33:40 IST 2018	January 03 20:33:40 IST 2018	30

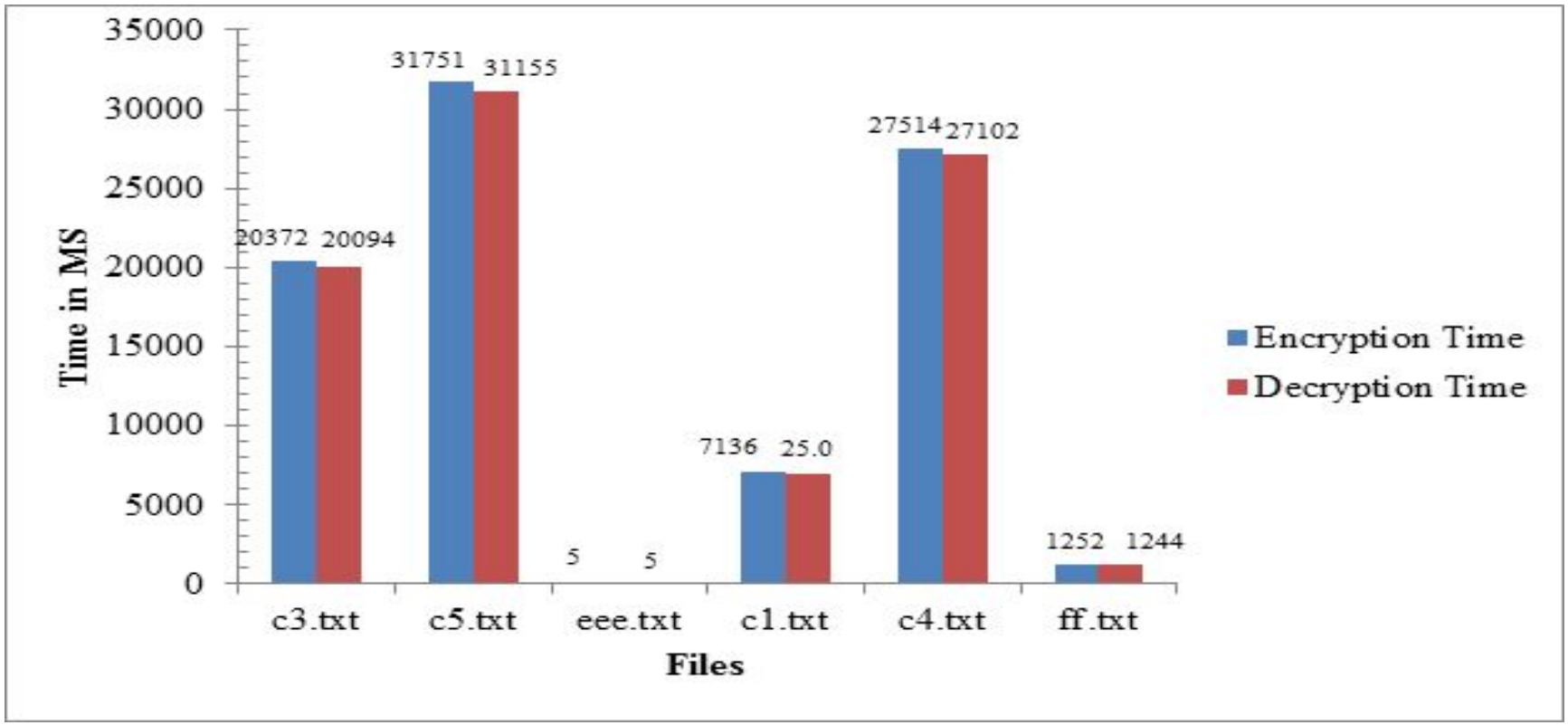
Continue..

Encryption and decryption time comparison based on AES



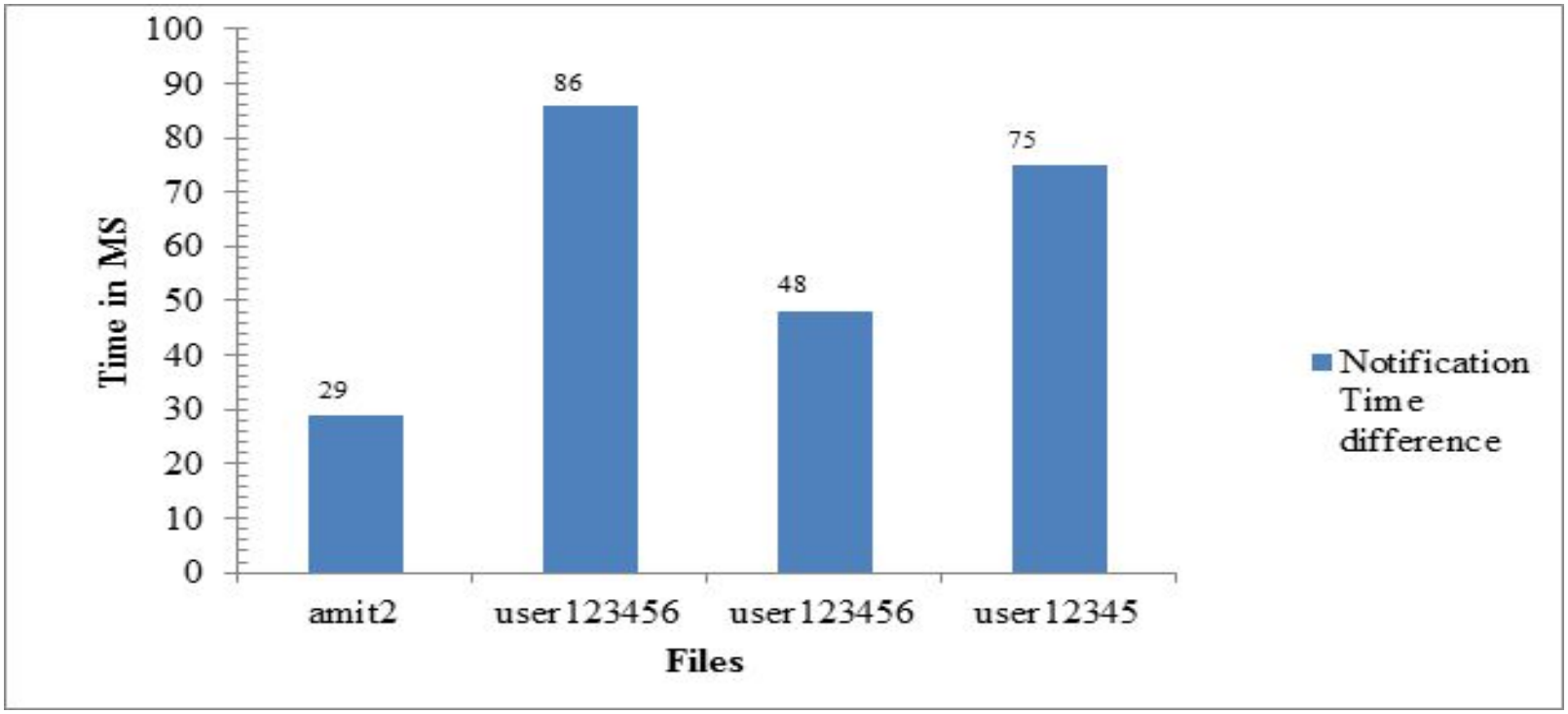
Continue..

Encryption and decryption time comparison based on RC6 + AES

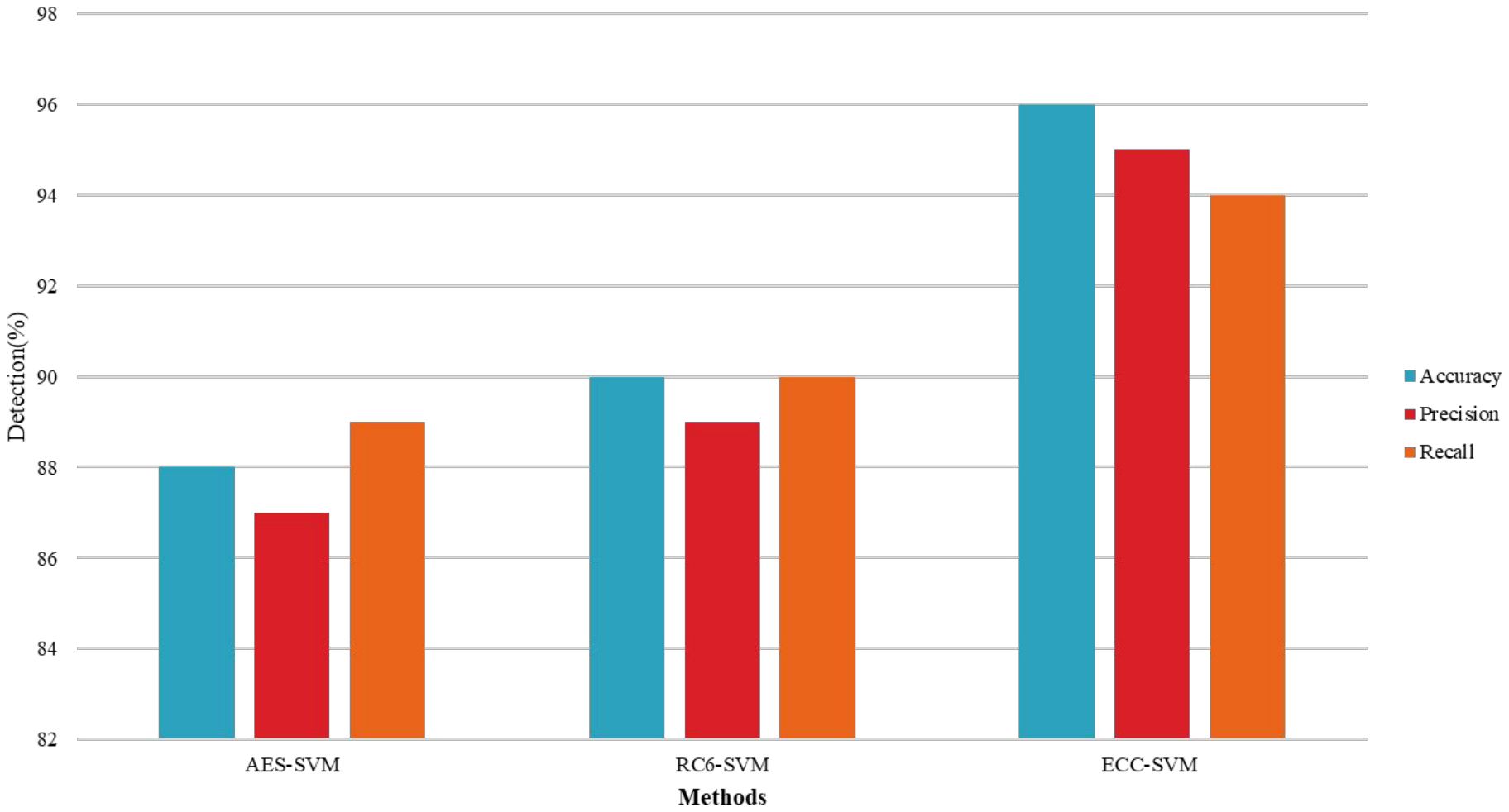


Continue..

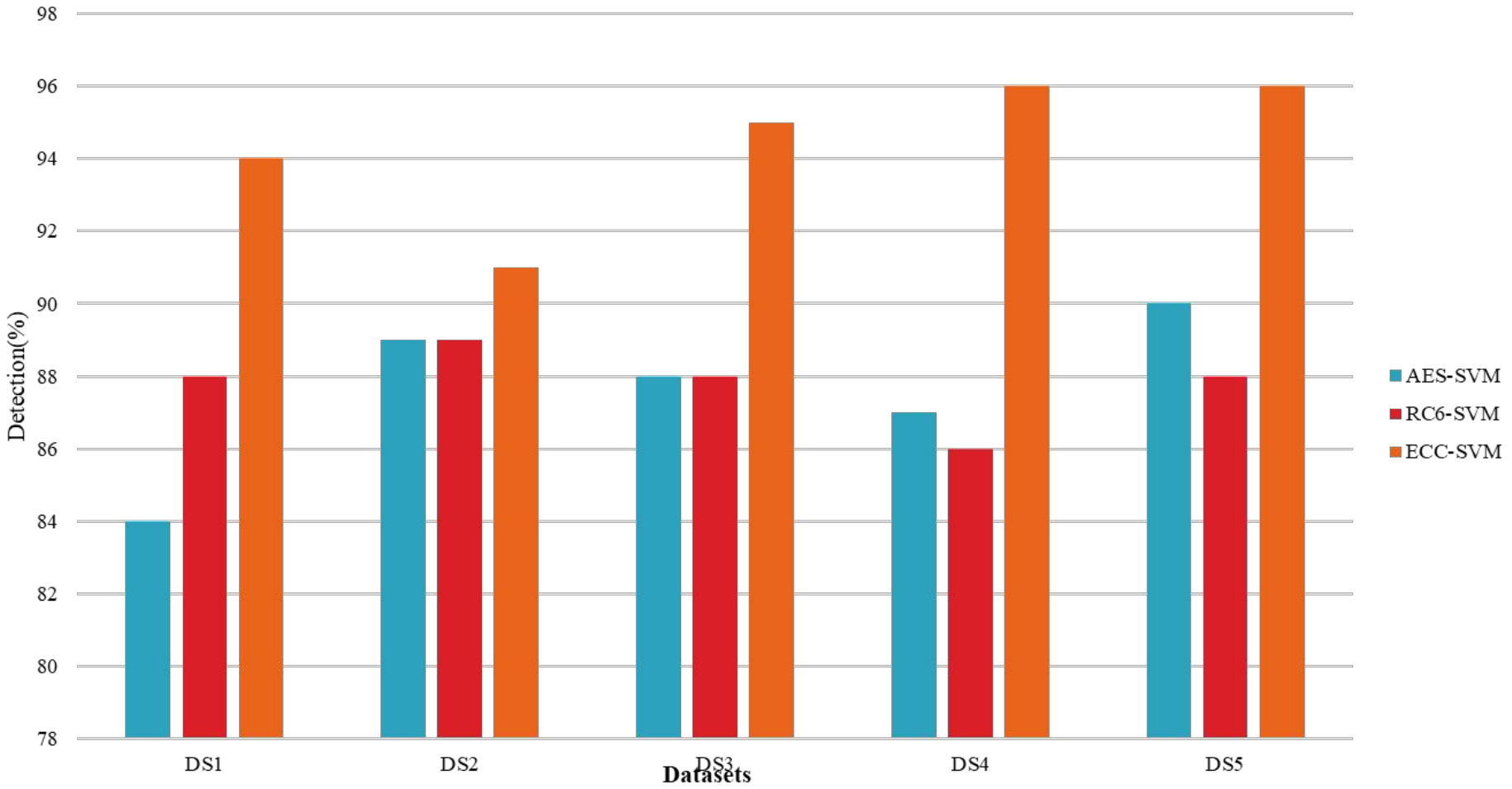
Attack Analysis



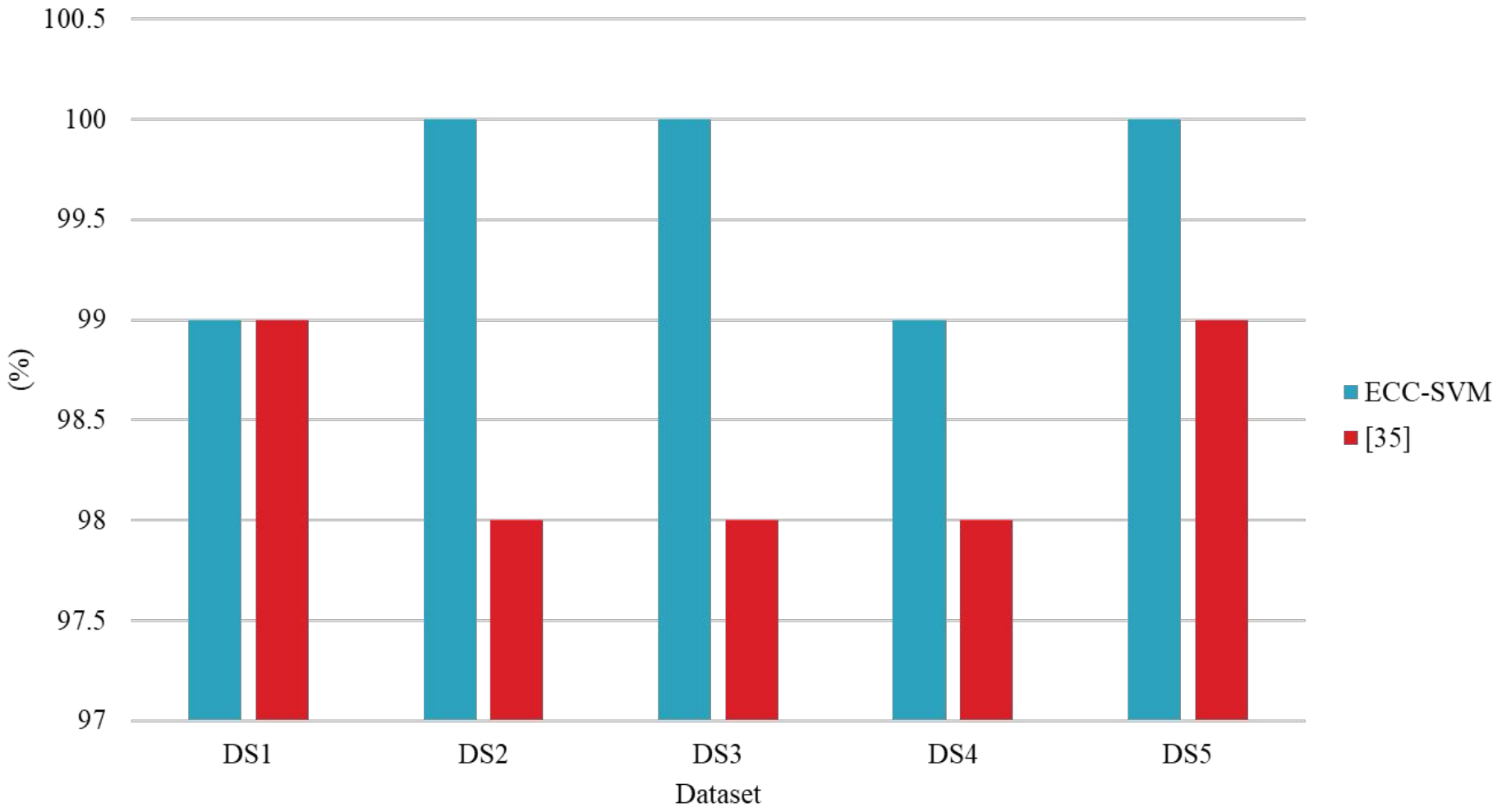
Performance comparison of AES-SVM, RC6-SVM and ECC-SVM based on accuracy, precision and recall



Accuracy comparison of AES-SVM, RC6-SVM and ECC-SVM based on different datasets



Average consistency accuracy comparison



Conclusions and Future Directions

- The ECC-SVM data security framework demonstrates a powerful and adaptable approach to cloud security, combining ECC's efficient encryption with SVM's machine learning-based threat detection.

- This hybrid approach addresses core security needs in cloud environments, offering both data confidentiality and real-time threat monitoring. The performance analysis across multiple datasets showed that ECC-SVM consistently achieved near-perfect accuracy and precision scores, with results reaching up to 100% accuracy and 99% precision in some datasets.

- Such high performance establishes ECC-SVM as a highly reliable framework, capable of effectively safeguarding sensitive data in cloud systems.

Continue..

- Compared to other encryption and threat detection combinations, such as AES-SVM and RC6-SVM, ECC-SVM consistently outperformed in terms of both accuracy and precision.

- The comparative results revealed that ECC-SVM achieved a notable improvement, with a 96% accuracy, 95% precision, and 94% recall rate, reflecting its robustness and efficiency. These findings validate the integration of ECC encryption and SVM threat detection as an optimal solution for cloud security, balancing strong data protection with resource efficiency.

Continue..

Future recommendations include:

1. Utilizing a combination of virtualization and optimization techniques.
2. Implementing boosting algorithms in the cloud for effective data sorting and classification.
3. Establishing a secure framework for scalable cloud computing that facilitates data access and management through generative AI.
4. Applying standard security mechanisms to assess and enhance security robustness and capability.
5. Addressing the significant challenge of preventing malicious identities in the cloud is a critical area for future research.

References

1. Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I. Above the clouds: A berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS. 2009; 28(13):2009.
2. Ruiz-Agundez I, Penya YK, Bringas PG. Cloud computing services accounting. International Journal of Advanced Computer Research. 2012; 2(2):7.
3. Singh A, Shrivastava M. Overview of security issues in cloud computing. International Journal of Advanced Computer Research. 2012; 2(1):41.
4. Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, Song D. Provable data possession at untrusted stores. In proceedings of the conference on computer and communications security 2007 (pp. 598-609). ACM.
5. Seng LK, Ithnin N, Said SZM. The approaches to quantify web application security scanners quality: a review. International Journal of Advanced Computer Research. 2018; 8(38): 285-312.
6. Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI international conference on software engineering 2012 (pp. 1-8). IEEE.
7. Malathi M. Cloud Computing Issues-A Survey. International Journal of Advanced Computer Research. 2012;2(2):113.
8. Nagar N, Jatav PK. A Secure Authenticate Framework for Cloud Computing Environment. International Journal of Advanced Computer Research. 2014; 4(1):266.
9. Adebisi AA, Adekanmi AA, Oluwatobi AE. A Study of Cloud Computing in the University Enterprise. International Journal of Advanced Computer Research. 2014; 4:450-8.
10. Tsai WT, Sun X, Balasooriya J. Service-oriented cloud computing architecture. In seventh international conference on information technology: new generations 2010 (pp. 684-689). IEEE.
11. Patra GK, Chakraborty N. Securing cloud infrastructure for high performance scientific computations using cryptographic techniques. International Journal of Advanced Computer Research (IJACR). 2014; 4(1):66-72.
12. Sikarwar C, Patidar K, Kushwah R. K-means and associated cuckoo based hierarchy optimization for document categorization. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(45): 297-302.
13. Zheng L, Hu Y, Yang C. Design and research on private cloud computing architecture to support smart grid. In2011 Third International Conference on Intelligent Human-Machine Systems and Cybernetics 2011 Aug 26 (pp. 159-161). IEEE.
14. Hay B, Nance K, Bishop M. Storm clouds rising: security challenges for IaaS cloud computing. In international conference on system sciences 2011 (pp. 1-7). IEEE.

Continue..

15. Ogigau-Neamtiu F. Cloud computing security issues. Journal of Defense Resources Management. 2012; 3(2):141.
16. Akhil KM, Kumar MP, Pushpa BR. Enhanced cloud data security using AES algorithm. InIntelligent Computing and Control (I2C2), 2017 International Conference on 2017 Jun 23 (pp. 1-5). IEEE.
17. Alsaidi A, Kausar F. Security Attacks and Countermeasures on Cloud Assisted IoT Applications. In2018 IEEE International Conference on Smart Cloud (SmartCloud) 2018 Sep 21 (pp. 213-217). IEEE.
18. Elliott D, Otero C, Ridley M, Merino X. A Cloud-Agnostic Container Orchestrator for Improving Interoperability. In2018 IEEE 11th International Conference on Cloud Computing (CLOUD) 2018 Jul 1 (pp. 958-961). IEEE.
19. Elsayed M, Zulkernine M. Towards security monitoring for cloud analytic applications. In2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS) 2018 May 3 (pp. 69-78). IEEE.
20. Feng S, Xiong Z, Niyato D, Wang P, Wang SS. Joint pricing and security investment for cloud-insurance: A security interdependency perspective. InWireless Communications and Networking Conference (WCNC), 2018 IEEE 2018 Apr 15 (pp. 1-6). IEEE.
21. Gordin I, Graur A, Potorac A, Balan D. Security assessment of OpenStack cloud using outside and inside software tools. In2018 International Conference on Development and Application Systems (DAS) 2018 May 24 (pp. 170-174). IEEE.
22. Halgaonkar PS, Kathole AB, Nadaf JS, Tambe KP. Providing Security in Vehicular Adhoc Network using Cloud Computing by secure key Method. In2018 International Conference on Information, Communication, Engineering and Technology (ICICET) 2018 Aug 29 (pp. 1-3). IEEE.
23. Lee BH, Dewi EK, Wajdi MF. Data security in cloud computing using AES under HEROKU cloud. InWireless and Optical Communication Conference (WOCC), 2018 27th 2018 Apr 30 (pp. 1-5). IEEE.
24. Li L, An X. Research on Storage Mechanism of Cloud Security Policy. In2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS) 2018 Aug 10 (pp. 130-133). IEEE.
25. Mary CJ, Mahalakshmi K, Senthilkumar B. Deep Dive On Various Security Challenges, Threats And Attacks Over The Cloud Security. In2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) 2023 Mar 17 (Vol. 1, pp. 2089-2094). IEEE.
26. Reddy MV, Charan PS, Devisaran D, Shankar R, Kumar PA. A Systematic Approach towards Security Concerns in Cloud. In2023 Second International Conference on Electronics and Renewable Systems (ICEARS) 2023 Mar 2 (pp. 838-843). IEEE.
27. Gahane S, Verma P. The Research Study on Identification of Threats and Security Techniques in Cloud Environment. In2023 1st DMIHER International Conference on Artificial Intelligence in Education and Industry 4.0 (IDICAIEI) 2023 Nov 27 (Vol. 1, pp. 1-6). IEEE.

Continue..

28. Kumar H, Gupta H. Cloud Security: An Innovative Technique for the Enhancement of Cloud Security. In2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) 2023 Dec 15 (pp. 411-416). IEEE.
29. Kanagasabapathi K, Mahajan K, Ahamad S, Soumya E, Barthwal S. AI-Enhanced Multi-Cloud Security Management: Ensuring Robust Cybersecurity in Hybrid Cloud Environments. In2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) 2023 Dec 14 (pp. 1-6). IEEE.
30. Vidhyasagar BS, Arvindhan M, Arulprakash A, Kannan BB, Kalimuthu S. The Crucial Function that Clouds Access Security Brokers Play in Ensuring the Safety of Cloud Computing. In2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI) 2023 Nov 23 (pp. 98-102). IEEE.
31. Dang F, Yan L, Yang Y. Research on Intelligent Centralized System Based on Security Architecture of Computer Cloud Security Protection. In2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI) 2023 May 26 (pp. 1281-1285). IEEE.
32. Zou Z. Research on user information security based on cloud computing. In2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC) 2023 Sep 15 (Vol. 7, pp. 35-39). IEEE.
33. Kumar ER, Reddy SS, Reddy MB. AMulti-Stage Cloud Security for Cloud Datausing Amalgamate Data Security. In2023 International Conference for Advancement in Technology (ICONAT) 2023 Jan 24 (pp. 1-5). IEEE.
34. Anithaashri TP. Novel Weight-Improved Particle Swarm Optimization to Enhance Data Security in Cloud. In2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2023 Oct 11 (pp. 195-200). IEEE.
35. Chen M, Wang H, Liang Y, Zhang G. Net and configurational effects of determinants on cloud computing adoption by SMEs under cloud promotion policy using PLS-SEM and fsQCA. Journal of Innovation & Knowledge. 2023 Jul 1;8(3):100388.

Continue..

36. Rajasekar P, Kalaiselvi K, Shanmugam R, Tamilselvan S, Pandian AP. Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments. In2024 Second International Conference on Advances in Information Technology (ICAIT) 2024 Jul 24 (Vol. 1, pp. 1-6). IEEE.
37. Kiran MS, Balajee RM, Sai KV, Kishore MS, Srithar S. Cloud Transformation and the Key Concerns for Cloud Security and Challenges. In2024 Second International Conference on Inventive Computing and Informatics (ICICI) 2024 Jun 11 (pp. 423-432). IEEE.
38. Bhavsar R, Thakar V. Identifying Hacking Failures in the IaaS, PaaS, and SaaS Networks to Secure Cloud Applications. In2024 Parul International Conference on Engineering and Technology (PICET) 2024 May 3 (pp. 1-6). IEEE.
39. Dhanalakshmi J, Pandeeswari N. Blockchain Enabled Security and Integrity in Cloud Computing. In2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2024 Oct 3 (pp. 1076-1082). IEEE.
40. Rawal BS. A Quantum Safe Approach for Security Challenges at the Edge of Cloud in 5G and Beyond. In2024 IEEE Cloud Summit 2024 Jun 27 (pp. 194-199). IEEE.
41. Gorantla VA, Gude V, Sriramulugari SK, Yuvaraj N, Yadav P. Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In2024 2nd International Conference on Disruptive Technologies (ICDT) 2024 Mar 15 (pp. 494-499). IEEE.
42. Feng M, Zhou J, Tang Y. Enhancing Cloud-Native Security Through eBPF Technology. In2024 IEEE 11th International Conference on Cyber Security and Cloud Computing (CSCloud) 2024 Jun 28 (pp. 165-168). IEEE.
43. Nair MC, Ankayarkanni B. Enhancing Cloud Security in DDoS: A Holistic Approach Leveraging Machine Learning Techniques. In2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT) 2024 Aug 8 (Vol. 1, pp. 1217-1222). IEEE.
44. Mallikarjunaradhya V, Yennapusa H, Palle RR, Suganyadevi K, Gupta N. Impacts of high denisty Cloud Computing on Data Protection and Security management for 6G Networking. In2024 2nd International Conference on Disruptive Technologies (ICDT) 2024 Mar 15 (pp. 617-622). IEEE.
45. Dhinakaran M, Sundhari M, Ambika S, Balaji V, Rajasekaran RT. Advanced Machine Learning Techniques for Enhancing Data Security in Cloud Computing Systems. In2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) 2024 Feb 9 (Vol. 5, pp. 1598-1602). IEEE.
46. Pizzato F, Bringhenti D, Sisto R, Valenza F. Security Automation in next-generation Networks and Cloud environments. InNOMS 2024-2024 IEEE Network Operations and Management Symposium 2024 May 6 (pp. 1-4). IEEE.

THANK YOU!
ANY QUERIES PLEASE !