IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# INNOVATIVE SECURITY FOR ACTIVE AND PASSIVE ATTACKS

[1]Harshitha S, [2]Dr . H. Srinivas Murthy,

[1]Post Graduation Student Master of Technology, Department of Computer Science and Engineering SJCIT, Chikaballapur, India.

[2]Associate Professor, Department of Computer Science and Engineering, SJCIT, Chikaballapur, India.

***Abstract:*** The continued build-out of online infrastructure and digital services has greatly increased the threat of both passive and aggressive cyber attacks and thus threatens the accessibility, privacy and integrity of Sensitive data. A hybrid encryption and analysis based security framework to mitigate both passive and active attacks The system combines RSA and AES cryptographic algorithms for providing strong data security during transmission. A genetic algorithm based optimization technique is used to improve the detection of suspicious patterns in web usage. In addition, the model gives importance to early threat detection and prevention through web usage mining and access log analysis. The approach supports secure data flow, user behavior profiling, and real-time response to unauthorized activities with results to demonstrate improved accuracy, encryption strength.It contributes to more resilient, privacy-aware communication environments in dynamic threat landscapes.

***Index Terms*** - Cybersecurity, Passive Attacks, Active Attacks, RSA, AES, Genetic Algorithm, Web Usage Mining, Data Encryption, Attack Detection, Secure Communication, Real-Time Monitoring, Intrusion Prevention System

## I. INTRODUCTION

The fast growth of digital technologies and Internet connected systems has resulted in a dramatic increase of cyber threats to individuals and organizations. Communication networks are vulnerable to cybercriminals' attempts to gain unauthorized access, listen in on confidential information, modify data or monitor users' activities. These threats are generally divided into passive and active attacks depending on their properties and they call for different methods of detection, prevention and mitigation.

Active attacks, such as data tampering, spoofing, and denial-of-service attacks, directly affect the security and availability of information systems. On the other hand, passive attacks, including eavesdropping and traffic analysis, secretly monitor communication to collect sensitive information without changing the data. As cyberattacks continue to evolve, traditional security methods like basic encryption and firewalls are often not enough to stop them. This creates the need for smarter and more flexible security solutions that can detect and prevent new types of attacks more effectively.

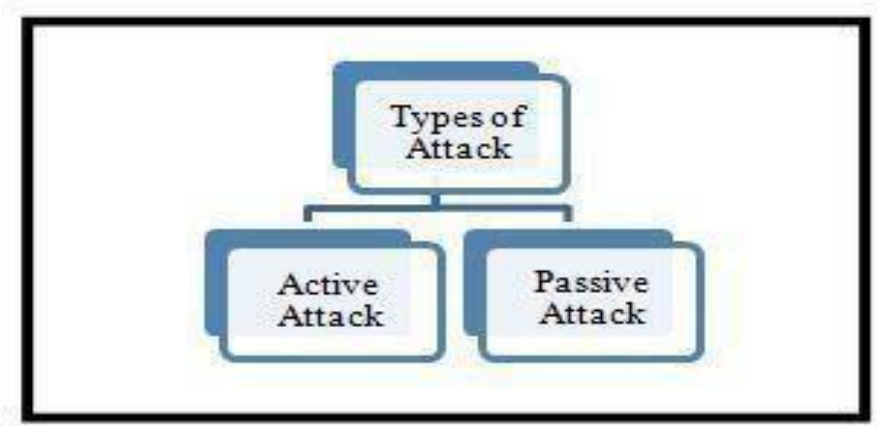


**Figure 1: Types of Attacks**

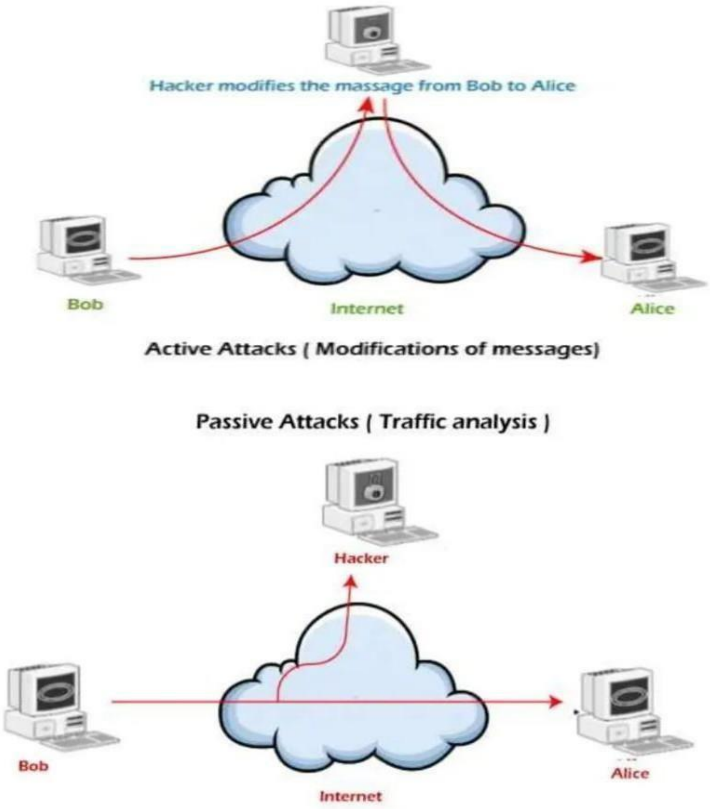


**Figure 2: Active and Passive Attacks**

It proposes a hybrid security model that integrates RSA and AES encryption techniques to protect data against interception, along with a genetic algorithm-enhanced analysis mechanism to detect abnormal web usage patterns indicative of potential attacks. The aim is to enhance information integrity and confidentiality and enable proactive monitoring of user activities through web usage mining.

The framework continuously reviews the access logs for early detection of suspicious activities and timely alert generation. It is evaluated on simulated attack scenarios and real-world datasets for its capability to detect passive and active attacks. The main goal is to provide a reliable, scalable and efficient security solution to support secure and uninterrupted communication in today's network environments.

## II. LITERATURE REVIEW

Recent developments in cybersecurity research have highlighted the increasing necessity for strong encryption techniques and sophisticated detection systems to counter both passive and active cyber threats. The shift toward hybrid encryption, behavioral analytics, and evolutionary algorithms is a response to the increasing complexity of modern cyberattacks, while traditional systems like firewalls and rule-based access control remain essential.

### A.Existing Security and Attack Prevention Techniques

Various methods have been explored to secure digital communications and identify unauthorized activities:

- **RSA and AES Encryption**: Widely used public-key and symmetric encryption algorithms provide a secure framework for data confidentiality and integrity RSA is used to securely exchange keys . AES is used for very fast and efficient encryption of data . However, these techniques alone may not be effective against new and ever evolving attack patterns.
- **Intrusion Detection Systems (IDS)**: These tools monitor network activity for suspicious behaviour but frequently rely on pre-defined rules or signatures. This means they could miss new or previously unknown cyber threats.
- **Web Usage Mining**: Studying user activity on websites can reveal abnormal access patterns that might signal a breach. However, traditional web usage mining does not adapt easily to new attack patterns and may not detect threats in real-time.
- **Genetic Algorithms (GA)**: Evolutionary techniques such as GAs are used to optimize the parameters for attack detection and to enhance classification.Although effective, genetic algorithms require proper configuration and higher processing time.
- **Traffic Pattern Analysis**: Helps identify eavesdropping and session hijacking attempts by recognizing irregularities in communication flow. However, it is less effective when network traffic is encrypted or tunnelled.

### B. Limitations of Existing Systems

- Despite widespread adoption, current systems face several challenges in defending against sophisticated passive and active threats:
- Lack of hybrid models combining encryption and behavioural analysis.
- Inability to adapt to evolving attack types in real time.
- High processing overhead in cryptographic and mining operations.
- Inadequate detection of silent attacks such as MITM and DNS spoofing.
- Poor scalability and responsiveness in high-volume traffic environments.
- Absence of intelligent automation in alert and response systems.

### C. Advancements in Hybrid Security Models

To address the challenges posed by traditional methods,An integrated approach leveraging encryption, intelligent analysis, and web usage mining. Key improvements include:

- Secure data encryption with AES for payload protection and RSA for key exchange.
- Web usage mining for profiling access behavior and detecting suspicious deviations.
- Genetic algorithm-driven anomaly detection to evolve and improve threat identification.
- Proactive detection of passive (e.g., sniffing, eavesdropping) and active (e.g., spoofing, tampering) attacks.
- Real-time log analysis for early alerts and quicker incident response.
- Modular architecture suitable for future enhancements and large-scale deployment.

These innovations enable continuous, adaptive protection against emerging threats by integrating advanced encryption with intelligent behaviour modelling. The system not only mitigates the limitations of static security frameworks but also empowers organizations to adopt predictive and preventive cybersecurity practices.

| Existing Methods | Proposed Enhancements |
|---|---|
| RSA or AES used independently | Combining AES for data secrecy with RSA for safe key exchange |
| Static IDS and firewall rules | Dynamic detection using web usage patterns and GA-based adaptation |
| Manual traffic pattern observation | Automated pattern recognition through mining and intelligent filters |
| Limited application of genetic algorithms | Optimized rule generation and anomaly classification using GA |
| Rigid security rules and configurations | Self-evolving systems that learn from web behavior and adapt accordingly |
| Centralized detection tools | Unified systems with intelligent alerting and automated response capabilities |

**Table 1.1: Comparison of Existing Methods and Proposed Enhancements**

## III. METHODOLOGY

The proposed system integrates advanced encryption algorithms, web usage mining, and genetic algorithm-based threat detection to protect against both passive and active attacks in network environments. The system analyzes web activity patterns, secures data through hybrid cryptographic techniques, and applies intelligent anomaly detection for robust security.

A. System Components

The security framework includes both software tools and algorithmic techniques that work in synergy to identify and stop dangers from the internet.

**i. Software Components:**

- **Python (Core Environment):** Used for building integration workflows, mining algorithms and encryption procedures.
- **RSA and AES Modules:** Data is encrypted using AES for faster processing and RSA for secure key exchange, thus making it a hybrid encryption.
- **Web Usage Mining Scripts**: Python scripts used for extracting and analyzing access patterns from usage data, logs and browsing history.
- **Genetic Algorithm Module**: This module uses evolving rules to detect anomalies in online activity that may indicate a danger.
- **Log Analyzer (log_parser.py):** This program analyzes system logs and generates alerts when suspicious activity is detected.
- **Pandas,Numpy,Scikit-learn:**Used for preprocessing, behavioral analysis, and managing rule-based detection thresholds.

**ii. Frontend Components:**

- **HTML/CSS & JavaScript Interface:** Lightweight UI to upload logs, monitor encryption status, and visualize detected threats.

- **Flask-based Dashboard**: Displays encryption processes, threat levels, and analysis outputs in real time.

- **Matplotlib/Plotly**: For plotting anomaly scores and usage graphs based on mining results.

**B. Working Principle**

**1. Data Collection:**

- Data on access patterns and web usage are collected in controlled test environments simulating both aggressive and passive threats.

**2. Hybrid Encryption Process:**

- RSA was originally used to generate secure key exchanges between the sender and the receiver.
- The data payload is then encrypted securely using AES.
- Encrypted traffic is stored and analyzed for the integrity and confidentiality.

**3. Web Usage Mining:**

- Mining user interaction logs extracts behavioral patterns.
- Any anomalous behavior is reported based on pattern deviation.

**4. Genetic Algorithm-Based Threat Detection:**

- Dynamic construction and optimization of rules with genetic algorithms for anomaly detection.
- These criteria change as data inflow from time to time and the accuracy of detection increases.

**5. Log Analysis and Alerting:**

- System and network logs are parsed to detect unusual access, sniffing, spoofing and tampering attempts.
- When a match is found with suspicious behavior patterns, real-time notifications are generated.

**6. Frontend Monitoring and Reporting:**

- The dashboard in Flask shows threat alerts, anomaly detection results and encryption status.
- Graphical charts are used to visualize data usage trends and highlight attack attempts.

**7. Deployment:**

- The whole system is modular and can be deployed locally or in a distributed network configuration for scalable defense.

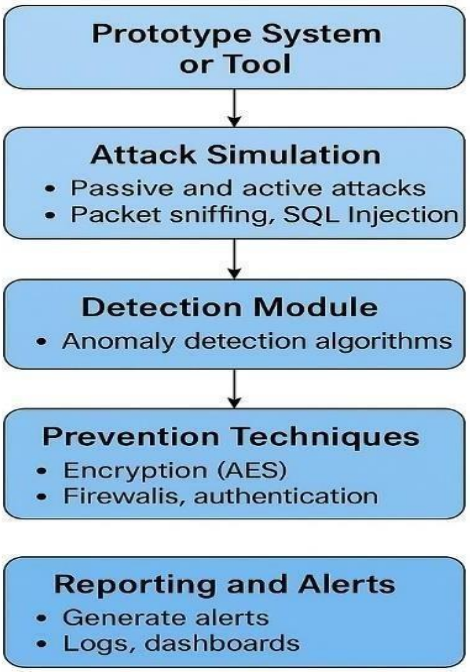


**Figure 3: Block Diagram of the Proposed Flow**

The proposed system follows a structured flow beginning with a prototype tool that simulates both passive and active cyber attacks, including packet sniffing and SQL injection. These simulated threats are then processed by the detection module, which uses anomaly detection algorithms to identify unusual or malicious behavior. Once threats are detected, the system triggers prevention mechanisms like AES encryption, firewalls, and authentication protocols to safeguard data. The final phase involves reporting and alerts, where the system generates real time notifications, logs, and dashboards for administrators to monitor threats and system responses effectively, ensuring robust cybersecurity management and continuous vigilance.

**C. Advantages of the Proposed System**

- Dual-layer encryption for robust protection of transmitted data.
- Behavior-based mining for early detection of passive and active threats.
- Evolving anomaly detection using genetic algorithms improves with time.
- Modular and adaptable system architecture.
- Real-time alerts and status monitoring via interactive dashboard.

## IV. RESULTS AND DISCUSSION

The proposed system integrates advanced encryption algorithms and genetic algorithms (GA) for preventing and detecting cyber threats, specifically passive and active attacks. It simulates attacks, detects anomalies, and applies hybrid prevention mechanisms. The following graphs present experimental results that validate the efficiency, performance, and accuracy of the approach.

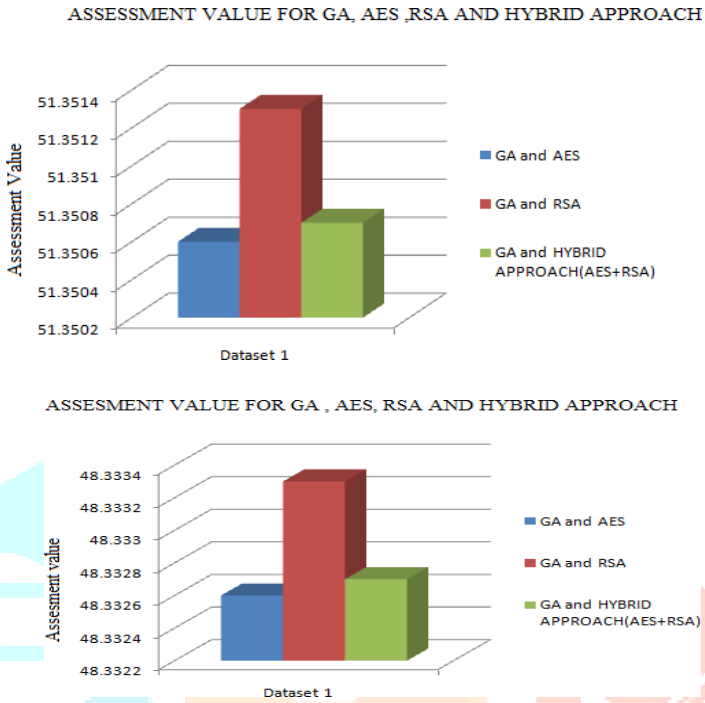


**Figure 4: : A comparison of several encryption algorithm combinations with GA**

The graph compares the assessment values of GA combined with AES, RSA, and a hybrid of AES+RSA. The results show that the combination of GA with RSA achieves the highest assessment value, indicating stronger encryption and better performance in securing network traffic. The hybrid approach also performs well, providing a good balance between speed and security. Although GA with AES produces satisfactory results, its assessment value is lower than the other combinations. These findings indicate that integrating RSA with Genetic Algorithms improves both encryption and threat detection, making it more suitable for applications that require stronger security.

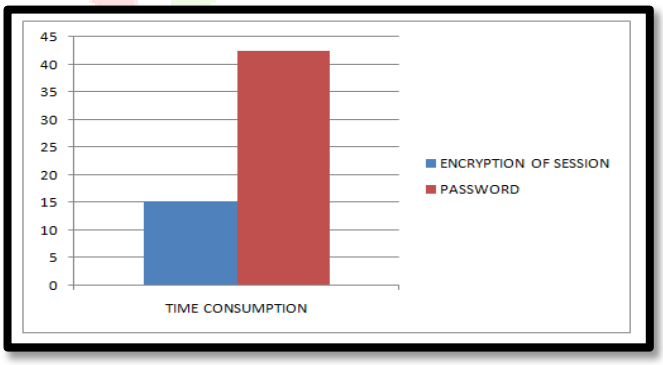


**Figure 5: A comparison of several IP spoofing attack prevention techniques based on time consumption is displayed.**

The time consumption comparison between two preventive methods—session encryption and password-based authentication—is shown in the bar chart below. The password technique has a higher computing overhead and takes a lot longer than session encryption. Session encryption, on the other hand, is better for real-time threat mitigation because it is quicker and more effective. This result demonstrates that encrypting session data not only improves security but also keeps the system responsive, which is essential for reducing the time it takes to respond to a danger during an IP spoofing attack.

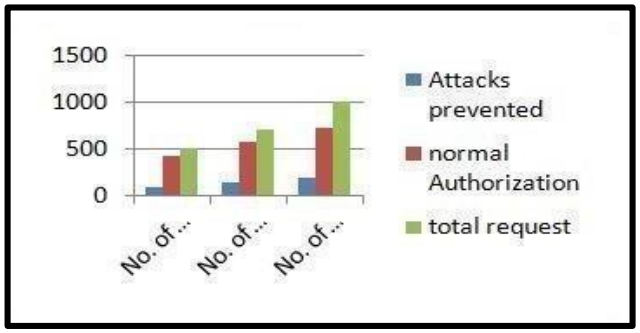


**Figure 6: Results Displaying Data on Attacks Prevented and Identified by the System Key Findings**

### A. ADVANTAGES

- **Effective Hybrid Approach**: By combining genetic algorithms with AES and RSA, protection was increased and assessment values in attack scenarios were improved.
- **Enhanced Attack Prevention**: The system successfully recognized and prevented both active and passive attacks, such as SQL injection and packet sniffing.
- **Decreased Time Consumption**: When compared to conventional password-based solutions, session encryption techniques dramatically reduced time consumption.
- **Robust Detection Metrics**: High attack prevention rates and few false alarms were the outcome of the anomaly detection module's accurate flagging of suspicious activity.
- **Detailed Reporting**:Dashboards, logs, and real-time alarms improved administrator responsiveness and system visibility.

### B. Limitations & Challenges

Despite strong results, a few limitations were observed:

- **Algorithmic Overhead**: When RSA and GA were combined, the computational overhead was greater than when AES was used alone.
- **Hybrid Complexity**:Considerable algorithmic optimization was needed for the hybrid encryption system's design and calibration.
- **Dataset Limitations**: The accuracy of the attack simulation relied on the diversity and realism of the test data used.
- **Manual Configuration**: Some of the detection rules and thresholds needed manual calibration for optimal performance.

## V. CONCLUSION

The proposed security framework combines the Genetic Algorithms (GA) with the AES and RSA encryption to improve the security against passive and active cyber attacks. IP spoofing, session hijacking and unauthorized access is prevented with a hybrid encryption method. The framework uses Genetic Algorithms and traditional encryption techniques to offer better data security and resistance to cyber-attacks.

The combined GA–AES–RSA model demonstrated better performance and detection capabilities than the individual encryption algorithms. It was also time efficient, especially for session level encryption, and it always caught unauthorized access attempts. The solution could deal with a large amount of malicious requests, which made it practically useful. Challenges that remain include algorithmic complexity, variability in data and difficulty inspecting encrypted traffic, which suggest directions for further refinement in production, high-traffic settings.

**Future Scope**

To strengthen and expand the system's capabilities, the following enhancements can be explored:

- **Advanced Hybrid Cryptography** – Incorporating quantum-resistant or lightweight methods to enhance performance in settings with limited resources.
- **Dynamic Threat Modeling:** This technique uses artificial intelligence (AI) to modify preventative tactics in real time in response to patterns of attacks.
- **Encrypted Traffic Handling:** To improve security without sacrificing privacy, techniques for examining encrypted packets utilizing metadata without complete decryption are being developed.
- **Automated Rule Tuning:** This technique uses machine learning to automatically modify firewall and access control policies in response to traffic patterns.
- **Cloud-Based Security Extension** – Deploying the framework in cloud and multi-cloud infrastructures for broader threat coverage.

By evolving in these directions, the proposed framework can serve as a resilient and intelligent cybersecurity system, capable of adapting to the rapidly changing threat landscape and securing modern digital infrastructures.

## VI REFERENCES

[1] Dilpreet kaur, Sukhpreet Kaur, ―A Study on User Future Request Prediction Methods Using Web Usage Mining‖, International Journal of Computational Engineering Research, Vol, 03, Issue, 4.

[2] S.Mirdula, D.Manivannan, ―Security Vulnerabilities in Web Application- an Attack Perspective‖, International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr May2013.

[3] Rimmy Chuchra, Bharti Mehta, Sumandeep Kaur, ―Use of web Mining in Network Security‖, International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com

[4] Jianli Duan, Shuxia Liu, ―Research on web log mining analysis‖, Instrumentation & Measurement,Sensor Network and Automation (IMSNA)

[5] Daxin Jiang Jian Pei Hang Li, ―Mining Search and Browse Logs for Web Search.

[6] Diallo Abdoulaye Kindy, Al-Sakib Khan Pathan, ―A Detailed Survey on Various Aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attack, and Remedies‖

[7] Sandra Sarasan, ―Detection and Prevention of Web Application Security Attacks‖, International Journal of Advanced Electrical and Electronics Engineering

[8] Sharmin Rashid, Subhra Prosun Paul, ―Proposed Methods of IP Spoofing Detection and Prevention‖ International Journal of Science and Research (IJSR), Volume 2 Issue 8, August 2013.

[9] Swati Paliwal, Ravindra Gupta, "A Review of Some Popular Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[10] K. F. Man, K. S. Tang, and S. Kwong, ―Genetic Algorithms: Concepts and Applications‖, IEEE Transactions on Industrial Electronics, vol. 43, no. 5, october 1996.

[11] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems. 2015.