International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Improved Rsa Algorithm for Data Security against DDoS Attack in a Cloud-based Intrusion Detection System

[1]Mrs. S. Sujitha, [2]Dr. R. Nirmalan, [3]Mrs. A. S. Malini, [4]Mrs. S. Vallimayil, [5]Mr. R. Kesavan
[1]Assistant Professor, Department of Computer Science and Engineering,
PSR Engineering College,
Sivakasi, Virudhunagar (Dt), Tamilnadu, India.
Email: sujitha@psr.edu.in
[2]Assistant Professor, Department of Artificial Intelligence and Data Science,
Mepco Schlenk Engineering College,
Sivakasi, Virudhunagar (Dt), Tamilnadu, India.
Email: nirmalan@mepcoeng.ac.in
[3]Assistant Professor, Department of Computer Science and Engineering,
PSRR College of Engineering,
Sivakasi, Virudhunagar (Dt), Tamilnadu, India.
Email: malini@psrr.edu.in
[4]Assistant Professor, Department of Electrical and Electronics Engineering,
PSR Engineering College,
Sivakasi, Virudhunagar (Dt), Tamilnadu, India.
Email:vallimayil2009@gmail.com
[5]Assistant Professor, Department of Artificial Intelligence and Data Science
PSR Engineering College,
Sivakasi, Virudhunagar (Dt), Tamilnadu, India.
Email:kesavan@psr.edu.in

Abstract— Today, more and more industries are using cloud computing for some integration operations, but ensuring the security of user data and system resources remains a challenge. This article proposes a method to identify and mitigate unwanted packets and traffic, especially duplicate packets, in cloud computing environments. The method includes creating an Intrusion Search and Detection (IF-AD) system to securely maintain user information and allocate secondary memory. To detect unwanted traffic, this method compares the size of the downloaded file with the original file, identifying any differences as potential DDoS. RSA encryption mechanism is used for subsequent file transfers for added security. The proposed approach aims to enhance the security posture of cloud-based systems by detecting and preventing unauthorized access and file modification.

Keywords- Cloud Computing, File Sharing, Key Generation, Encryption, Decryption, RSA

I. INTRODUCTION

Cloud computing (CC) is an advanced internet-based architecture that enables customers access to various IT resources, including software services, hardware services, storage services, network infrastructure, and operating systems, at an affordable cost [1]. This technology boasts scalability, minimal management effort, cost efficiency, and rapid development [2]. Cloud computing has revolutionized information processing, prompting scholars and researchers to focus on ensuring its security. Securing information processing in any system is vital for the success of a knowledge procurement system. Grid computing and Cloud computing enable swift and location-independent information processing, but this has raised concerns about trust among cloud users while utilizing shared resources [3], [4]. The CC's complex architecture makes it susceptible to various types of attacks, and employing a cooperative Intrusion Detection System (IDS) enhances detection accuracy compared to a single IDS due to limited knowledge of attack patterns [5].

Consequently, developing effective IDS is crucial to mitigate such threats [6]. IDS employs two main approaches for attack detection: signature-based and behavior-based. The signature-based method, although accurate, is vulnerable to new types of attacks. However, the behavior-based IDS performs better at discovering novel harmful attack types, making it a more appealing deployment solution [9]. Additionally, IDS can be divided into host-based IDS (HIDS) and network- based IDS (NIDS) based on where it is deployed [10]. HIDS is installed nearer to the host and more capable of capturing intrusions than NIDS, intended to identify intrusions at the network level. Software-defined technology is widely used in contemporary cloud environments to improve application services accessibility and dependability, but this also raises the risk of a significant intake of malicious attacks. By contrasting the present system with a known normal profile, anomaly-based IDS can identify deviations, but its application in the actual world is challenged by false alarms. Hybrid IDS, which combines anomaly-based and signature-based detection, addresses this issue by employing adaptive algorithms to reduce false alarms.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

II. RELATED WORK

Cloud computing has become a widely adopted computing paradigm, offering organizations numerous benefits such as flexibility, scalability, and cost efficiency [6,7]. However, cloud environments' distributed nature and resource sharing also present unique security challenges, making cloud security a critical research topic. Software security, Data security, and network security are key areas of focus for addressing these challenges. Researchers have proposed collaborative network security management systems to tackle security concerns. The work [8] introduced a practical collaborative network security management system to address Internet security issues.

Similarly, the vCNSMS, a collaborative network security prototype system, was developed in [9] to safeguard multi-tenant data centers from potential network attacks.Due to the importance of data and the growing usage of it across industries, data security in the cloud has become one of the most prominent security issues. Various security methods, such as intrusion detection systems (IDS), access control, and encryption, have been developed to ensure cloud data availability, integrity, and confidentiality. For instance, attribute-based encryption (ABE), distributed hash table (DHT) network, and identity-based timed-release encryption (IDTRE) have been proposed in an effective and secure access control model [10]. To enforce fine-grained access control policies for IoT data, a secure industrial data access control method based on cipher text policy- attribute-based encryption (CP-ABE) was created for the cloud-assisted Industrial Internet of Things (IIoT) [11].

Researchers have introduced intrusion detection systems (IDS) to identify and reduce potential attacks to strengthen cloud security. As an illustration, a methodology for deploying an IDS to defend against Distributed Denial of Service (DDoS) assaults in the cloud was suggested [12]. A protecting and securing IDS that can analyze system events in real- time to find possible attacks has been proposed. The productivity and effectiveness of intrusion detection systems (IDS) must be improved to ensure cloud data security. Implementing machine learning methods enhances anomaly detection and its accuracy in cloud systems. For instance, a study used deep neural networks to build an IDS based on machine learning to identify and stop internal and external threats in cloud computing systems. Researchers examined using blockchain technology in addition to IDS to increase the privacy and security of cloud data storage and sharing. Cloud data is more secure and private because of the blockchain's decentralized and unchangeable ledger. Using a consortium blockchain, a business model proposed in secures and enables data sharing across various clouds, assuring reliable and secure sharing procedures.

III. PROPOSED METHODOLOGY

The proposed approach has two components, one is the implementation of RSA-based cryptography, and the other is raising the security threshold at the user registration method. One of the widely used safe procedures in cloud computing is RSA, but utilizing this, other existing mechanisms have security problems. This motivates us to increase authentication's level of security.

Our proposed methodology aims to identify and mitigate unwanted traffic and packets, particularly duplicate packets. The methodology begins with registering cloud users' details by the cloud server. To ensure security, the cloud server creates an Intrusion- Finder and Detector (IFD) system, which maintains and secures user information such as name, email address, and contact number. Additionally, the IFD system allocates secondary storage ranging from 1TB to 5 TB. Within our system, users can access and retrieve files of various formats, such as audio, video, and text files. To maintain security and identify potential DDoS, we closely monitor the flow of network traffic and compare the file sizes of downloaded files with their original counterparts. If the file sizes match, it indicatesthe absence of any intrusions. However, any inconsistencies in file sizes imply possible tampering or unwanted alterations in the downloaded content. To combat this, we employ the robust RSA cryptography mechanism. Whenever a DDoS is detected, the files undergo RSA cryptography encryption during subsequent uploads and downloads. This process ensures that the content remains securely transmitted and received, effectively thwarting unauthorized individuals from manipulating or gaining access to the files.

By incorporating these measures, our methodology enhances the system's overall security by detecting and preventing unwanted traffic and unauthorized modifications to files. Implementing the IFD system, along with using RSA cryptography, ensures that user data remains protected and provides a robust defense against potential intrusions.

In our proposed technique, we want to detect and eliminate incorrect data and packets, especially duplicate packets.

A. Algorithm for IF-D

1. Begin
2. {
3. Number of user register in cloud server (U1, U2, U3…Un);
4 User details:
5. Name, mail id, personal information;
6. Gmail, YouTube, and Facebook Updated to the cloud server;
7. Visit social media websites, upload and download the file;
8. Download the file (audio, video, text, or pdf);
9. For (audio, video)
10. Check the file size before sending;
11. Check after-download file size (check actual size);
12. If there is any difference between (the actual and less than the actual size);
13. Maybe DDoS ;
14. Using cryptography RSA;
15. }
16. End

B. RSA Encryption

1. Convert the plaintext message into a numerical representation. This could be done by encoding each character to its ASCII value or using other suitable schemes.

2. Break the message into smaller blocks if it is longer than the RSA key size (usually in bytes).

3. For each block, compute the ciphertext c using the public key (n, e) as follows:

$c = m^e \pmod n$,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

where m is the numerical value of the plaintext block.

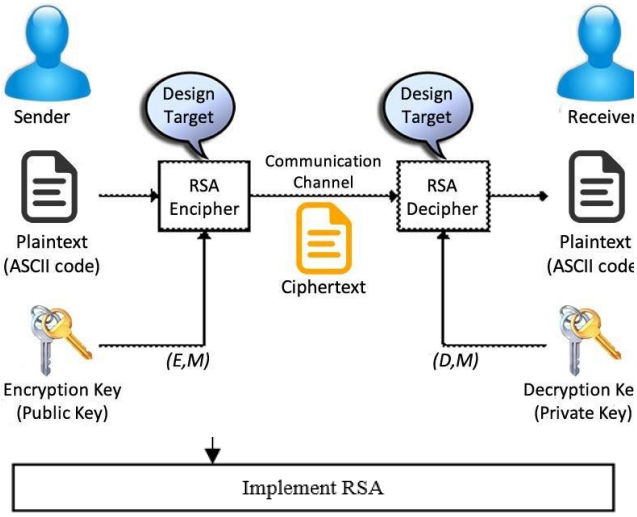

Figure 1. Proposed Methodology

C. RSA Decryption

1. Take the ciphertext block c.
2. Compute the plaintext block m using the private key (n, d) as follows:

$$m = c^d \pmod{n}.$$

Note: It's essential to ensure that the plaintext block size is smaller than the modulus n. Hybrid encryption schemes that combine symmetric encryption with RSA encryption are often used for longer messages. The symmetric key is encrypted using RSA, and the actual data is encrypted with the symmetric key using algorithms like AES.

It is essential to remember that RSA's security relies on the complexity of factoring large composite numbers, making it a good option for secure communication when used correctly with enough key sizes.

IV. Experimental Results

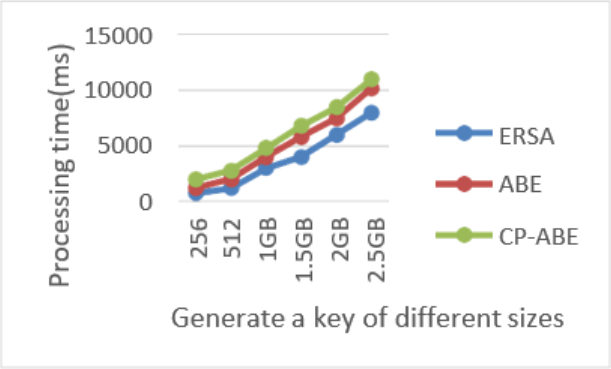

Figure 2. Processing Time vs Generate Keys of Different Sizes

Figure 2 shows the comparison work conducted between the proposed Enhanced Rivest-Shamir-Adleman (ERSA) with the existing attribute-based encryption (ABE) and ciphertext policy-attribute-based encryption (CP-ABE). In this experiment, the processing time for generating keys of different sizes by each algorithm is plotted graphically and analyzed. The x-axis represents generated keys of different sizes, and the y-axis represents the obtained time for keys generated by the algorithms. Which proposed ERSA has attained 750 ms for a 256 MB key size, 1200 ms for a 512 mb key size, 3000 ms for a 1GB key size, 4000 ms for a 1.5 GB key size, 6000 ms for a 2 GB key size, and 8000 ms for 2.5 GB key size. The graphical representation proves the proposed algorithm's time for generating keys on all ranges is much less than the others.

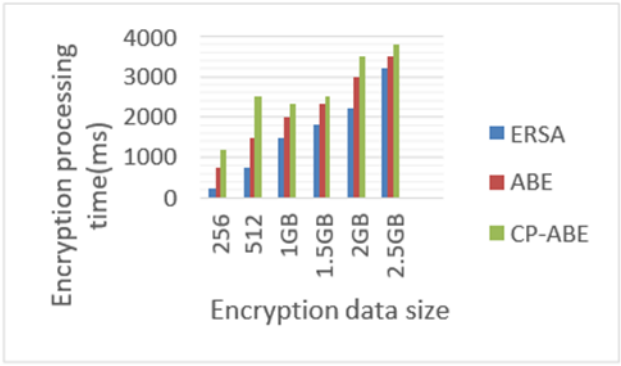

Figure 3. Processing Time vs Encryption Sizes

Figure 3 shows the comparison work conducted between the proposed Enhanced Rivest-Shamir-Adleman (ERSA) with the existing attribute-based encryption (ABE) and ciphertext policy-attribute-based encryption (CP-ABE) in the aspect of encryption processing time. In this experiment, the processing time for encryption data of different sizes by each algorithm is plotted graphically and analyzed. The x-axis represents encryption data of different sizes, and the y-axis represents the obtained time for keys generated to the algorithms. Which proposed ERSA has attained 250 ms for 256 MB data, 750 ms for 512 MB data, 1500 ms for 1GB data, 1800 ms for 1.5 GB data, 2200 ms for 2 GB data, and 3200 ms for 2.5 GB data. The graphical representation proves the proposed algorithm's time taken for processing encryption data on all ranges is much less than the others.

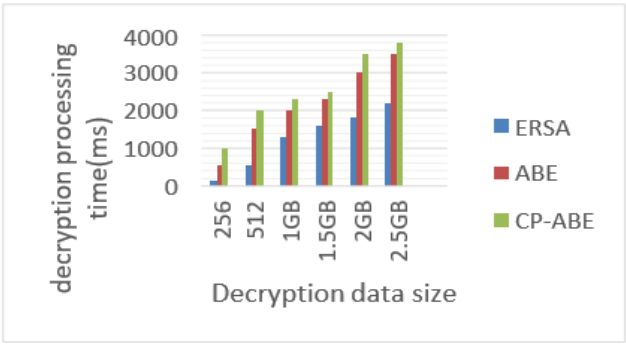

Figure 4. Processing Time vs Decrytpion Sizes

Figure 4 shows the comparison work conducted between the proposed Enhanced Rivest-Shamir-Adleman (ERSA) with the existing attribute-based encryption (ABE) and ciphertext policy-attribute-based encryption (CP-ABE) in the aspect of decryption processing time. In this experiment, the processing time for decrypting data of different sizes by each algorithm is plotted graphically and analyzed. The x-axis represents decryption data of different sizes, and the y-axis represents the obtained time for keys generated by the algorithms. Which proposed ERSA has attained 150 ms for 256 MB data, 550 ms for 512 MB data, 1300 ms for 1GB data, 1600 ms for 1.5 GB data, 1800 ms for 2 GB data, and 2200 ms for 2.5 GB data. The graphical representation proves proposed algorithm's time taken for processing and decrypting data on all ranges is very minimum than the others.

V. CONCLUSION

In this paper, we proposed an Enhanced Rivest-Shamir-Adleman (ERSA)against DDoS attacks in cloud computing. The DDoS attacks represent a significant risk, particularly the flooding attack, one of the simplest and most destructive types of attack. Most current DDoS detection techniques could be more effective at achieving security. Additionally, the time required for processing encryption and decryption is very high, leading to overall performance issues. These drawbacks are addressed by the proposed ERSA, which introduces Intrusion-Finder and Detector (IF- AD) system and RSA cryptography mechanism for enhancing security. To measure the efficiency of the proposed system, a comparison work is conducted between the proposed Enhanced Rivest-Shamir-Adleman (ERSA) with the existing attribute-based encryption (ABE) and ciphertext policy- attribute-based encryption (CP-ABE). The evaluation metrics considered are processing time for generating keys, encryption time, and decryption time. These metrics are calculated with different sizes, and the responses of each algorithm are graphically plotted for discussion. The obtained result proves that the performance obtained by the proposed ERSA is far better than the others on all metrics.

REFERENCES

[1] B. Hajimirzaei, N. J. Navimipour, "Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm." Ict Express pp. 56- 595, no. 1, 2019.

[2] J. Fontaine, C. Kappler, A. Shahid, E. D. Poorter, "Log-based intrusion detection for cloud web applications using machine learning." In Advances on P2P, Parallel, Grid, Cloud and Internet Computing: Proceedings of the 14th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC-2019), Springer International Publishing, pp. 197-210, vol.14, 2020.

[3] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions." Computer Communications pp. 2022.

[4] Z. Zhang, J. Wen, J. Zhang, X. Cai, L. Xie, "A many objective-based feature selection model for anomaly detection in cloud environment." IEEE Access pp. 60218-60231, vol. 8, 2020.

[5] A. Aldribi, I. Traoré, B. Moa, O. Nwamuo, "Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking." Computers & Security pp. 101646, vol. 88, 2020.

[6] Cheng L, Kotoulas S (2018) Efficient skew handling for outer joins in a cloud computing environment. IEEE Trans Cloud Comput 6(2):558–571

[7] Cheng L, Kalapgar A, Jain A, Wang Y, Qin Y, Li Y, Liu C (2022) Cost-aware real- time job scheduling for hybrid cloud using deep reinforcement learning. Neural Comput Appl 34(21):18579–18593

[8] Chen Z, Han F, Cao J, Jiang X, Chen S (2013) Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua Sci Technol 18(1):40–50

[9] Chen Z, Dong W, Li H, Zhang P, Chen X, Cao J (2014) Collaborative network security in multi-tenant data center for cloud computing. Tsinghua Sci Technol 19(1):82–94

[10] Namasudra S (2019) An improved attribute-based encryption technique towards the data security in cloud computing. Concurr Comput Pract Exp 31(3):e4364

[11] Qi S, Lu Y, Wei W, Chen X (2020) Efcient data access control with fine-grained data protection in cloud-assisted iiot. IEEE Internet Things J 8(4):2886–2899

[12] Nagar U, Nanda P, He X, Tan Z (2017) A framework for data security in cloud using collaborative intrusion detection scheme. In: Proceedings of the 10th International Conference on Security of Information and Networks. ACM, pp 188–193

[13] Snehi J, Snehi M, Bhandari A, Baggan V, Ahuja R (2021) Introspecting intrusion detection systems in dealing with security concerns in cloud environment. In: 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART). IEEE, pp 345–349

[14] Chiba Z, Abghour N, Moussaid K, Rida M et al (2019) Intelligent approach to build a deep neural network based ids for cloud environment using combination of machine learning algorithms. Computer Security 86:291– 317

[15] Shen M, Duan J, Zhu L, Zhang J, Du X, Guizani M (2020) Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE J Sel Areas Commun 38(6):1229–1241.