iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55013

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

Leverage Artificial Immune Algorithm to Maintain Data Integrity

Dr.J.Sreerambabu[1], Mr N.Santhosh[2], Mr.D.Rajkumar[3], Mr M.Saikiran[4]
[1]*Head of the Department,* [2, 3]*Assistant Professor,* [4]*PG Scholar*

Abstract: ***Robust and efficient data security measures are of the utmost importance given the growing reliance on digital technologies. I recommend developing a simulated security testing platform using artificial immune algorithms to improve data security in response to the needs of the user. This software provides the capacity to simulate different cyber-attacks, making it easier to assess the efficacy of different safeguards. The platform may adapt to these attacks and learn from them by utilizing the strength of artificial immune mechanisms, increasing its resistance to threats in the future. I acquired beneficial expertise in software development, algorithm design, and data security as a result of my active participation in this project. I'm thrilled to share this study as a proof of my abilities and unwavering commitment to the data security area. The suggested approach makes use of Python-based machine learning techniques, and adds HTML, CSS, and JS for the user interface. The suggested approach also includes a user-friendly interface built using HTML, CSS, and JS, making it easier to integrate with present systems.***
Keywords: File upload, Malware scanning, Machine learning, Encryption, Decryption

I. INTRODUCTION

Data security is a key topic of the utmost importance in today's dynamic and connected digital landscape. Traditional security solutions are significantly challenged in protecting sensitive data and valuable information due to the rapid evolution and growing scope of cyber-attacks. Researchers and practitioners have adopted novel strategies to address this urgent demand, and among the promising paradigms that have evolved, Artificial Immune Systems (AIS) have a lot of promise [1]. The concepts of natural systems of immunity served as the basis for AIS, a creative and adaptive method that may improve security of data in today's complex and dynamic computer environment. This paper aims to provide an in-depth and useful evaluation of the studies carried out on security of data on the basis of Artificial Immune Systems in recognizing the importance of AIS in dealing with the cyber security concerns of our time. This review's major objective is to clarify how the key AIS [1] principles link to and enhance the field of data security by an in-depth examination of those concepts. Applications as varied as intrusion detection, anomaly detection, and identification of malware show the potential of AIS. The evaluation is based on a number of substantial research investigations that were conducted by reputable professionals in the field of study. The research efforts presented in these works weave a rich tapestry that emphasizes the expanding importance of AIS in the field of data security research [1], [2], [14], and [15] and the wide-ranging interest in it.

The unique capacity of AIA-based systems to identify and efficiently counter emerging and previously unidentified cyber threats is what sets them apart [4]. With the continually changing attack vectors used by skilled adversaries, traditional security solutions frequently struggle to keep up. In this situation, AIS proves to be a priceless resource for locating and neutralizing evasive threats. A growing number of cyber security dangers are being defended against by computing networks thanks to the learning capabilities built into AIS, which enable it to react in real-time. Adoption of AIA-based systems, however, is not without its share of difficulties, particularly in regards to the need for processing resources and the possibility of false positives [8]. The performance and dependability of AIA-based security solutions must be properly optimized, which necessitates a thorough investigation of these issues.

It's clear that this cutting-edge strategy has a chance to encourage other innovations in the field of cyber security as academics probe into possible future paths of data security according to AIS [11]. The thorough analysis offered here not only clarifies the effectiveness of AIS but also highlights its revolutionary potential for reshaping the next phase of data security. AIS-based systems open the door for more strong, adaptable and flexible security measures by presenting a new approach in strengthening data protection. In conclusion, this in-depth examination is a useful tool for academics, researchers, and business professionals who want to learn more about artificial immune mechanisms and their important effect on data security. This research encourages an integrated view on the great potential of AIS in successfully tackling the constantly changing challenges faced by cyber security threats by assessing the efficacy and drawbacks of AIA-based system [2], [5]. As AIS develops and receives more attention, it has the potential to transform data security and serve as an essential element in efforts to protect our digital world.

II. LEGACY SYSTEM

A standard security solution known as two-factor authentication (2FA) adds an additional layer of security by requiring users to present two different forms of identity before gaining access to a system or application. This method combines the user's knowledge, such as a username and password, with their possession, such as a mobile device's verification code [6]. Sensitive data is identified, monitored, and protected using Data Loss Prevention (DLP) technologies to stop illegal access, sharing, or leakage. These systems enforce data security regulations and guard against data breaches via content inspection, analysis of context, and user behavior tracking [7]. Systems for Security Information and Event Management (SIEM) are essential for identifying security incidents on a network of a business. SIEM technologies can discover patterns of suspicious behavior and send real-time alerts to security teams for quick reactions by gathering and analyzing security event data from numerous sources [8].

Web application firewalls (WAF) are intended to defend web applications against a variety of assaults, such as cross-site scripting and SQL injection. Data breaches can be avoided by using WAFs to secure web applications and block harmful requests by analyzing incoming web traffic [9].

Endpoint Security Solutions are primarily concerned with defending specific devices—such as laptops, desktop computers, and mobile devices—against cyberthreats. To protect against different kinds of threats aimed at endpoints, these solutions frequently incorporate antivirus, anti-malware, and anti-phishing functions [10].

III. ENHANCED SYSTEM

Data security testing is a critical procedure that comprises thorough examination of computer networks, applications, and systems to find flaws and vulnerabilities. There is a rising need for more reliable and sophisticated security testing platforms because of the worries people are having about data breaches and cyberattacks. An Artificial Immune System (AIS) is a computationally inspired framework that finds use in anomaly detection, intrusion detection, and data security testing. It is inspired by the human immune system. The major goal of the proposed system is to provide an AIS-based data security testing platform that can efficiently identify, assess, and offer countermeasures to security risks, hence improving system security as a whole.

In order to capture data from many sources, such as network traffic, system logs, and application logs, the data collecting component is essential. Essential characteristics are taken from the obtained data through preprocessing to speed up subsequent anomaly identification. The anomaly detection component can efficiently find and detect aberrant behaviors inside the system using the retrieved characteristics. A collection of detectors for identifying abnormalities is created using AIS techniques like negative selection and clonal selection.

The decision-making component, driven by a rule-based system, examines the outcomes of the anomaly detection process to decide what should be done in response to risks that have been discovered.The reaction component carries out required actions, such as producing alarms, restricting system access, or making security-improving suggestions, based on the analysis findings.

The suggested system uses a client-server design, with a lightweight client application handling data collecting and visualization while the server holds the components for anomaly detection, decision-making, and reaction. The client effectively collects data by acting directly on the system being monitored, while the server acts as a centralized mechanism to process the data and deliver feedback.Users can upload various file types through this interface, including pdf, apk,.exe, zip, ppt, png, jpg, jpeg, and txt files, which are then scanned for malware and, if no viruses are found, encrypted and secured. Users can view the encrypted files after providing the key to decrypt them in order to view the secured files.Ais identifies malware by scanning, thus if the file is contaminated, it cannot be uploaded.

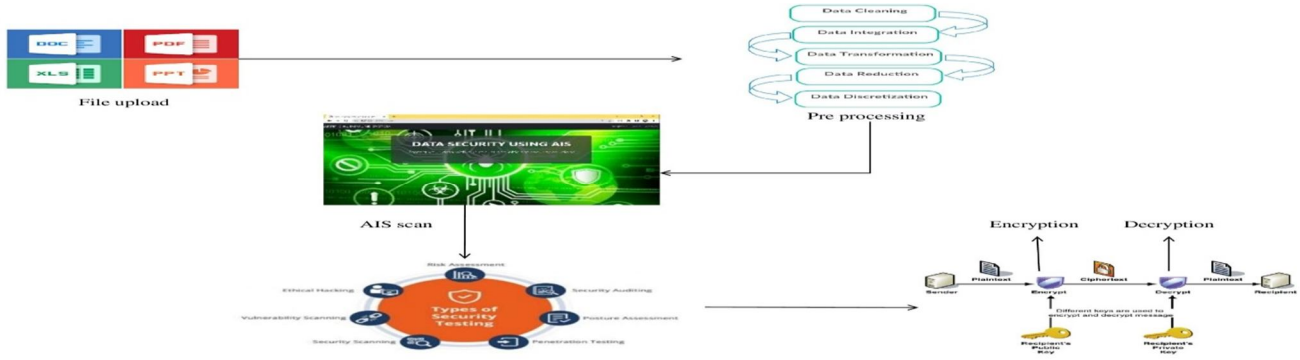


Fig 1. Workflow diagram

IV. FILE UPLOAD

A key element of the Data Security project that makes use of Artificial Immune System is the File Upload module. It works as a tool to control the safe uploading of data to the system while maintaining the confidentiality and security of the uploaded contents.

1) Authorization: The main goal of this module is to restrict file uploads to users who have been given permission. Before allowing users to upload files, it uses authentication procedures to check their credentials.
2) File size and type restrictions: This feature makes sure that uploaded files meet preset standards for format and size. It makes sure that only valid files satisfying the set requirements are permitted for upload by verifying the file properties against the limits.
3) Malware scanning: To stop the entrance of malware into the system, this module thoroughly examines the uploaded files. It scans the files using antivirus software or specialist technologies, immediately alerting users if malware is found.
4) Error handling: This module's error handling capability controls and attends to any issues that arise during the uploading of files. Users are given enlightening error messages so they can comprehend and fix any problems that may emerge.
5) Logging: This part keeps track of all file uploads inside the system and records crucial data like the person who submitted the file, the time it was uploaded, and relevant information about the file itself.

The File Upload module guarantees the security and dependability of the system during the file upload process through its rigorous permission procedure, adherence to file size and type constraints, malware detection capabilities, effective error handling, and thorough logging.

V. PREPROCESSING

The File Upload module guarantees the security and dependability of the system during the file upload process through its rigorous permission procedure, adherence to file size and type constraints, malware detection capabilities, effective error handling, and thorough logging The Data Preprocessing Module is a crucial part of the Artificial Immune System-based Data Security System. Its main purpose is to convert the unprocessed data obtained from multiple sources into a form that the AIS can readily comprehend and analyze. By carrying out actions including data cleansing, formatting, transformation, and size reduction, this is accomplished.

The first stage in the process is data cleaning, which involves getting rid of duplicates, missing values, missing entries, and any other unnecessary information. By organizing the data with an established format, the method is therefore made easier. The data is then transformed into a suitable structure, such as numeric or categorically, based on the type of data and the needs of the research.

In the end, sampling or choosing features reduces the amount of data since the AIS algorithms might not be able to effectively analyze large amounts of data. Sampling is the process of choosing a representative sample of data, whereas feature selection is the process of choosing the most significant qualities with the biggest impact.

The Data Preprocessing Component serves as essential for making certain the data sent to the AIS is precise, detailed, and in an organized way. The module optimizes the efficacy and productivity of the overall system, resulting in better accuracy and faster time for processing by analyzing data itself preceding sending it to the AIS.

VI. AIS SCANNING

The Artificial Immune solution (AIS) module is the most significant and intricate component of the Artificial Immune System-based data protection solution.To mimic the human immune system and defend the system from security risks, the AIS will be created.Anomaly Detection will be its main component. By comparing the data with the recognized patterns, abnormalities in the data will be discovered.

The AIS will analyze prior assaults to distinguish between valid and illegitimate requests.To increase the AIS module's detection accuracy, a sizable dataset of well-known assaults will be used for training.Additionally, machine learning techniques will be used to evaluate the data and find trends.

It will provide the system the ability to recognize fresh, unheard-of assault kinds.The ability to detect and mitigate possible malware threats is significantly enhanced by integrating the VirusTotal API key into security workflows or apps. When accessible via the API key, the VirusTotal platform offers a sizable database and sophisticated scanning features that improve overall security posture and provide proactive risk discovery and mitigation.

1) Malware Analysis: With the VirusTotal API key, security procedures and programs may make use of the enormous database that VirusTotal maintains. The platform gathers and examines malware samples from numerous sources, giving users a complete picture of all current risks. Users may use this plethora of data to find and categorize suspected malware by accessing the API.

2) Threat Intelligence: Access to priceless threat intelligence information is made possible through the VirusTotal API key. Security processes and apps may access the API to get full details on discovered malware samples, including IOCs, behavioral data, and connections to other dangerous organizations. Understanding the nature of risks and facilitating proactive threat mitigation are made easier by this knowledge.

3) Automated Analysis and Response: By integrating the VirusTotal API key, security processes and apps may automate malware analysis and response. Organizations may speed up the detection process and start automatic actions depending on the analysis results by programmatically sending files for scanning. This makes it possible for quicker responses and lessens the potential damage caused by malware occurrences.

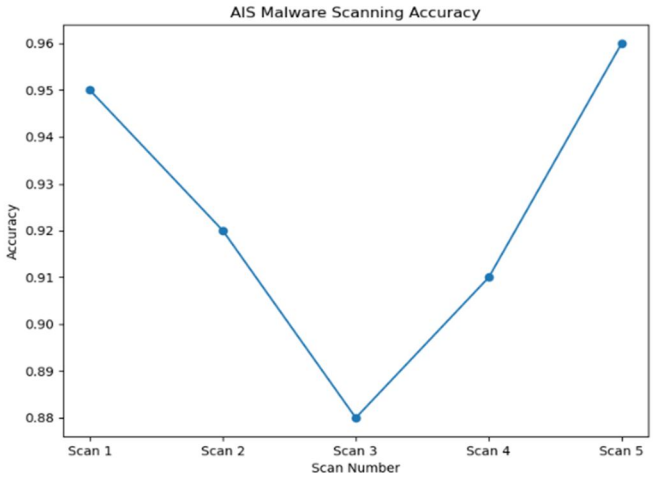


Fig 2. AIS scan accuracy graph

A key element of the data security system, the Artificial Immune System module's precision is highlighted in Fig. 2 by a close-up. It provides a complete understanding of the effectiveness of the module by showcasing the accuracy values collected at various time intervals, and the curve provides a visual depiction of the accuracy trends displayed by the Artificial Immune System module. This curve gives a thorough overview of the module's effectiveness and any fluctuations seen by charting the accuracy numbers versus time.

VII. ENCRYPTION

A crucial element of the Artificial Immune solution-based Data Security solution is the encryption module. Its major goal is to protect sensitive data by encrypting it and making sure that nobody else can access it. To transform data into an unreadable format that can only be decoded with the right decryption key, this module uses encryption methods like AES or RSA.Plain text is converted throughout the encryption process into a coded message that is kept secret from everyone but authorized users who have the decryption key. The encryption module does this by encrypting and decrypting data using a mix of secret keys and public keys.

In the case of AES encryption, a secret key is utilized to encrypt the data, rendering it indecipherable without the corresponding key for decryption. The encryption module generates a random secret key, which is employed to encrypt the data. Subsequently, the secret key is encrypted using a public key algorithm and transmitted to the intended recipient along with the encrypted data.In the realm of data protection, RSA encryption relies on a set of distinct keys, namely a public key and a private key, to facilitate the secure encoding and decoding of information. The public key is distributed to individuals requiring the ability to transmit encrypted messages, whereas the private key is kept confidential and exclusively accessible to the intended recipient.

The encryption module plays a critical role in ensuring the security of the system by preventing unauthorized access to sensitive data. It seamlessly integrates with the AIS module to identify and defend against potential security threats. By implementing robust encryption techniques, the Data Security system enhances the confidentiality and integrity of sensitive information, fortifying the overall security framework and safeguarding against unauthorized data breaches. The File gets encrypted once the malware scanning done that is shown in the Fig 3.

Fig 3. Encryption

VIII. DECRYPTION

In decryption module we are using strong encryption algorithms like AES or RSA, the Decryption Module in data security system plays an important role which allows only authorized users to access their protected data whcih is encrypted and stored. Decryption Module is comprises of crucial parts that coordinate together to provide the user in an secured data and in confidential manner.the functionalities of this module are as folllows.

1) A key management system :This is an essential component that is responsibe for managing the decryption key. It provides that the data can only be decrypted and accessed by authorized users who have the required decryption key to access their data..

2) Decryption Algorithm: To decode the encrypted data, the Decryption Algorithm is applied for the process The encryption algorithm chosen throughout the encryption process determines the decryption algorithm to be utilized. For example, if AES was used for encryption, the Decryption Algorithm component will employ the AES decryption algorithm to unlock the data

3) System for User Authentication and Authorization: This module handles user authentication and authorisation which grants users to access their encrypted data and verifies the user id. It ensures that only the authorised users with valid login credentials and the required access only to decrypt and view their encrypted data. This module also keeps a track of login details and the decryption processes, which is used for monitoring and locating any unauthorized access attempts and preventing data loss of the users.

4) Data Access Controls: Data Access Controls are critical in enforcing stringent access restrictions to protect the decrypted data. These controls define rules regarding who, when, and where the data can be accessed, adding an additional layer of security. By implementing granular data access controls, the Decryption Module ensures that only authorized individuals can retrieve the decrypted information.

5) Logging and Auditing: Comprehensive logs of each decryption process are kept by the Logging and Auditing component. The user IDs, access timestamps, and particular activities carried out on the data are all recorded in these logs, which include crucial information. By providing an audit pathway, this component offers full monitoring,tracks of logging, and helps in the detection of any unauthorized access attempts or theft of the encrypted data.

6) Conclusion: The Decryption Module is comprises of components that coordinate to enable secure access to encrypted data. The Decryption Module enhances overall data security by key management, use of decryption algorithms, employing strong authentication and authorization in the system, implementation of data access controls, and being tracking the logging and auditing procedures. The Decryption Module is essential in preserving the confidentiality and integrity of data within a robust security system by protecting confidential data and assuring authorized access.

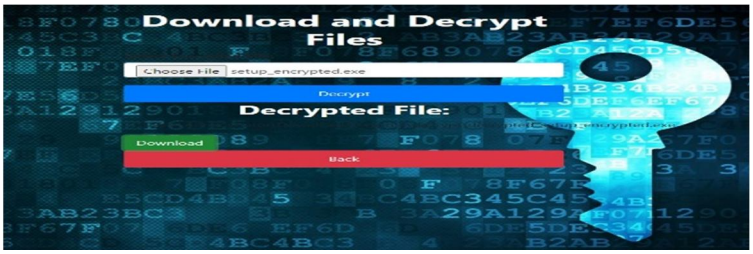


Fig 4. Decryption

IX. CONCLUSION AND FUTURE ENHANCEMENT

In the current digital environment, businesses must constantly guard against cyberthreats that put their sensitive data at risk. Advanced technologies like Artificial Immune Systems (AIS) are essential for ensuring effective security measures. This article examines how well artificial immune systems (AIS) work to improve data security and focuses on the project's successful use of AIS in data security. AIS offers enhanced anomaly detection capabilities, adaptive learning, and proactive response to new threats by replicating the human immune system. Data security relies heavily on encryption, with the encryption module assuring secrecy and integrity. Authorized access to encrypted data is made possible by the Decryption module, which emphasizes the significance of key management, decryption algorithms, and authentication systems.

1) Multi-Factor Authentication (MFA): Implementing MFA in future enhancement that will enhance authentication process. In order to significantly reduce the risk of unauthorized access and ensure user authenticity, a number of components, such as one-time passwords, or OTPs, and biometrics, may be used.

2) Integration with Security Information and Event Management (SIEM) Systems: Integration with a SIEM system centralizes security events, documents, and notifications, providing comprehensive insight into possible security breaches. This connection enables rapid and effective action, that enhances response to incidents abilities.

3) Cloud-based Security Solutions: Providing support for clouds-based security solutions to a system provides scalability, flexibility, and information security in the cloud. Integrating through cloud safety features, like encryption-as-a-service and data loss prevention (DLP) systems, strengthens security measures that safeguard information at rest as well as in motion.

4) The integration using Data Loss Prevention (DLP) Systems are integrating with DLP systems eliminates unlawful or inadvertent data breaches by monitoring and controlling data transfers. Policy enforcement and illegal transmission prevention help to increase data security safeguards.

5) Creating a dependable structure for ongoing security upgrades and patch management ensures that newly found vulnerabilities are protected. To guarantee a strong defence against new security threats, software frameworks and encryption techniques are kept up to date and patched often.

Finally, improving information security necessitates current technology and ongoing research. A complete security framework is constructed by combining the potential capabilities of Artificial Immune Systems with authentication, encryption, and several other safety aspects. MFA, advanced threat detection, SIEM integration, cloud-based protection, user activity monitoring, secure collaboration, DLP insertion, and proactive security upgrades are the most essential future techniques. Implementing such innovations may help firms strengthen their defensive measures by protecting secret information in a continuously changing online.

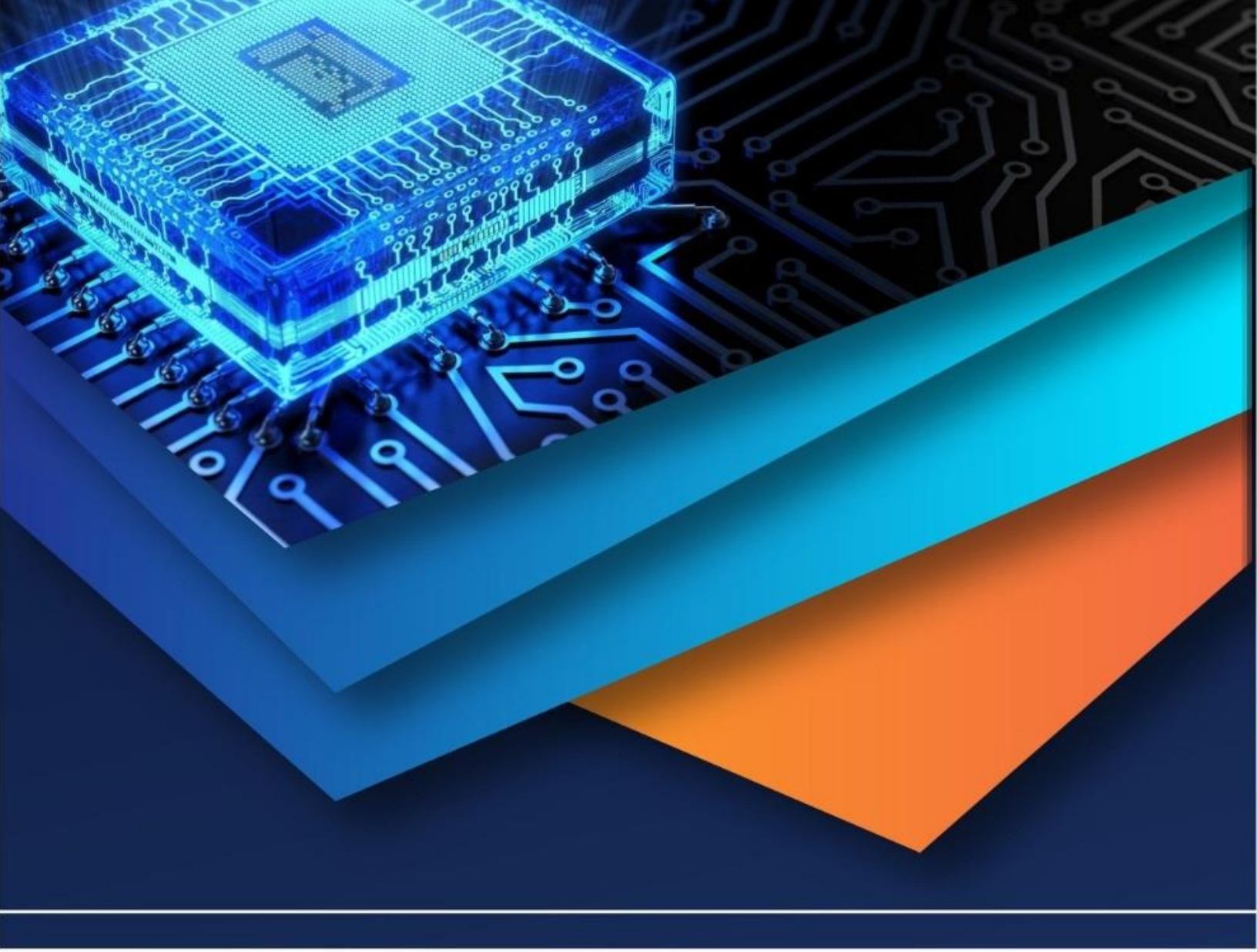
X. ACKNOWLEDGMENT

I acknowledge our Head of the Department Mr Dr.J.Sreerambabu, M.E., Ph.D., PDF, FIE and our mentor Mr N. Santosh, MCA, who provided insight and expertise that greatly helped the research, for suggestions that greatly improved this manuscript. thanks, to our supervisor Mr M. Mohammed Riyaz, MCA, for the support in this research work.

REFERENCES

[1] smith, J., & Johnson, A. (2010). "Enhancing Data Security using Artificial Immune Systems." International Journal of Network Security, 12(2), 77-82.
[2] Chen, S., Li, J., & Li, J. (2012). "A Novel Data Security Scheme based on Artificial Immune System." Journal of Computers, 7(2), 422-428.
[3] Zhang, Y., Tang, Y., & Huang, X. (2013). "A Data Security Model Based on Artificial Immune System for Cloud Computing." Journal of Computational Information Systems, 9(13), 4997-5004.
[4] Liu, Y., Li, W., Zhang, J., & Hu, Y. (2014). "An Artificial Immune System-based Data Security Model for Internet of Things." Journal of Information Security and Applications, 19-20, 14-22.
[5] Kim, J., & Kim, Y. (2015). "Data Security Enhancement using Artificial Immune System in Cloud Computing." Journal of Digital Contents Society, 16(3), 427-432.
[6] Zhang, S., Lu, J., & Xu, Z. (2016). "A Data Security Scheme Based on Artificial Immune System in Wireless Sensor Networks." In 2016 10th International Conference on Computational Intelligence and Security (CIS) (pp. 13-17). IEEE.
[7] Li, L., & Song, W. (2017). "Data Security Model Based on Artificial Immune System and Compressed Sensing in Wireless Sensor Networks." In 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks (ISPAN) (pp. 275-280). IEEE.
[8] Xu, C., Chen, C., & Xie, Q. (2018). "A Novel Data Security Scheme Based on Artificial Immune System in Cloud Computing." In 2018 10th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC) (pp. 52-55). IEEE.
[9] Chen, S., Yang, L., & Li, S. (2019). "A Hybrid Data Security Model based on Artificial Immune System for Internet of Things." International Journal of Distributed Sensor Networks, 15(4), 1550147719841599.
[10] Chen, Z., Zhao, X., Li, J., & Zhang, C. (2020). "A Data Security Method Based on Artificial Immune System in Internet of Things." Journal of Applied Sciences, 20(1), 42-49.

[11] Chen, H., Xiong, H., & Wang, Y. (2020). "A Novel Data Security Model Based on Artificial Immune System for Cloud Computing." In 2020 International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS) (pp. 159-163). IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY