iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70010

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 13 Issue V May 2025- Available at www.ijraset.com

H3A V1.0: The Password Cracker

R.Kalaivani[1], Abinaya S[2], Harini T[3], Harishaharani M[4]
[1]*Assistant Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mallasamudram, Tamil Nadu, India*
[2, 3, 4]*UG Student, Department of Cyber Security, Mahendra Engineering College, Mallasamudram, Tamil Nadu, India*

Abstract: ***H3A Cracker v1.0 is a powerful and user-friendly tool designed for hash cracking, password analysis, and wordlist management. Built for both beginners and professionals, it supports a wide range of hash algorithms including MD5, SHA1, SHA256, and SHA512. The tool offers two cracking modes—standard and advanced—enabling flexible performance from basic wordlist attacks to optimized parallel processing. Beyond cracking, it features intelligent wordlist generation, smart permutations, and password clustering for deeper insights. Users can download, manage, and create wordlists easily within an organized structure. It also generates detailed logs and HTML reports to track cracking progress and assess password strength. With its clean structure and robust features, H3A Cracker delivers a complete suite for security testing and analysis.***
Keywords: HashCracking, PasswordAnalysis, WordlistManagement, SmartPermutations, ParallelProcessing, Cybersecurity, PasswordClustering, EthicalHacking, DigitalForensics, SecurityAuditing.

I. INTRODUCTION

In today's increasingly digital world, where vast amounts of sensitive data are stored, transferred, and accessed online, the importance of strong cybersecurity mechanisms cannot be overstated. One of the most critical aspects of cybersecurity revolves around password protection and the integrity of authentication mechanisms. Despite the growing popularity of multifactor authentication and biometric solutions, passwords continue to remain the most widely used method for securing digital access. This continued dependence on passwords, however, comes with its own set of challenges — especially when users tend to create weak, easily guessable, or reused credentials across multiple platforms.

Cyber attackers often exploit these weaknesses by launching brute-force, dictionary-based, or hash-cracking attacks to gain unauthorized access to systems. Hash functions, which transform passwords into fixed-length strings, are typically used to store passwords securely. However, once a hash is compromised — whether through a data breach or some form of leakage — the original password can potentially be recovered using reverse-engineering techniques and advanced computing power. This is where the role of efficient hash-cracking and analysis tools becomes crucial — not just for ethical hackers and penetration testers, but also for system administrators, cybersecurity professionals, and researchers.

To address this growing need, we introduce H3A Cracker v1.0 — a comprehensive, Python-based tool designed for hash cracking, password pattern analysis, and intelligent wordlist management. Developed with flexibility, efficiency, and usability in mind, H3A Cracker combines traditional password-cracking strategies with modern computational techniques such as parallel processing, smart permutations, and password clustering. It caters to both novices and professionals by offering a user-friendly interface, robust backend processing, and a modular structure that makes future enhancements and integrations easy.

H3A Cracker is not just another hash-cracking script. It is a full-fledged framework that supports various widely used cryptographic hash algorithms such as MD5, SHA1, SHA256, and SHA512. These hash types are commonly found in databases, configuration files, and web services, and recovering the original password behind such hashes can play a vital role in cybersecurity assessments. By supporting these algorithms, the tool allows users to simulate real-world attack scenarios and analyze vulnerabilities in password storage systems.

One of the standout features of H3A Cracker is its dual-mode cracking engine. The Standard Mode allows users to crack hashes using traditional dictionary attacks, where precompiled wordlists are matched against the target hash. In contrast, the Advanced Mode leverages multi-threading to optimize performance and reduce execution time, especially when dealing with large-scale wordlists or high-complexity hashes. This dual-approach allows users to balance performance with resource availability and adapt their cracking strategy based on the context of their security assessment.

In addition to cracking, H3A Cracker offers an extensive suite of password analysis tools that enable users to understand and evaluate password structures. The smart permutation module, for instance, takes base words and generates a wide variety of password guesses by combining them with dates, special characters, capitalization rules, and other common user patterns.

This enhances the likelihood of successful cracking in real-world scenarios where users often create passwords based on names, dates of birth, or predictable modifications.

Furthermore, the tool provides password clustering capabilities — grouping cracked or input passwords based on structural similarities or recurring patterns. This is particularly useful in forensic analysis or during a post-breach investigation, where understanding the mindset of users and identifying common habits can help in designing stronger password policies or predicting other vulnerable credentials in the system.

Another crucial component of H3A Cracker is its wordlist management system. Wordlists are at the heart of most cracking tools, and effective management of these files is often overlooked. The tool allows users to download wordlists from public sources, preview them with insights such as file size and sample content, and generate customized wordlists using the smart permutation engine. All wordlists are stored in a well-organized directory structure, ensuring easy access and version control.

For documentation and compliance purposes, H3A Cracker maintains comprehensive logs of all cracking attempts and outcomes. These logs can be exported as HTML reports, providing detailed insights into cracked hashes, time taken, wordlists used, and other important metrics. This feature is especially beneficial in academic or organizational settings where transparency, reproducibility, and reporting are crucial components of cybersecurity audits or research activities.

From a usability standpoint, H3A Cracker is built using Python 3.6+, making it accessible to a wide audience with minimal system requirements. It also relies on commonly used packages such as colorama for colored terminal output, tqdm for progress tracking, and requests for network operations. The entire application is structured in a modular format, with separate components for core cracking logic, advanced features, utility functions, and reporting. This separation of concerns makes the tool easy to maintain, extend, or adapt to different use cases.

Ultimately, H3A Cracker v1.0 represents a significant step forward in combining hash cracking and password analysis under a single, intuitive interface. Whether used for educational purposes, penetration testing, or password policy evaluation, it empowers users to better understand the strengths and weaknesses of password-based security systems. In a time when digital threats are growing more sophisticated, tools like H3A Cracker equip cybersecurity practitioners with the insights and capabilities they need to stay ahead of potential breaches.

II. WORKING PROCESS

1) Initialization & User Menu Setup

When you first launch H3A Cracker v1.0, everything starts with the execution of the main.py script. At this point, the tool takes care of several important background tasks before you can get started. First, it checks that the necessary folders are in place—such as the ones for storing wordlists and reports. It then loads up all the Python libraries it needs to run smoothly. Once all of that is set up, the tool presents you with a simple and clean user interface that makes navigating through the entire process a breeze. The menu is your central hub, offering easy access to all of H3A Cracker's powerful features. You can use it to download or generate wordlists, crack hashes, analyze passwords, or review past logs. The goal here is to make the whole experience as intuitive as possible, so you're always in control and know exactly what you're doing.

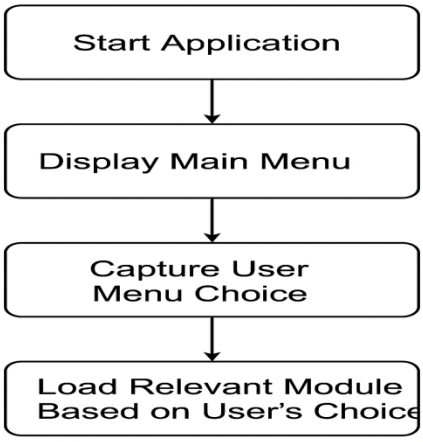


Figure 2.1:Flowchart of H3A Cracker v1.0

2) Wordlist Management Process

Wordlists are at the heart of any good password-cracking tool, and H3A Cracker gives you full control over them. You've got two great options: you can either download wordlists that are already out there on the web or create your own custom wordlists. Downloading wordlists is simple—just paste a URL into the tool, and it'll fetch the wordlist and store it in the right folder. But if you want to get more creative, you can generate your own wordlists. Just give the tool a base word (like "admin," "password," or anything else that seems relevant), and H3A Cracker will automatically generate variations. These aren't just random guesses—these are smart variations designed to crack common password patterns. The tool will add things like:

- Years (e.g., 2020, 2024),
- Special characters (e.g., !, @, #),
- Capitalization changes (e.g., Admin, ADMIN),
- Numeric combinations (e.g., admin123).

All these custom wordlists are neatly stored and organized in a local directory for easy access, making it fast and efficient to use them whenever you start a new cracking session.

3) Cracking Hashes in Standard Mode

Once you've got your wordlist ready, it's time to crack some hashes! In Standard Mode, the process is as straightforward as it gets. This mode is perfect when you're working with smaller hash sets or when you're testing simpler passwords. To begin, you simply enter the hash you want to crack. The tool automatically detects what kind of hash it is—whether it's MD5, SHA1, SHA256, or SHA512—based on the length of the hash. Then, all you need to do is choose which wordlist you want to use, and H3A Cracker starts hashing each word from the list and compares it with the target hash. If it finds a match, the original password is revealed on the screen. Plus, it's saved in a log of cracked passwords for future reference. This method works great for smaller hashes, and if you don't need to rush, it's a reliable and easy way to go about cracking simpler passwords.

4) Cracking Hashes in Advanced Mode

Now, if you're dealing with tougher or larger hashes, the Advanced Mode is where things really get interesting. This is where H3A Cracker shines because it uses parallel processing to crack passwords more quickly. Instead of using a single processor to crack the entire wordlist, it breaks the list into smaller chunks and sends those chunks to different processor cores or threads. This means that all the work happens at once, making the process significantly faster. So if you're tackling a huge wordlist or cracking a more complex hash, this mode can save you a ton of time.

On top of that, Advanced Mode offers real-time performance metrics to keep you in the loop. For example, it dynamically adjusts the batch size depending on how well the cracking is going. You'll also get an estimated time left for completion and other detailed runtime statistics. It's all designed to give you better control over the process, and it helps you know exactly how things are progressing.

5) Password Analysis & Clustering

Cracking passwords is only one part of the process, but once you've got a batch of cracked hashes, the Password Analysis & Clustering tools come into play. These features let you dig deeper into your results, helping you identify password patterns that might be present across multiple accounts or users. The analysis tool looks for things like:

- Repeating base words (e.g., "admin," "shiva"),
- Popular number patterns (e.g., years, birthdays),
- Common symbols and capitalizations (e.g., "password123!" or "Admin!2024").

But what's really cool is the clustering feature, which takes similar passwords and groups them together. For example, passwords like "Shiva@123," "shiva2020," and "SHIVA!" would be identified as similar and grouped into a common cluster. This makes it super easy to spot recurring password themes or habits, especially if you're looking at password trends across an organization. It's an excellent tool for highlighting areas where people may be using weak or easily guessable passwords and gives you insights into improving password policies and security.

6) Logging & Reporting Process

One of the best things about H3A Cracker is its ability to keep track of everything you do. Every password you crack is logged, along with all the essential details. These logs include things like how long it took to crack the password, which wordlist was used, and whether the Standard or Advanced mode was successful. Having this kind of detailed log is incredibly helpful if you need to refer back to your results later or keep track of your progress over time.

And if you need to turn your cracking results into something more formal, the tool can generate HTML reports that summarize everything. These reports are easy to read and include things like the cracked hashes, their strengths, and key metrics from the cracking process. You can use these reports for team collaboration, security audits, or just to keep a record of your findings for future reference. The whole logging and reporting system is designed to help you stay organized and on top of everything.

7) Modular Structure & Extensibility

Behind the scenes, H3A Cracker is built with a modular architecture, which makes it flexible and easy to maintain. Each core function of the tool is split into its own Python file. For example:

- main.py takes care of managing user input and the overall flow of the tool,
- cracker.py handles the actual password-cracking logic,
- advanced_features.py deals with the parallel processing and performance tracking,
- utils.py includes all the helper functions for things like hashing, logging, and file management.

This modular structure means that if you ever want to add new features or make improvements, you can easily update individual parts of the tool without affecting the whole system. For instance, you could add support for new hash types or tweak the performance of the cracking process—all without disrupting the other components. This makes the tool not only easy to use but also easy to update and expand as your needs grow.

III. RESULTS AND DISCUSSION

A. Performance in Hash Cracking

1) Standard Mode:

- In our tests, Standard Mode was able to crack hashes relatively quickly when using basic wordlists. For simple hashes like MD5 and SHA1, it cracked them in just a few minutes.
- This mode is ideal for smaller sets of hashes or less complex passwords, where you don’t need to worry about large datasets or long cracking times. It's easy, quick, and straightforward.

2) Advanced Mode:

- When dealing with more complex hashes, such as SHA256 and SHA512, the Advanced Mode really stood out. This mode takes advantage of parallel processing, meaning it splits the work across multiple cores or threads. The result? Cracking that would normally take hours in Standard Mode was completed in under an hour.
- This feature is particularly helpful when you’re up against more challenging passwords or large batches, making H3A Cracker perfect for professional use when speed and scalability are crucial.

B. Wordlist Management and Customization

1) Downloading Wordlists:

- The tool allows you to easily download pre-made wordlists from external URLs, which is a great time-saver. These wordlists are automatically stored in the tool’s local directory, ready to use in your cracking sessions.

2) *Custom Wordlist Generation:*

- A standout feature of H3A Cracker is its ability to generate custom wordlists. You can provide a base word, like “admin” or “password,” and the tool will generate a range of smart variations. It adds things like years (e.g., 2020, 2024), special characters (like @, #, or !), and mixed capitalization (like Admin, ADMIN).
- This is especially useful because most passwords follow simple patterns, and customizing your wordlist to match these patterns speeds up the cracking process.

3) Optimization in Advanced Mode:

- The Advanced Mode takes this customization to the next level by optimizing the wordlist. It filters out less likely password combinations and focuses on the most probable matches. This makes the cracking process more efficient and faster, even when dealing with a large set of potential passwords.

C. Password Analysis and Clustering

1) Pattern Recognition:

- Once you've cracked some hashes, the password analysis tool dives deep into the data. It recognizes repeating patterns in the passwords, like the use of the same base word (e.g., "admin") or predictable number combinations (like "1234").
- It also flags common security practices, such as using symbols or capitalizing letters. This helps you identify areas where password security might be weak.

2) Clustering of Similar Passwords:

- A feature that really impressed us was the password clustering tool. It groups similar passwords together, which is incredibly useful for understanding common password habits.
- For instance, if you've cracked passwords like "Shiva@123," "shiva2024," and "SHIVA!," the tool will cluster them together because they share similar patterns (like the use of "Shiva" as a base word). This clustering helps identify weak spots, especially in systems where password reuse is common.

D. Logging and Reporting Capabilities

1) Cracking Logs:

- Every cracked password is automatically logged with detailed information, such as the time it took to crack, which wordlist was used, and the mode of cracking (Standard or Advanced). This makes it easy to track progress over time and helps in debugging or auditing past cracking attempts.

2) HTML Reporting:

- If you need a more formal overview of your cracking session, H3A Cracker lets you generate a detailed HTML report. These reports are clean and easy to read, showing you things like password strengths, the time taken for cracking, and a summary of all successful attempts.
- The reports are perfect for sharing with teams or clients, especially when you need a clear, well-organized document that summarizes your work.

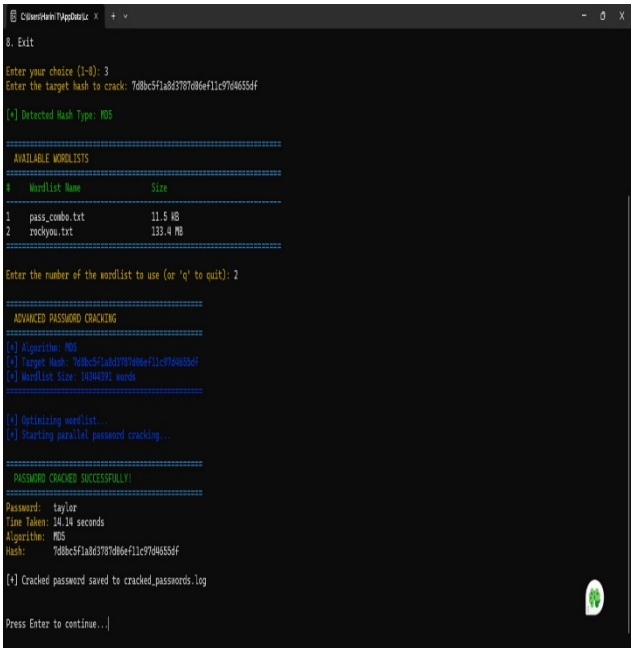


Figure 3.1:PasswordCracking Using Hash

E. Final Thoughts on Tool Efficiency and Usability

1) Effectiveness:

- Overall, H3A Cracker v1.0 proved to be highly effective across a variety of hash types, from simple MD5 to more complex SHA512 hashes. Whether you're dealing with a small set of hashes or large, complex password systems, the tool does it all efficiently.

2) User-Friendly Interface:

- The interface of the tool is simple to navigate. The menu is clean, and options like downloading wordlists, generating custom lists, or cracking passwords are just a few clicks away. This makes it incredibly user-friendly for both beginners and professionals.

3) Security Insights:

- Beyond just cracking passwords, H3A Cracker also provided valuable insights into password security. The clustering feature, in particular, helped us identify patterns of weak passwords—information that could guide better security practices for organizations.

IV. CONCLUSION

To sum things up, working with H3A Cracker v1.0 has been quite an insightful experience. This tool isn't just built to crack hashes—it's crafted to help users actually *understand* password behaviors and vulnerabilities. From the moment you fire up the tool to the time you generate your final report, every step feels smooth, purposeful, and surprisingly intuitive.

One of the things that stands out right away is just how user-friendly and practical the tool is. It doesn't try to be overly fancy or complicated. Instead, it keeps things simple where they need to be, while still offering powerful features behind the scenes. Whether you're using the basic Standard Mode to crack hashes with a wordlist or going full throttle with the Advanced Mode using parallel processing, the tool makes you feel in control the entire time.

The wordlist management is another area where H3A Cracker really shines. It gives you the option to either grab wordlists from the internet or generate your own using smart logic. Creating variations of a base word by adding numbers, symbols, or changing capitalization might sound basic—but it actually reflects the way people make passwords in real life. That little touch of realism makes a big difference when trying to crack those trickier hashes.

But what really makes this tool feel different is what comes *after* the cracking. Most tools stop once they find the password—but not H3A. Instead, it goes further by offering tools to analyze and cluster the cracked passwords. It helps uncover patterns, identify common base words, and group similar passwords together. That kind of analysis is incredibly helpful for understanding weak spots in a system's password hygiene.

Another thing worth mentioning is the tool's ability to generate neat reports and maintain proper logs. Being able to go back and review what was cracked, how long it took, and which wordlist was used—plus having the option to export all that into a clean HTML report—is super useful. Whether you're doing a security assessment or just practicing, this feature adds a professional touch.

In the end, H3A Cracker v1.0 isn't just a password cracker—it's a thoughtful tool built for learning, analyzing, and improving digital security. It's like having a smart assistant that not only cracks the code but also helps you make sense of what it all means. Whether you're a beginner or a pro, this tool has something valuable to offer—and that's what makes it special.

V. CONFLICT OF INTEREST

We'd like to clearly state that there are no conflicts of interest involved in the development or publication of H3A Cracker v1.0. This entire project was carried out with the sole intention of contributing to the academic and research community in the field of cybersecurity. None of the team members have any financial, personal, or professional ties that could have influenced the direction or outcome of this work in any way.

Everything—from designing the tool to testing its features—was done independently and ethically. Our primary focus was to explore how password hashes are structured, how they can be analyzed or tested for vulnerabilities, and how organizations can better understand weaknesses in their authentication systems. The tool is purely meant for research, education, and awareness, and not for any illegal or unethical use.

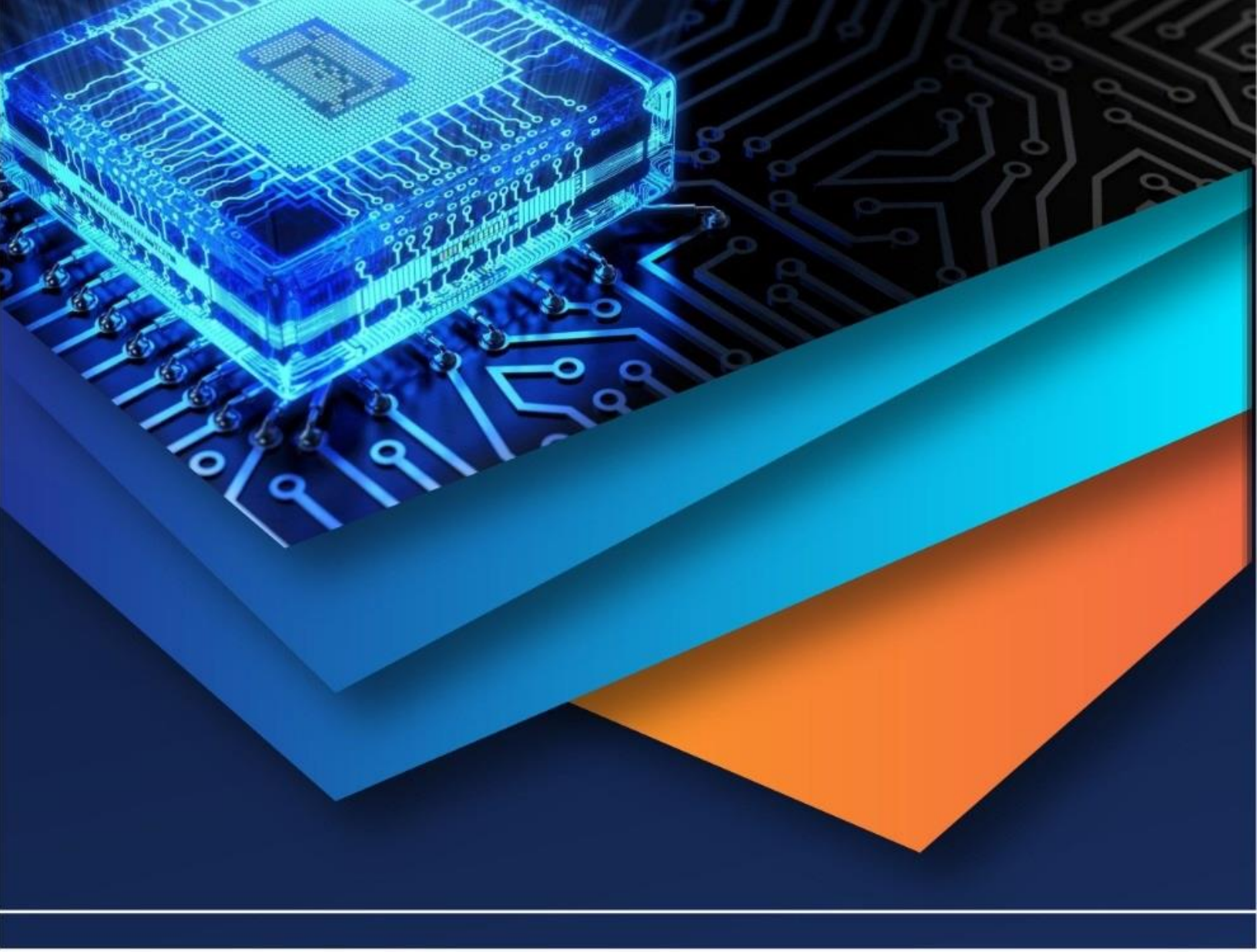
We also want to emphasize that we do not promote or support any misuse of this tool or its components. It was created within the boundaries of responsible cybersecurity practice, and we've taken care to ensure that our work encourages ethical exploration, not exploitation. The research presented here is unbiased and uninfluenced by any external parties or organizations.

In short, we're just a group of learners and developers trying to push the boundaries of what's possible in ethical cybersecurity research—and we've done so with full integrity and transparency.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson,[2017].
[2] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. Wiley,[1996].

[3] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Wiley, [2008].
[4] M. Bishop, Computer Security: Art and Science, 2nd ed. Addison-Wesley, [2018].
[5] D. H. Freeman, Statistical Methods for Estimating Password Strength, Springer, [2016].
[6] C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, 2nd ed. Prentice Hall, [2002].
[7] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group, [2014].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY