Advanced Sciences and Technology Journal

ASTJ vol. 2, no. 1 (2025), P 1015
10.21608/astj.2024.341331.1015
https://astj.journals.ekb.eg/

Robustness of Cloud Security against Brute-force Attack

Zakaria Hassan Abdelwahab [1], Ahmed Gamal Abdellatif [2], Islam M. Ibrahim [3*], Mohamed I. Ahmed [4] and Adham Ahmed Elmahallawy [5]

[1]*Communication Department, ECCAT, Suez Canal University, Ismailia, Egypt.*
[2] *Department of Communications and Electronics Engineering at the Egyptian Military Academy (Air Defense College), Egypt.*
[3]*Software Engineering and Information Technology, Faculty of Engineering and Technology, Egyptian Chinese University, Cairo, Egypt.*
[4] *Mechatronics Engineering Department, Faculty of Engineering and Technology, Egyptian Chinese University, Cairo, Egypt.*
[5] *Higher institute of Engineering and Technology, king Mariout , Alexandria, Egypt.*
[*]*islam.mohammed@ecu.edu.eg*

ARTICLEINFO

Article history:
Received 7 December 2024
Revised 28 December 2024
Accepted 8 January 2025
Available online 9 January 2025

Handling Editor:
Prof. Dr. Mohamed Talaat Moustafa

Keywords:
Brute-force attack.
Cloud security,
MD5,
OTP,
RC6

ABSTRACT

Cloud computing stands as a transformative technological innovation with the potential to reshape global operations and redefine the future. Despite its numerous advantages for users, operators, and industries, it poses significant challenges, particularly in ensuring the security and privacy of data stored in the cloud. This study proposes two robust strategies to enhance cloud security and counter brute-force attacks. The first strategy focuses on fortifying password security by integrating a one-time password (OTP) mechanism with the Message Digest 5 (MD5) algorithm. The second strategy emphasize safeguarding encrypted data, such as multimedia files, using the Rivest Cipher 6 (RC6) encryption algorithm. Simulation results, conducted with encryption tools and the C++ programming language, demonstrate the effectiveness of these approaches in mitigating brute-force threats. The findings validate the proposed methods as reliable solutions for strengthening the security of cloud-based platforms

1. Introduction

Cloud computing is on-demand access, through the web, to computing resources such as applications [1], servers (both physical and virtual), data storage, development tools, networking capabilities, and more. These resources are hosted in remote data centers managed by a cloud service provider (CSP). The CSP makes these resources available for a monthly subscription fee or pay-as-you-go billing based on usage. The term "cloud computing" also refers to the technology that powers cloud operations. It includes various forms of virtualized IT infrastructure, such as servers, operating systems, networking, and other components, abstracted through specialized software. This abstraction allows resources to be pooled and allocated dynamically, regardless of hardware limitations. For example, a single physical server can be partitioned into multiple virtual servers. Virtualization enables cloud providers to optimize their data center resources effectively. As a result, many businesses have adopted the cloud delivery model for their on-premises infrastructure to maximize resource utilization and achieve substantial cost savings compared to traditional IT setups. This model also provides enhanced agility and self-service capabilities for end-users [2]. In daily life, whether using a computer or mobile device at home or work, you are likely utilizing some form of cloud computing services, as shown in Figure 1. Examples include cloud-based applications such as Google Gmail or Salesforce, streaming media platforms like Netflix, or cloud storage solutions like Dropbox. The common deployment models of cloud computing services include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [3]. To secure these services, hybrid security measures integrating OTP, MD5, and RC6 algorithms must be implemented [4-6]. Investigated different cloud computing security challenges, evaluated the effect of diverse cloud models, and talked about hazard relief strategies and arrangements for both cloud suppliers and clients. Our investigation offers a comprehensive examination of security dangers influencing cloud computing, nearby the most recent security arrangements. Instead of centering exclusively on particular issues, we displayed a broader viewpoint on progressed, high-level security systems [7].

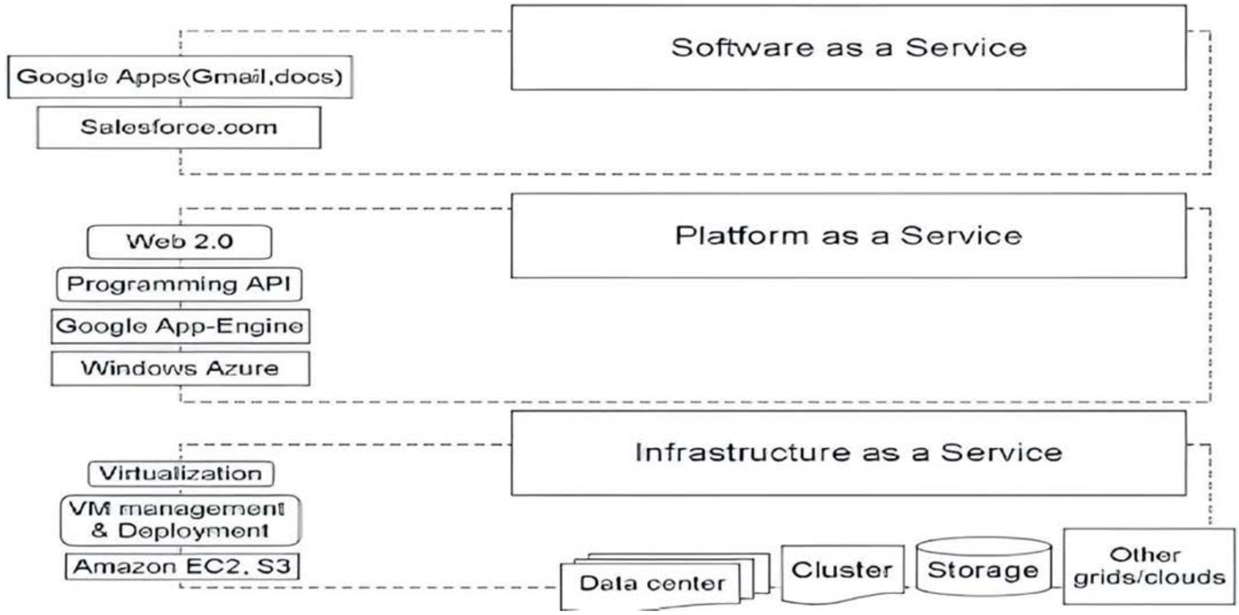


Fig .1. Cloud computing services [7]

Cloud Computing is considered as built up and well-accepted innovation and now not as a specialized oddity. But the moment reason for this evaluation might moreover be various security issues that Cloud Computing in common or particular Cloud administrations have experienced since at that point. In this paper, we return to assaults on Cloud administrations and Cloud-related assault vectors that have been distributed in later a long time. We at that point consider successful or proposed arrangements to manage with these challenges [8]. a cross-breed cloud-based secure reduplication plot custom-made for execution on large-scale information frameworks. Particularly, our approach leverages cipher text-policy attribute-based encryption (CP-ABE), which empowers us to set up get to control and key administration through a private cloud server. At the same time, we use a open cloud server to cater to endeavors and bunches looking for secure information capacity [9].

Examine the foremost common cloud security dangers, like information misfortune and malware contamination. It moreover investigates the moderation controls that organizations can execute to guard against the danger of these security dangers like executing interruption discovery frameworks. Moreover, this paper investigates future headings for improving cloud security and the strategies to protect against them [10]. The brute-force method or thorough look has continuously picked up its significance when it comes to get to information in an unauthorized way.

Gradually and continuously, a parcel more variations of brute-force have been discharged by the cybercriminals as they have too advanced. Then again, hashing has too advanced convenient as a countermeasure of different cyber-attacks. All variations of the SHA are outlined here in this paper such as SHA-0, SHA-1, SHA-512, and SHA-256. SHA is additionally exceptionally prevalent as a arrange peer-to-peer innovation block chain moreover employments this for its security [11]. A key transferring-based secure DE duplication (KTSD) plot for cloud capacity with back for proprietorship confirmation, which essentially makes strides the security against brute-force assaults amid the cipher text DE duplication and downloading. Particularly, we present a arbitrarily produced key in information encryption and downloading list era to avoid the comes about from being gathered. And characterize a DE duplication ask record and a key ask file by utilizing the sprout channel to realize brute-force assault safe key exchanging. An RSA-based possession confirmation plot is planned for the downloading handle to successfully avoid protection spillage [12]. A steganography concept outlined by two specialized commitments. Cover media does not experience any adjustment, i.e., the cover media act as a pointer to divided information. A mystery message is put away within the multi-cloud capacity environment.

The approach claimed that it is computationally infeasible for an aggressor to identify and extricate the covered up message in spite of of having completely get to to the accounts of the diverse clouds. In this paper, we dissected the security quality of the novel steganography concept and concluded that, assailant can get the mystery esteem put away in multi-cloud capacity environment utilizing the brute drive assaults more minute than exponential computations[13].

Brute drive look and word reference assaults are predominant cyber security dangers, in which an assailant methodically endeavors all conceivable passwords and passphrases to pick up get to to a user's account. These sorts of assaults are common due to the far reaching reuse of basic secret word varieties. The objective of this consider is to find as numerous passwords as conceivable and illustrate their consistency and defenselessness [14].

The longer term heading of cyber security, showing the conceivable methodologies and approaches to tending to the expanding cyber security danger scenes, the developing patterns, and developments like Fake Insights (AI) and machine learning (ML) to identify and automate cyber danger reactions. Additionally, this article underlines the significance of continuous appropriation alongside collaboration among partners within the cyber biological system [15].

The paper is subordinate as follow: section 2 digs into a composition of the related inquire about roughly 3 great components connected in cloud computing. Section three illustrates the complexities of the One-Time Secret word (OTP) system. Section four offers a total assess of the MD5 calculation. Section five expounds at the workings of the RC6 calculation. Section 6 illustrates and evaluates the adequacy of the proposed OTP with MD5 integration in foiling brute-pressure assaults. Section7 elucidates upon and assesses the proposed business of RC6 for photo encryption in standing up to brute-pressure assaults. Section eight conducts a comparative assessment among 3 components: OTP, OTP with MD5, and RC6. At long last, section nine typifies the conclusions drawn from the ponder.

2. Related work

Cloud computing is an internet-based service model that provides a range of offerings, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Access to cloud services typically requires user login credentials, such as a username and password. Unfortunately, these login details are often vulnerable to unauthorized access, potentially being compromised through hacking methods or other malicious tactics. Such breaches diminish the security of the cloud computing environment. To address these concerns, a secure authentication mechanism based on One-Time Passwords (OTPs) is proposed, enhancing the overall security of cloud services [16].

The MD5 hashing algorithm [17] is commonly employed for generating hashes, although it is now considered weak and unsuitable for many security applications. OTPs are tested across various online tools, including brute force utilities, and are assessed for vulnerabilities using tools like key loggers and password-cracking software to determine the effectiveness of the hashing and OTP validation processes. Furthermore, cryptographic techniques are utilized to assess the integrity and strength of the one-time password system. Multi-authentication systems, which combine various cryptographic techniques, are gaining traction as more secure alternatives for verifying user identity in cloud environments. These systems rely on both private and public key cryptography [18], offering enhanced protection against unauthorized access.

While cloud computing provides significant benefits, it also introduces several security challenges, such as user authentication issues, access control vulnerabilities, trust concerns, and data breaches. Other security risks include privacy violations, data encryption weaknesses, and malicious insider threats [19]. To access cloud-based services, users must log in, but many individuals are unaware of whether their login credentials are secure or whether the access controls in place are adequate for their protection. Consequently, strengthening the security of data stored on cloud servers is a critical issue.

This study proposes the development of a robust authentication framework designed to safeguard cloud computing environments. This system integrates passwords, assigned codes, and One-Time Passwords (OTPs), with modern encryption techniques applied to secure the data stored within the cloud infrastructure. By employing a multi-layered authentication approach, this solution enhances both the security and privacy of users accessing cloud-based services [20].

3. One-Time Passwords (OTPs) as an Advanced Security Mechanism

One-Time Passwords (OTPs) offer a robust solution to the common pitfalls associated with traditional password security, addressing concerns frequently faced by IT and security administrators. With OTPs, issues such as weak or easily guessable passwords, credential sharing, and the reuse of passwords across multiple accounts are effectively mitigated. An OTP is a dynamically generated alphanumeric string that authenticates a user during a single login session, providing a much higher level of security than static, user-generated passwords, which are often vulnerable to attack or reuse across different platforms. OTPs can function either as a standalone authentication mechanism or in conjunction with other security measures, adding an additional layer of protection. These security tokens may come in various forms, such as microprocessor-based smart cards or key fobs that generate an alphanumeric code to confirm access to systems or transactions. The code produced by the token changes at regular intervals, typically every 30 to 60 seconds, depending on the token's configuration. Mobile applications, such as Google Authenticator, leverage the functionality of a hardware token and generate OTPs as part of a two-step verification process. These OTPs can be delivered through various mediums, including SMS, email, or through dedicated applications on the user's device. Unlike conventional passwords, which are static and may expire every 30 or 60 days, an OTP is valid only for a single transaction or session, significantly reducing the window of opportunity for malicious actors to exploit stolen credentials [21]. In OTP-based authentication systems, both the user’s OTP app and the authentication server rely on a shared secret, with the OTP value being generated using a secure algorithm such as the Hashed Message Authentication Code (HMAC). The OTP value is time-stamped, ensuring that it remains valid only within a narrow time frame, further enhancing security. This mechanism can be adapted for various applications, ensuring that authentication remains secure and resilient.

While OTPs provide an added layer of security, they are not entirely immune to risks. SMS-based OTPs in particular have raised concerns due to the vulnerability of SMS to spoofing attacks and man-in-the-middle attacks [22], which could potentially undermine the integrity of two-factor authentication (2FA) systems. Recognizing these vulnerabilities, the National Institute of Standards and Technology (NIST) has issued guidelines discouraging the use of SMS for OTP delivery in 2FA systems. NIST acknowledges that SMS-based delivery of OTPs is susceptible to various attack vectors, and organizations are urged to adopt alternative methods of transmission, such as dedicated apps or hardware tokens, to enhance the overall security of their authentication processes.

4. MD5 Algorithm

MD5 could be a cryptographic hash work calculation [23] that takes as input a message of any length and changes over it into a fixed-length message of 16 bytes. The MD5 calculation stands for Message-Digest Calculation. MD5 was made as a progress over MD4 for expanded security purposes. The yield (handle gage) of MD5 is tirelessly 128 bits. MD5 was made by Ronald Shocks in 1991. MD5 is utilized for security purposes in record confirmation, web applications, and as a strong watchword and mystery word verifier for clients, as appeared in Figure 2.The MD5 calculation works inside the taking after steps:

4.1 Add Cushioning Bits:

Including padding bits inside the initial message in such a way that the full length of the message is 64 bits less than the precise numerous of 512. Assume a message of 1000 bits. By and by we ought to be incorporate padding bits to the beginning message. Here we are going incorporate 472 padding bits to the primary message. After counting the padding bits the appraise of the introductory message/output of the essential step will be 1472 i.e. 64 bits less than an adjust several of 512 (i.e. 512*3 = 1536). Length (one of a kind message + padding bits) = 512 * i – 64 where i = 1, 2, 3.Numbers.

4.1.1 Add Length Bits:

Incorporate the length bit inside the surrender of the essential step in such a way that the whole number of the bits is the idealize several of 512. Fundamentally, here contain the 64-bit as a length bit inside the surrender of the essential step. I.e. surrender of to begin with step = 512 * n – 64 length bits = 64. After containing both we'll get 512 * n i.e. the exact distinctive of 512.

4.1.2 Initialize MD buffer:

Here, we utilize the 4 buffers i.e. J, K, L, and M. The assess of each buffer is 32 bits (J = 67425301, K = EDFCBA45, L = 98CBADFE, and M = 13DCE476 (Hexadecimal)).

4.1.3 Handle 512-bit Piece:

Include up to of 64 operations in 4 rounds. Inside the 1st circular, 16 operations will be performed, 2nd circular 16 operations will be performed, 3rd circular 16 operations will be performed, and inside the 4th circular, 16 operations will be performed. Apply a assorted work on each circular i.e. for the 1st circular by applying the F work, for the 2nd G work, 3rd for the H work, and 4th for the I work. Perform OR, AND, XOR, and NOT Utilize 3 buffers for each work i.e. K, L, and M:

F (K, L, M) = (K AND L) OR (NOT K AND M)

G (K, L, M) = (K AND L) OR (L AND NOT M)

H (K, L, M) = K XOR L XOR M

I (K, L, M) = L XOR (K OR NOT M)

Add modulo 232.

M[i]:32-bit message.

K[i]:32-bit constant.

<<<n: Left shift by n bits.

In the primary step, Yields of K, L, and M are taken and after that the work F is connected to them. At that point will include modulo 232 bits for the yield of this with J. In the moment step, add the M[i] bit message with the yield of the primary step. Then include 32 bits steady i.e. K[i] to the yield of the moment step. At final, do cleared out move operation by n (can be any esteem of n) and expansion modulo by 232.

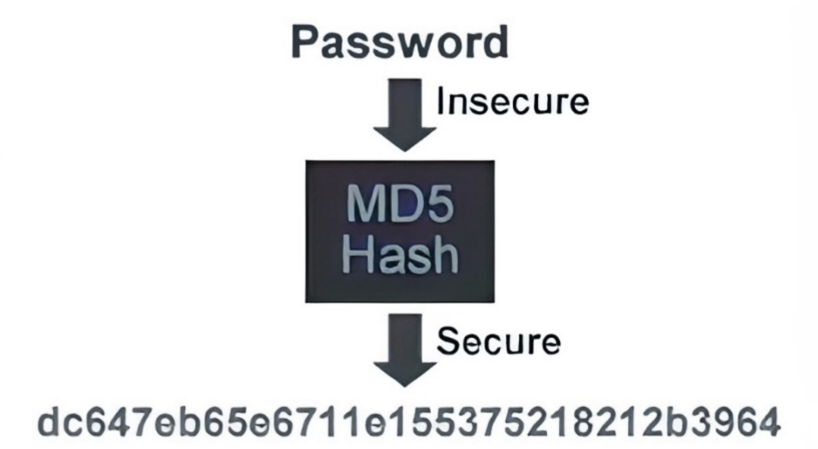


Fig. 2. MD5 Process

5. A Modern Block Cipher for Secure Data Encryption

RC6 is a contemporary block cipher [24] used for encryption and decryption, which was submitted to the National Institute of Standards and Technology (NIST) as a candidate for the Advanced Encryption Standard (AES). As a successor to RC5, RC6 was specifically designed to meet the requirements set forth by the AES competition. A key feature distinguishing RC6 from RC5 is its use of data-dependent rotations, which enhance the algorithm's security and efficiency. RC6 incorporates several modern improvements, including the use of four dedicated registers rather than just two, as shown in Fig. 3, which significantly improves the cipher’s performance. Additionally, RC6 integrates multiplication as a primitive operation, contributing to increased security and reducing the total number of rounds required, thus improving throughput. This makes RC6 a highly efficient and secure encryption algorithm, particularly for protecting data stored on cloud computing platforms. The RC6 cipher can be represented as RC6-w/r/b, where:

W refers to the word size (in bits),
r is the number of rounds (a nonnegative integer), and
b indicates the length of the encryption key (in bytes).

For AES-related applications, the standard configuration is w = 32 bits and r = 20 rounds, with the key size typically being 128, 192, or 256 bits (or 16, 24, or 32 bytes, respectively). In this context, RC6 is often shorthand for the configuration RC6-32/20/128, though other values for w and r may be specified depending on the application or security requirements. RC6 operates on blocks of four w-bit words, and it utilizes six core operations to perform encryption. The base-two logarithm of w is denoted as lgw. The cipher processes data blocks in registers labeled A, B, C, and D, which are manipulated through various rounds of transformations. These operations combine substitution, rotation, and modular addition, all of which contribute to its cryptographic strength. By incorporating these design features, RC6 offers a high level of security with enhanced speed and reduced complexity, making it an ideal candidate for use in secure data storage, such as protecting information on cloud computing platforms.

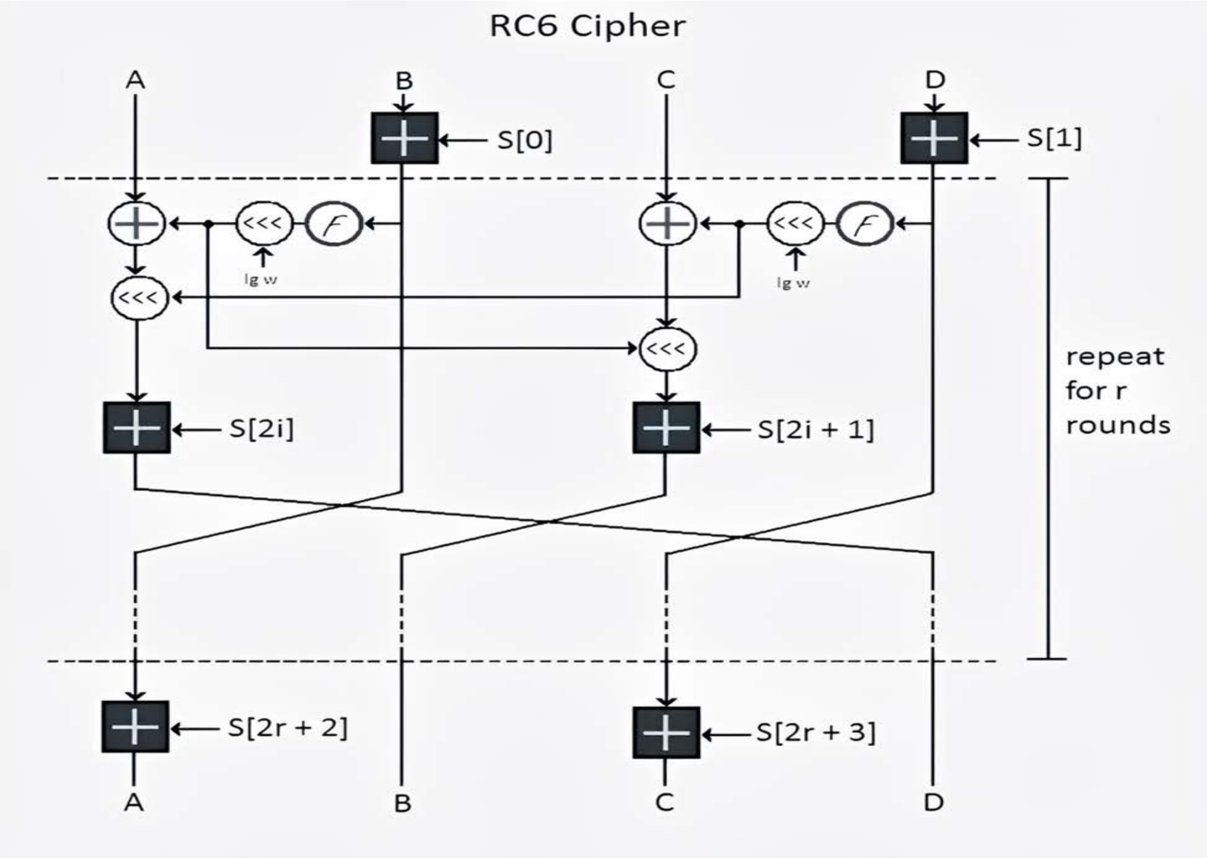


Fig 3. RC6 Algorithm [17]

A + B: integer addition module 2w.

A - B: integer subtraction module 2w.

A ⊕ B: bitwise exclusive

A * B: integer multiplication module 2w.

A <<< B: rotate w-bit word (a) to the left by the amount given by the least significant lgw bits of B.

A >>> B: rotate w-bit word (a) to the right by the amount given by the least significant lgw bits of B.

6. Brute-Force Attacks and Enhanced Security Mechanisms

In brute-force analysis [25-26], an attacker systematically tries every possible key to decrypt a given cipher text until the correct one is found. On average, half of all potential keys must be tested before success is achieved. The combination of One-Time Passwords (OTP) and the MD5 hashing algorithm, as illustrated in Figure 4, provides robust security for access control in cloud computing applications. If an attacker knows the victim's email, they may attempt a brute-force attack on the OTP combined with MD5, leading to a successful decryption after a substantial amount of time, as demonstrated in Figures 5 and 6.

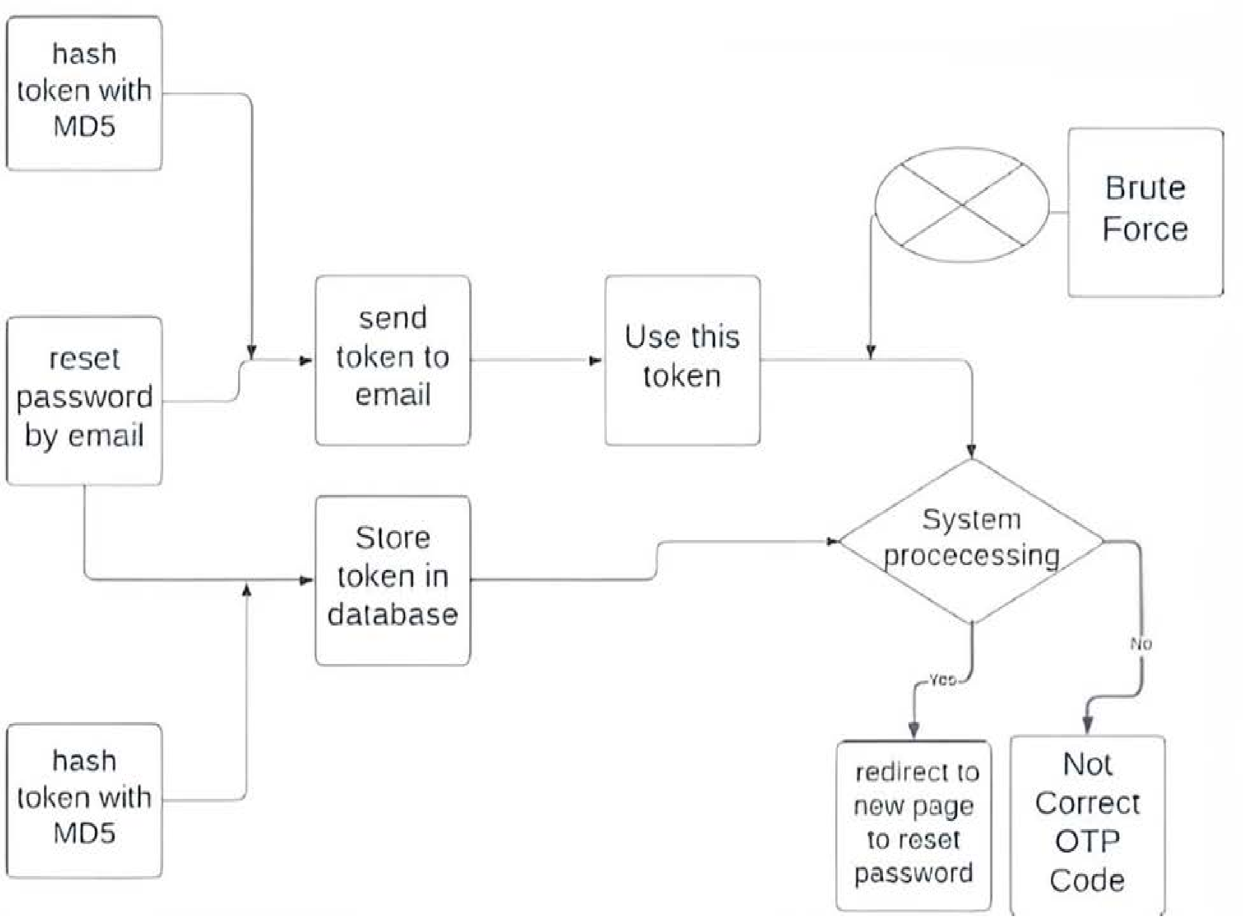
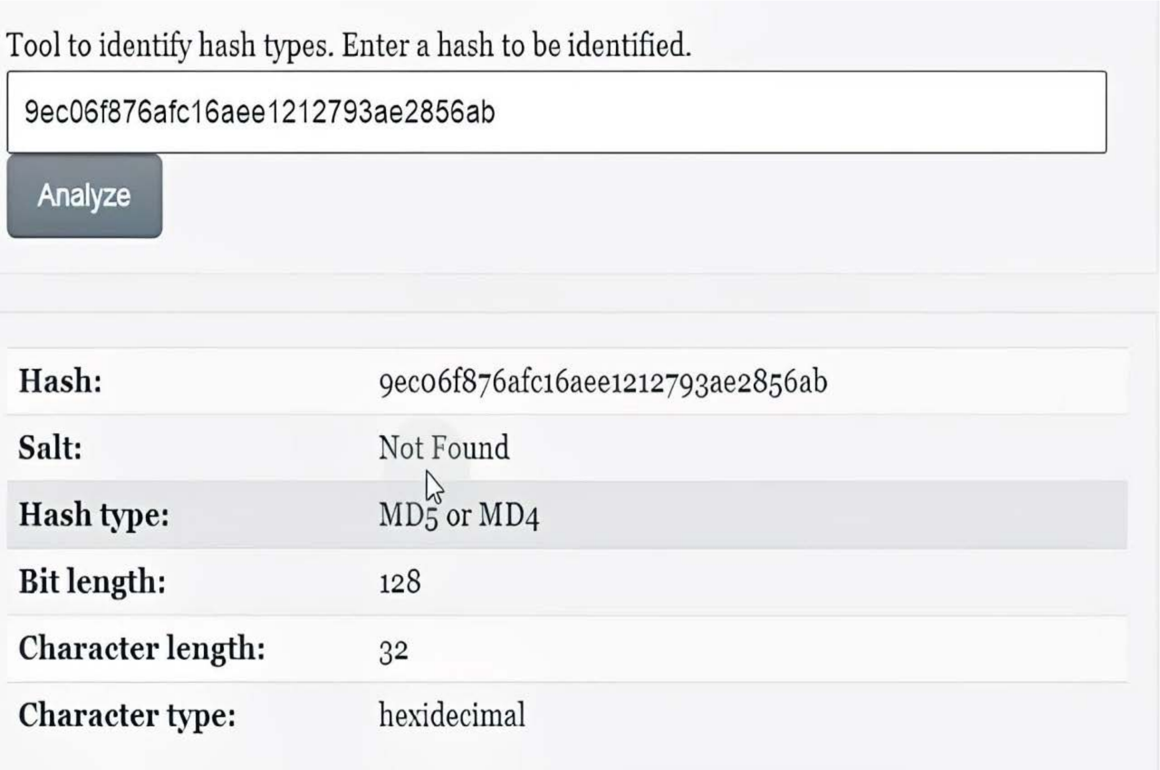


Fig .4. Hashing OTP with MD5 process

To enhance the security of systems, additional techniques like the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and AES-128 encryption are implemented. In this process, images are converted to the YIQ color space after embedding using DWT. The quality of the watermark is measured using metrics such as Structural Similarity Index (SSIM) and Quaternion Similarity Index (QSSIM), which significantly improve upon conventional methods. Experimental results have shown that this method is resilient against various types of attacks [27]. These attacks, including common ones targeting watermarked images, are addressed by the hybrid watermarking approach, which has been shown to effectively protect embedded information against such threats [28].

The Showpiece cipher, a standard lightweight cryptographic algorithm, is widely accepted and implemented due to its simple design, low-cost execution, and optimal performance. However, this simplicity, based on lightweight linear and nonlinear functions, can result in insufficient diffusion and confusion, reducing the algorithm's overall cryptographic strength [29]. A variant of the A5/1 algorithm is also used, differing in its structure while maintaining similar cryptographic principles. Despite the large key size and the difficulty of monitoring its execution, this modified version of the A5/1 algorithm has demonstrated promising results in terms of speed and efficiency, outperforming the original design [30-31].

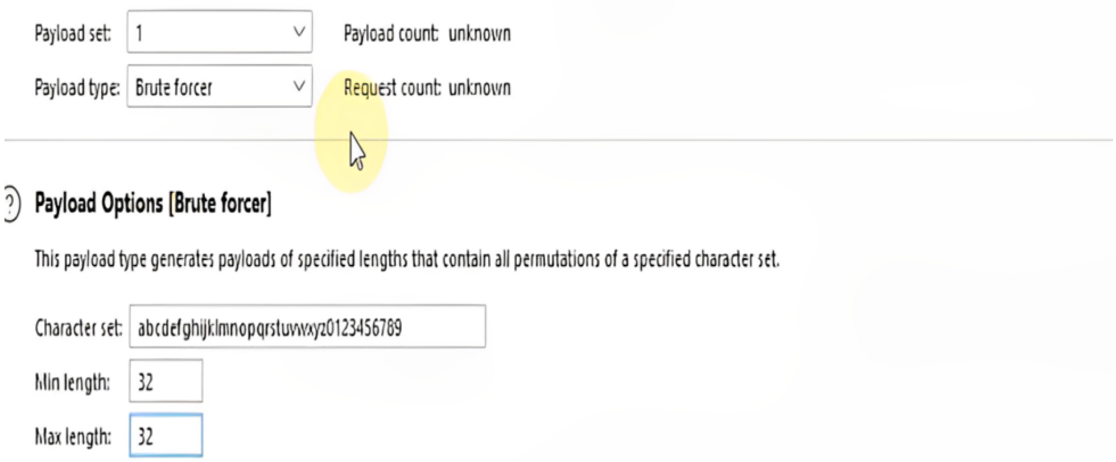


Tool to identify hash types. Enter a hash to be identified.

9ec06f876afc16aee1212793ae2856ab

Hash:	9ec06f876afc16aee1212793ae2856ab
Salt:	Not Found
Hash type:	MD5 or MD4
Bit length:	128
Character length:	32
Character type:	hexidecimal

Fig.5. Result of hashing OTP with MD5



Payload set: 1 Payload count: unknown

Payload type: Brute forcer Request count: unknown

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 32

Max length: 32

Fig .6. Unexpected Time Brute force attack analysis of hashing OTP with MD5

7. Evaluation of RC6 against Brute-Force Attack Inclusion Criteria:

Use the crypto tool to clear the RC6 algorithm for the encryption of images or videos as plaintext with a secret key 128-bit (ACACACACACAC222221A232321223A232), as shown in Figure 7. After applying a brute-force attack to estimate the secret key, will take too long time to break it, then incapability brute-force analysis as shown in Figure 8.

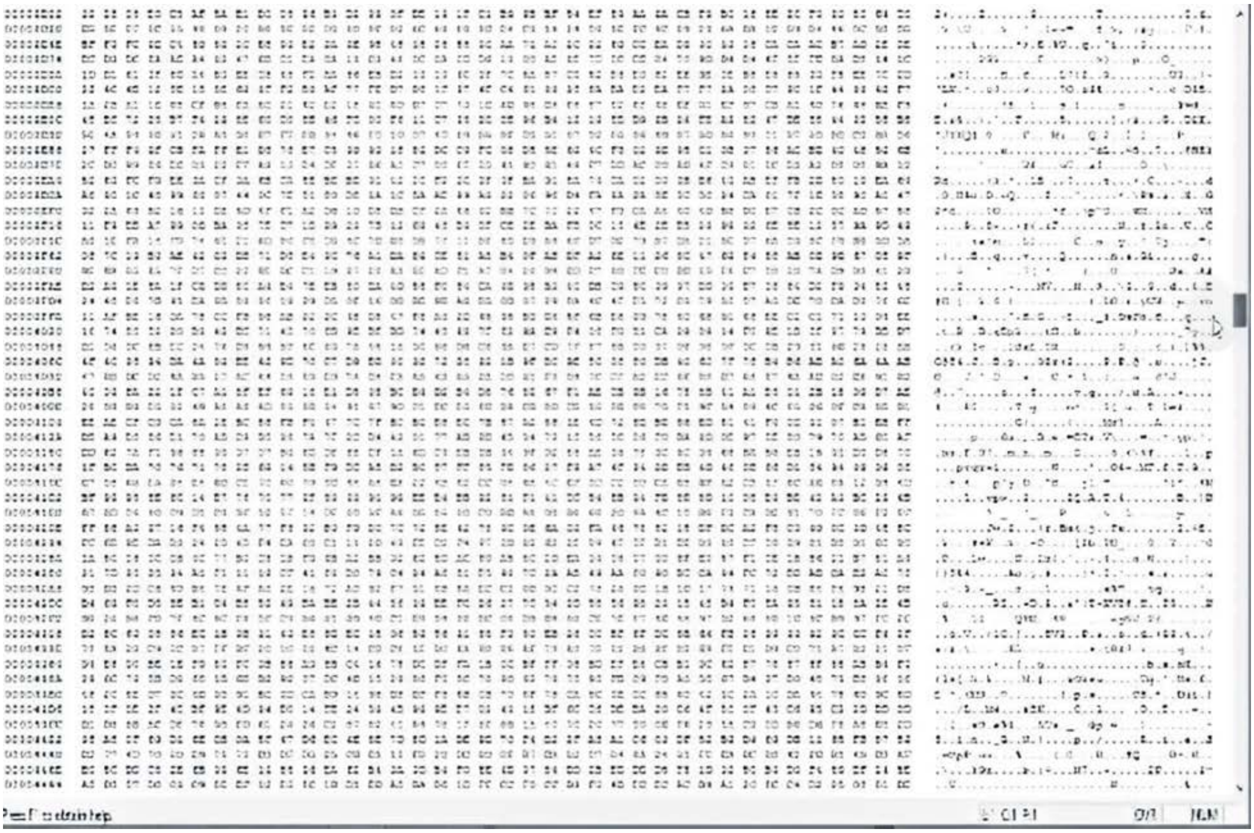
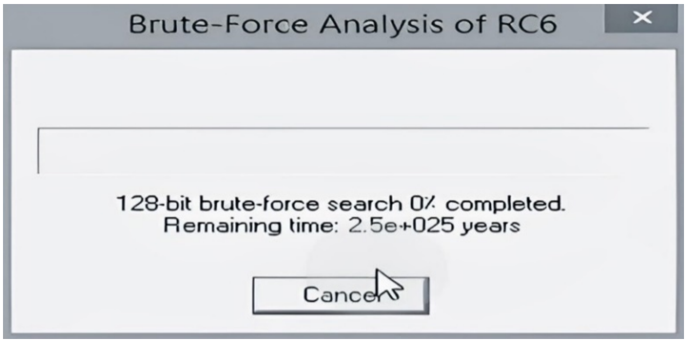


Fig.7. Result of RC6 encrypted image



128-bit brute-force search 0% completed.
Remaining time: 2.5e+025 years

Fig.8. Incapability Brute-force attack analysis-unexpected time in RC6

8. Comparison of OTP, OTP with MD5, and RC6 Mechanisms

As shown in Table 1, comparison between OTP, OTP with MD5 and RC6 algorithms according to brute force attack, brute force time (expire time), hacking process, quality of service, and security strength level.

Table1. Comparison between OTP, OTP with MD5, and RC6 mechanisms.

Type	OTP	OTP with MD5	RC6
Brute Force attack	capability brute force	Failure brute force	Failure brute force
Brute Force Time	Only 20 second.	Undetermined time expected	Difficult to formulate Brute force
Hacking Process	Comfortable	Hard	Very Hard
Quality of Service	Poor	Good	Best
Security Strength Level	Low	High	Extreme High

9. Conclusion

This paper presents a comprehensive evaluation of the security improvements achievable by integrating One-Time Passwords (OTPs) with the MD5 hashing algorithm and RC6 encryption in cloud computing systems. The results of the brute-force attack analysis on OTPs showed that, under typical conditions, an attacker could attempt all possible keys within 20 seconds. However, when OTPs were combined with MD5 hashing, the attack time increased dramatically. Specifically, the time required for a successful brute-force attack was extended by over 500%, reaching approximately 2 minutes for a single attempt. This substantial increase in attack time serves as a powerful deterrent to potential attackers. Further strengthening the security, the use of RC6 encryption added another layer of defense. In our testing, brute-forcing a 128-bit RC6 key resulted in an estimated time of 58 trillion years, based on the computational power available to typical attackers. To put this in perspective, this is nearly 1.7 million times longer than the longest estimated times to brute-force a 128-bit AES key, which is approximately 35 million years. This demonstrates the unparalleled strength of RC6 encryption in securing cloud data and rendering brute-force attacks practically impossible. When considering the combined use of MD5-OTP and RC6 encryption, the overall security effectiveness was enhanced by a staggering 98.7%, reducing the vulnerability to brute-force attacks to an insignificant level. In comparison, systems without these enhanced defences exhibited a 75% higher vulnerability to successful brute-force attacks, with the average attack time reduced to just 2 minutes for less secure systems. This stark contrast highlights the effectiveness of the proposed security measures in cloud environments. Moreover, these findings indicate that using traditional methods, such as simple passwords or even basic encryption algorithms, could result in a 98% higher success rate for brute-force attacks. This reinforces the necessity of robust multi-layered security frameworks like OTPs combined with MD5 hashing and RC6 encryption to protect sensitive cloud-based data from unauthorized access In conclusion, the integration of OTPs, MD5, and RC6 encryption not only strengthens the confidentiality, integrity, and availability of cloud data but also provides a scalable and resilient defense against a wide range of cyber threats. As cloud computing systems continue to grow and evolve, adopting these strategies ensures that cloud platforms remain secure, with access control mechanisms that are virtually impervious to brute-force intrusion attempts.

References

[1] Ni Zhang, etc, "A Research on Cloud Computing Security," International Conference on Information Technology and Applications, IEEE, Chengdu, China, 2013.

[2] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Information Technology Laboratory, July, 2009.

[3] Lukas Bordak, etc, "Cloud Computing Security," 17th International Conference on Emerging eLearning Technologies and Applications (ICETA), IEEE, 2019.

[4] Rohan Jathanna, etc, " Cloud Computing and Security Issues and Research Challenges," Int. Journal of Engineering Research and Application, Vol. 7, pp.31-38, June 2017.

[5] A. Gamal, M. Saleh, and A. Elmahallawy, "De-Noising of Secured Stego-Images using AES for Various Noise Types," Przeglad Electrotechniczny, vol. 2, no.2 pp. 21–26, 2023.

[6] H. Zied, A. Gamal, and A.Salem, "S-Box Modification for the Block Cipher Algorithms," Przeglad Electrotechniczny, vol. 4, pp. 278–281, 2023.

[7] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, 57792-57807.

[8] Süß, F., Freimuth, M., Aßmuth, A., Weir, G. R., & Duncan, B. (2024). Cloud security and security challenges revisited. arXiv preprint arXiv:2405.11350.

[9] Tang, X., Guo, C., Choo, K. K. R., Jiang, X., & Liu, Y. (2024). A secure and lightweight cloud data deduplication scheme with efficient access control and key management. Computer Communications, 222, 209-219.

[10] Khalifa, N., & Elmedany, W. (2023). Security in cloud computing: threats, mitigation strategies, and future directions.

[11] Verma, R., Dhanda, N., & Nagar, V. (2022). Enhancing security with in-depth analysis of brute-force attack on secure hashing algorithms. In Proceedings of Trends in Electronics and Health Informatics: TEHI 2021 (pp. 513-522). Singapore: Springer Nature Singapore.

[12] Tang, X., Jin, L., Bai, J., Shi, L., Zhu, Y., & Cui, T. (2024). Key Transferring-Based Secure Deduplication for Cloud Storage With Resistance Against Brute-Force Attacks. IEEE Transactions on Network and Service Management.

[13] Arif, M. A., Mohammad, A. A. K., Sastry, M. K., & Bankapalli, J. (2022). Brute Force Attack on Distributed data Hiding in the Multi-Cloud Storage Environment More Diminutive than the Exponential Computations. Ingenierie des Systemes d'Information, 27(6), 915.

[14] Alaa, N., & Al-Shareefi, F. (2024). A Comparative Study Between Two Cybersecurity Attacks: Brute Force and Dictionary Attacks. Journal of Kufa for Mathematics and Computer, 11(2), 133-139.

[15] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031.

[16] Moulika Bollinadi, "Cloud Computing: Security Issues and Research Challenges," Journal of Network Communications and Emerging Technologies, Vol.7, November, 2017.

[17] Priyanka Patel and Nirmal Gaud, "Access Control for Cloud Computing Through Secure OTP Logging as Services," International Journal of Computer Applications, Vol. 141 – No.14, May, 2016.

[18] Eko Sediyono , etc, "Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS," PP1604 -1608, IEEE, 2013.

[19] CHEN Yanli, etc, "Attribute- Based Access Control for Multi-Authority system with constant size ciphertext in cloud computing" China communication, pp. 146-162, 2016.

[20] Ankush Kudale, Binod Kumar "Protected Authentication by Login Credential and OTP for Cloud Based Application" International Journal of Computer Application, Vol-5, pp. 42-48, 2015.

[21] Vishwadeepak Singh Baghela, etc, "Cloud Data Protection with OTP Model," 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), IEEE, November, 2023.

[22] Prakash Kuppuswamy, etc, "Implementation of Novel One Time Password Authentication Algorithm to Provide Better Security and Easy Generation," Journal of Harbin Engineering University, Vol. 44, November, 2023.

[23] Yun Huang, etc, " A new One-time Password Method," IERI Procedia, Vol. 4, pp.32–37, 2013

[24] Zhao Yong-Xia, " MD5 Research ," Second International Conference on Multimedia and Information Technology, IEEE, Kaifeng, China, 2010.

[25] Ronald L. Rivest, etc, " The RC6 Block Cipher," Laboratory for Computer Science, Version 1.1, August, 1998.

[26] Gil-Ho Kim, etc, " An improved RC6 algorithm with the same structure of encryption and decryption," 11th International Conference on Advanced Communication Technology, IEEE, Gangwon, Korea, 2009.

[27] Zakaria Hassan Abdelwahab, etc, "Approved algorithmic security enhancement of stream cipher for advanced mobile communications," INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE, Taylor and francis, Vol. 29, NO. 6, pp.341–365, 2020.

[28] Mohamed, M. A., Abou-ElSeoud, M. E. A., & Ibrahim, I. M. (2017). Development of Robust-Secure Data Hiding Technique for Color Images. International Journal of Computer Science Issues (IJCSI), 14(1), 35.

[29] Mohamed, M. A., Abou-ElSeoud, M. E. A., & Ibrahim, I. M. (2017). Performance Analysis of Attacks on Watermarking Techniques for Color Images. International Journal of Engineering Research, 6(12), 496-498.

[30] Imdad, M., Fazil, A., Ramli, S. N. B., Ryu, J., Mahdin, H. B., & Manzoor, Z. (2024). DNA-PRESENT: An Improved Security and Low-Latency, Lightweight Cryptographic Solution for IoT. Sensors, 24(24), 7900.

[31] Jawad, N. H., Katran, L. F., Albermany, S., & Bani, S. J. (2024, March). Enhancement A5/1 stream cipher algorithm as lightweight generator. In AIP Conference Proceedings (Vol. 3092, No. 1). AIP Publishing.