International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Communication Security in Hybrid Cloud Environments Through an Innovative Cryptographic Algorithm

Kuber Datt Gautam *[1], Dr. Rajeev G. Vishwakarma [2]

Submitted: 04/11/2023 **Revised**: 21/12/2023 **Accepted**: 03/01/2024

Abstract: Cloud computing, a relatively recent innovation, enhances potential without requiring costly hardware or software updates. It reduces overall system costs by facilitating resource sharing across hardware, software, and platforms. Its widespread adoption and practicality have made it indispensable in today's business world. However, its popularity and reliance on third parties also make it a prime target for cybercriminals. For service providers, security is crucial to gaining customer trust and maintaining a positive brand image. Consequently, many large businesses are shifting their services to the cloud to benefit from its cost-effective and efficient infrastructure sharing. With an abundance of data stored remotely and third-party involvement, prioritizing security is essential. Various security algorithms have been evaluated for their ability to protect sensitive data with minimal resource consumption. This study focuses on data integrity, considering ECC and RC6 as alternatives to ECC + RC6 and MD5. It proposes an enhanced security system based on the ECC and RC6 algorithms and the Role-based Access Control Model. To demonstrate the system's effectiveness, a public cloud application using Java technology was created. The application's computation time for different file sizes and formats was analyzed, offering insights into its performance and potential for secure cloud computing.

Keywords: *Cloud Computing, Elliptic Curve Cryptography , Rivest Cipher 6, Message Digest Algorithm 5, Public Cloud.*

1. Introduction

Cloud computing enables several users to access the resources of a single server and connect to data centres to enable service delivery. Such technology has the potential to become increasingly sharp and precise over time. To stay up-to-date, it is essentuse of alterations in trend or the introduction of cutting-edge technologies, regular revisions are necessary. The complexity of data storage has increased as a result of recent technological developments. The term "cloud computing" is commonly used as a solution to these data storage issues. The reader is introduced to cloud computing in this chapter [1] by going through the fundamentals, including its architecture and key characteristics. Customers can access networks and storage on-demand thanks to cloud computing without the service provider having to perform a lot of manual management or engagement.

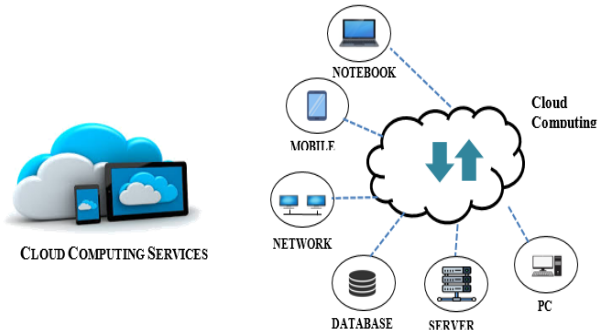

Fig 1. The Cloud Computing Services

1.1 Models For Cloud Services:

Infrastructure as a Service (IaaS) IaaS offers infrastructure services that enable the installation of any kind of operating system or application. It is fundamental in nature. • Technical knowledge is necessary for operation. Some of the goods that are part of this service are the virtual machine, storage, network, and server. The main users of this product are researchers and developers. Platform-as-a-Service, or PaaS, is a platform-providing service. • Offers platform-related services. The platform includes the necessary hardware and software. Services for infrastructure • Only rudimentary knowledge is needed. works at runtime, on the server, and with databases. • It is primarily used by developers to make apps. Software-as-a-service (SaaS): • Helps with programme usage. Pre-configured software is additionally accessible.

[1,2]*Department of Computer Science and Engineering*
[1] *Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore*
[2] *Research Supervisor and Pro Vice-Chancellor, Dr. A. P. J. Abdul Kalam University, Indore, (M.P.), India.*
*E-mail Id: [1]kuber.datt@gmail.com, [2]rajeev@mail.com**
Corresponding Author: Kuber Datt Gautam
Email: kuber.datt@gmail.com

• It's There is no demand for technical expertise because SaaS providers handle all technological issues. The app has features for e-mail, Facebook, Twitter, and additional social media platforms. This can be seen, for instance, in mail and social media platforms.

1.2 Cloud Application:

1. In a web application, the client operates on the user's browser, while the server is executed by web browsers on the server.
2. Cloud-based web apps merge the features of web applications into web solutions. As a service to other locations, they offer a platform for the exchange of software.
3. Knowledge of cloud computing is necessary to appreciate the value of cloud-based applications.

Fig 2. Applications of cloud computing

2. Literature Survey

Arora et al. discuss a variety of algorithms in [2], including RSA, DES, His technique uses Blowfish or AES to determine the amount of memory needed, the number of processor requests, and the amount of time.

Processor requests, and time comparisons. Conf and co. To deal with safeguards for the safety and confidentiality information that has been stored in the cloud, he utilized authentication codes for messages in [3].

In[4], Shereek, B., et al. offered recommendations for RSA, which is an open key cryptography system, including its safeguards, benefits, and security. Among other trials, the researcher's primality test made use of Fermat's Little Theorem. In this work, the usage of huge prime numbers and the the Fermat Theorem for RSA are employed to reduce time complexity.

among others, B. Samanthula. [5] Covers safety and safety maintenance via integrity, confidentiality, and end-to-end the authentication process, a key element in stopping outsiders form tampering with the sender's capacity to sniff messages. Data is protected by the owner and then outsourced to a cloud; however, efficiency issues occur when user negligence prohibits encrypting utilising the private key from functioning. Data is categorised for us by its access control. Based on implementation criteria, such as those regarding verification, proof of identity, gadget type, location, and time, it decides whether to permit or deny access. In order to avoid server conspiracies, random numbers are used in the procedure.

Jeong-Kyung Moon, Jin-Mook Kim, and others. We describe a powerful authentication strategy for hybrid cloud computing to improve security, availability, and adaptability among others, B. Samanthula. [5] Covers safety and safety maintenance via integrity, confidentiality, and end-to-end the authentication process, a key element in stopping outsiders form tampering with the sender's capacity to sniff messages. Data is protected by the owner and then outsourced to a cloud; however, efficiency issues occur when user negligence prohibits encrypting utilising the private key from functioning. Data is categorised for us by its access control. Based on implementation criteria, such as those regarding verification, proof of identity, gadget type, location, and time, it decides whether to permit or deny access. In order to avoid server conspiracies, random numbers are used in the procedure.

Jeong-Kyung Moon, Jin-Mook Kim, and others. We describe a powerful authentication strategy for hybrid cloud computing to improve security, availability, and adaptability. among others, B. Samanthula. [5] Covers safety and safety maintenance via integrity, confidentiality, and end-to-end the authentication process, a key element in stopping outsiders form tampering with the sender's capacity to sniff messages. Data is protected by the owner and then outsourced to a cloud; however, efficiency issues occur when user negligence prohibits encrypting utilising the private key from functioning. Data is categorised for us by its access control. Based on implementation criteria, such as those regarding verification, proof of identity, gadget type, location, and time, it decides whether to permit or deny access. In order to avoid server conspiracies, random numbers are used in the procedure [6].

Mrudula Sarvabhatla et al.'s [7] goal is to use the distributed file system in the Hadoop environment to store data. HDFS is the subject of the entire study. The feature of authentication is being evaluated for the security model. presented an improved version of a mutual authentication technique. It is safe and does not use up expensive resources. Hash computations and other less expensive processes are incorporated into it.

The entire cloud architecture was offered as the answer by Moyo et al. [8] as the result of organisational adoption. Security barriers in the cloud are an important topic that is discussed in this book. The sorts of cloud computing and its open environment were also covered by the author. The open nature of cloud computing means that security concerns still exist. However, it helps people acquire the greatest on-demand services, which is incredibly advantageous and positive. With the adoption of various methodologies and developers, the security issue in cloud computing is getting better.

Nasrin Khanazeai et al. [9] made a proposal regarding security concerns in cloud computing after realising how

important they are in this area. To increase the level of security, the author built a security method employing RSA and AES. The system improves security for potential attackers. In cloud computing, a system based on keys is employed. With respect to the RSA and AES algorithms, a combination of symmetric and asymmetric keys is used. The performance of these algorithms improves cryptographic encryption.

Deyan Chen and others. proposed regarding cloud security architecture and its shortcomings in [10]. Designing and analysing cloud security involves many different factors. The entire piece explains that cloud adoption is not yet complete, and its scope has not yet been established. This thesis discusses the benefits and drawbacks of cloud security as well as its design and advancement. The effectiveness of cloud services affects data security. They stop data from the cloud environment from leaking.

C. Y. Chen and others. A FHE system, or fully homomorphism encryption, was published in [11]. Which is employed in the resolution of crucial challenges in cryptography? This method is employed to compute encrypted data without first decrypting it. Rivest has found this problem. This technique effectively protects system confidentiality and has numerous uses.

"Prakash et al." The security concerns in the cloud are discussed in [12]. Additionally, he conducts experiments to demonstrate how encryption and decryption during inverter and shifter are advantageous since they shorten processing time and address security threats.

B. Chor et al. In [13], a database is simulated, a survey is conducted, and potential options for private access to data are tested.

Zissis, D., et al. According to [14], there are problems with Information security, accessibility, reliability, hazards, and integrity among a trusted third party in cloud computing

Moghaddam and others. According to [15], HE-RSA is A faster, more successful look at based on RSA is present, but it needs time and memory constraints. It is encrypted using a system that uses RSA and AES are used to regulate and manage the amount of time and memory overhead.

3 Proposed Solution

As part of the progress of the project, an encryption parameter must be created. Overall problem in order to secure any sensitive data. When we discuss sensitive information, we mean anything that needs to remain private. When a user receives data from a third-party supplier, there is a trust problem. The user either distrusts third-party vendors or, in some situations, believes they are dishonest. Since web apps can run on any platform, independent of the software used, cross-platform functionality is only possible with them. The two most important security concerns are authentication and authorization, and they must be addressed in appropriately. Hackers conduct an attack at this exact moment, putting the security of the system at risk. Web apps have long understood the importance of safeguarding confidential data both within and outside. Sensitive information is protected by data encryption, however when dealing with massive amounts of data, it considerably increases the processing and memory needs of web services. Web applications must constantly employ little processing overhead to ensure the fastest computation possible. RC6 is a more rapid and stronger security strategy than AES and ECC. combined, was used to replace the AES method. The ECC algorithm can offer RSA-like security with an extensive modulus and key. By modifying the Kerberos authentication protocol and using MD5 to verify the input's uniqueness, this was made possible.

3.1 Theory of the Study

This approach is for you if you want to encrypt and decrypt your data securely without compromising security. A customized version of the Before the client may access the resources of the web application, it must first be authenticated using the Kerberos protocol. After an authentication server verifies the client's identity, the resource server authorizes access to its resources. Data that the client uploaded is encrypted and decrypted using the ECC and RC6 algorithms, respectively. The application of the MD5 algorithm further ensures the data's integrity.

The graphic below depicts the overall flow of the architecture:

1. The text is kept basic.
2. The text is broken up into portions to make it simpler for the reader to follow.

C1, C2, C3, and C4 compounds.

4. The pieces are divided into groups of even and odd sizes.
5. Even sections are encrypted with the ECC method, while odd parts are encrypted with RC6.
6. After that, cypher text was created by encrypting the plain text.

The block Figure that follows illustrates the entire project's workflow.

3.2 Framework for Authentication Modeling

A modified version of Kerberos is used by the Kerberos server to authenticate users so that their credentials may be verified when they sign in. If the login information is accurate, the user's home page will be sent successfully. This technique is used to verify the accuracy of the data in the study at hand. We employ the Authentication Server rather than the two servers required by the Kerberos 5 protocol for authentication and token creation in order to restrict access to only authorised users. The user that engages in illicit behaviour is the hostile intruder or attacker who must be identified and kept on hand in case future security issues arise. The algorithms of the previous system engage in unlawful activities. the previous system's algorithms were primarily concerned with authentication, integrity, or confidentiality. This particular set of security requirements has never before been met. [1] suggests combining the RSA and AES algorithms to produce a hybrid cryptography system. Despite the fact that the AES technique requires more processing power than other symmetric key algorithms, researchers still use it for

primary encryption. ECC is more secure than RSA, on the other hand. The absence of integrity and honesty in [1] is another issue. The most efficient methods for web application data security were integrated into the planned effort to address these problems. The finest and quickest solution for web application data security will be the one proposed. By incorporating the suggested work with the current paradigm, this method enables the user to obtain secure and original content in addition to Access authorization, anonymity for posting and downloading, and authenticated and accepted access.

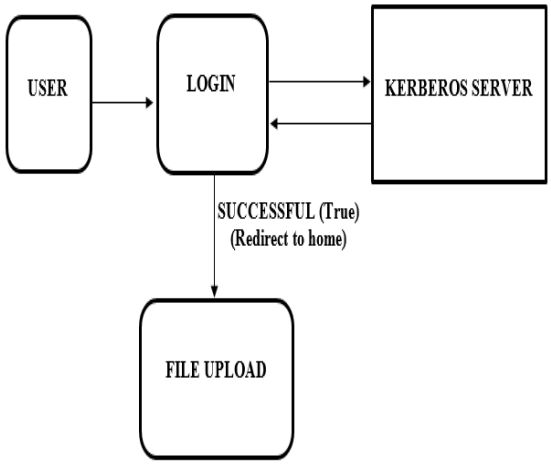

Fig 3: Shows the authentication model's block.

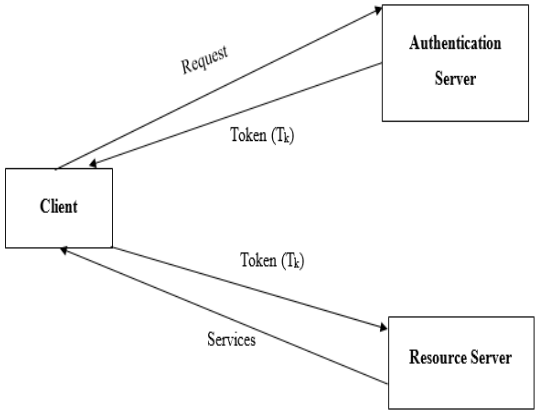

Fig 4. Improved Kerberos Authentication Protocol

The suggested authentication procedures are as follows:
Here are some suggestions about ways to verify your account:

The client must first log in to the authentication server logging into the resource server with their password and email address that handles authentication uses the RC6 technique to create an encrypted token (ETK), which it then gives to the user after confirming the client.
The Client then makes service requests to the resource server using the encrypted token (ETK).

Before checking the resource server checks the token (TK) to verify whether it is no longer valid or not. first decrypts the token (ETK) provided by the client.
If Token (TK) has not yet expired,
The token (TK) will be deleted and the service will end if the resource server does not start offering services to the client.The token (TK) will be deleted and the service will end if the resource server does not start offering services to the client.

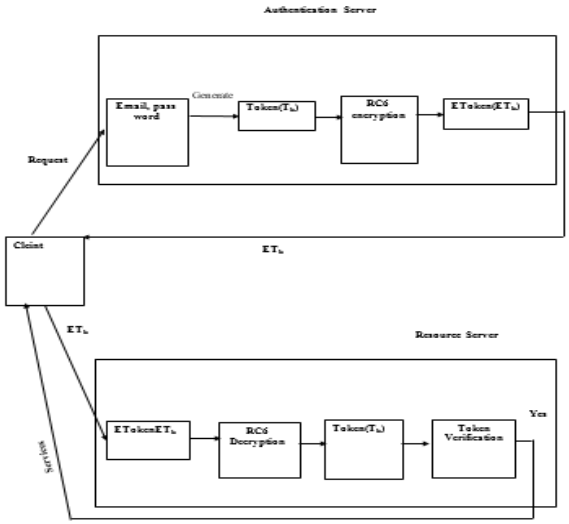

Fig 5. Authentication Protocol Architecture in Detail

Calculation of Integrity Model : The file is being uploaded while the MD5 algorithm generation 256 bit encryption is applied to it. During this procedure, the file's integrity is examined. It will examine the file's uniqueness. Encrypting and decrypting a file can be used to determine its level of confidentiality.

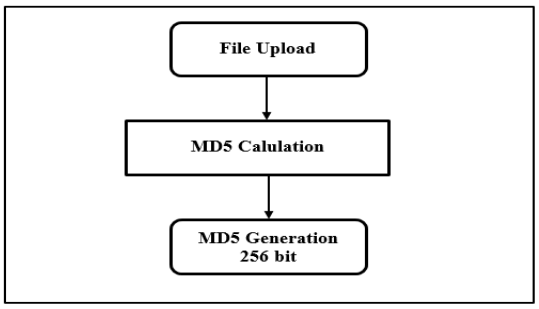

Fig 6. Block Illustration of Integrity Calculation

A file's confidentiality may be determined by encrypting and decrypting it.

3.3 Encryption Model:

Encryption begins by taking a file as input and then dividing it into a number of pieces (C1, C2,... Cn). Separation of even and odd pieces is performed. After that, even and odd chunks are encrypted using the ECC algorithm and RC6 algorithm, respectively, and the cipher chunks are generated.

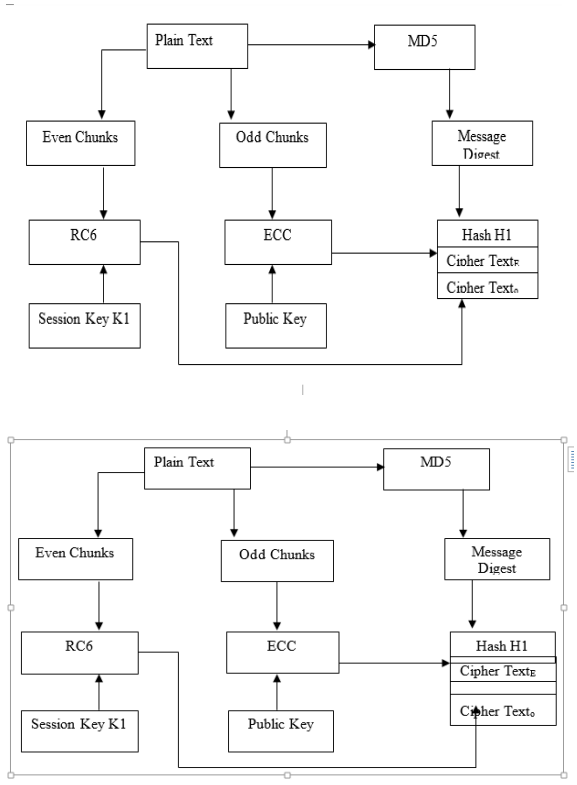

Fig 7. Block Figure of Encryption Architecture

3.4 Decryption Model:

An algorithm to identify even and odd pieces of ciphered data after it has been decrypted. All even chunks are encrypted with ECC and all odd chunks using RC6 are encrypted with ECC. To finish the file, each of these sections is rebuilt.

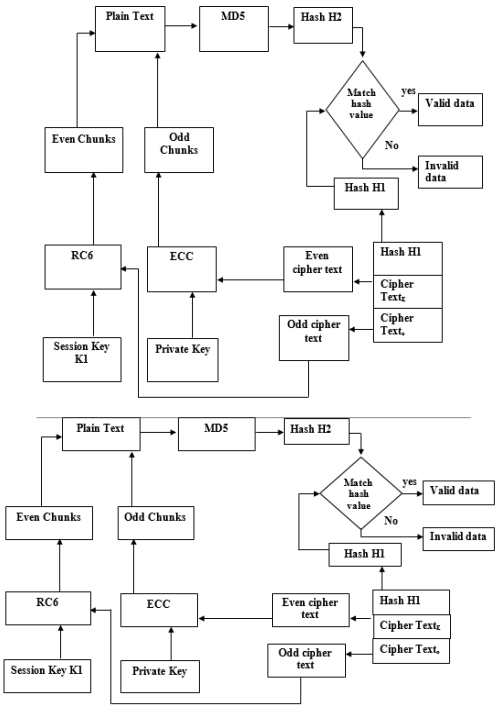

Fig 8. The Decryption Architecture block Figure

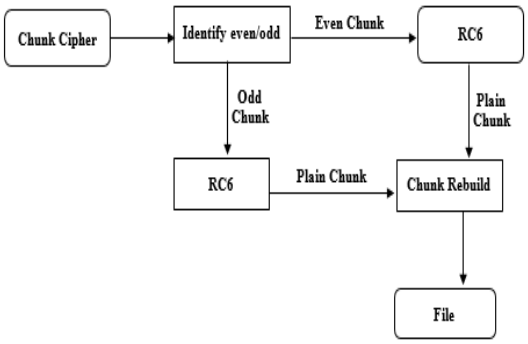

Fig 9. Model for Decryption

3.5 Comparison Model for Integrity:

MD5 is used to recalculate the integrity of the chunk file. A comparison will be made between the recalculated file Hash 2 and the original calculation, and if the results match, the file is accepted and not rejected.

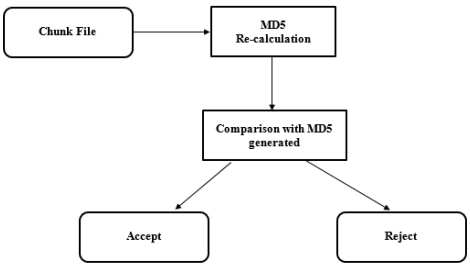

Fig 10. Integrity Check block

4 Implementation Snapshots

The interface used by the finished product is displayed in this chapter. A collection of thumbnails for the project are displayed. The user's email address or password, which is displayed in a screenshot of the client-side authentication interface, is used to log in and send authentication requests. Additionally, information about encrypted and decrypted files is displayed, along with a link to The server's resource page where data can be uploaded or downloaded.

Figure 11 displays the authentication login screen for the user must provide both an email address and a password in order to access the resource server's services. The resource server's services

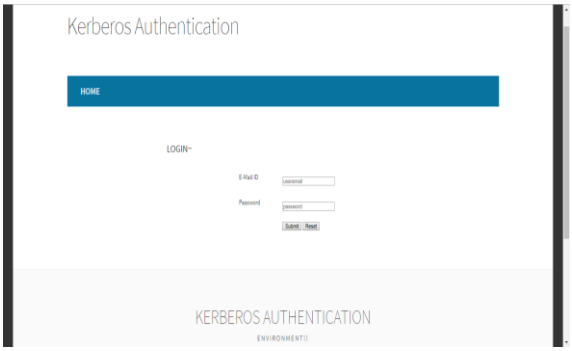

Fig 11. the login page, illustrates Kerberos authentication

In Figure 12, the encrypted token is displayed. You must first authenticate yourself with the authentication server by comparing your credentials to the database records before you can utilise. The services of the resource server

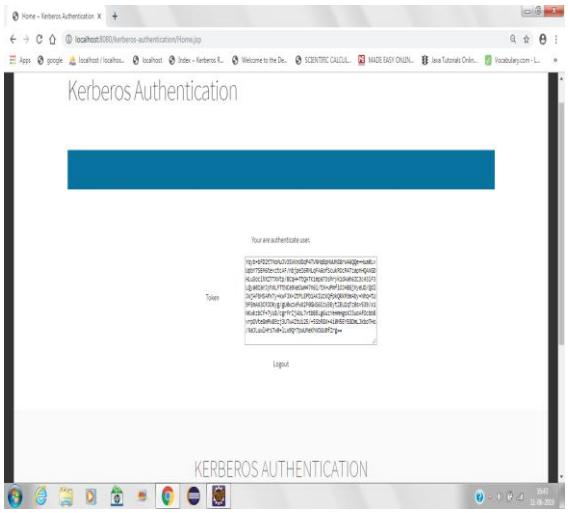

Fig 12. Token Generated

Next page shows the resource server page

Fig 13. Login page via the resource server

Figure 14 shows the resource's home page is depicted

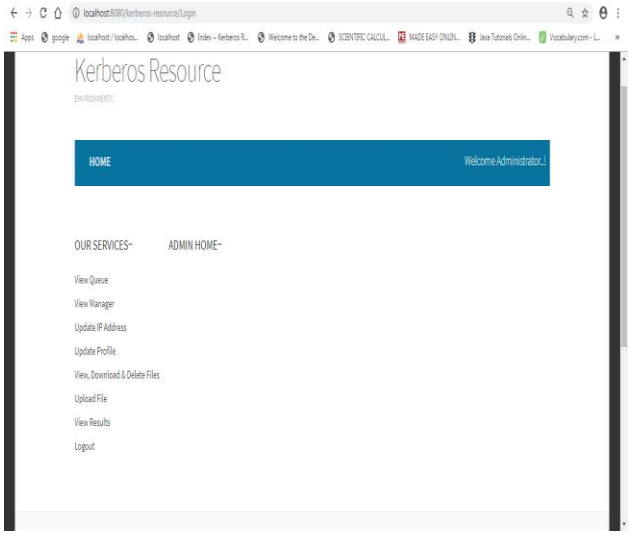

Fig 14. Kerberos resource (Home page)

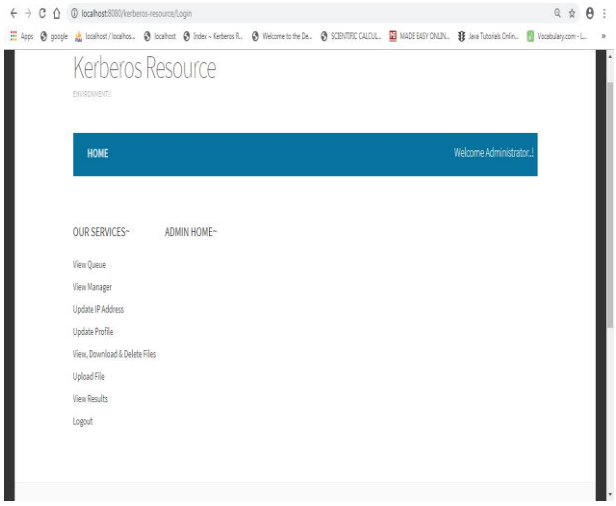

Fig 15. shows the upload window home page

Fig 16. File upload window

Figure 16 displays statistics for encrypted files. After encryption, file, key, and time statistics are displayed in this window The file's id, record name, the size of the file including before and after the encryption, and message digest size are all included in file statistics and the number of chunks the file is divided into. ' The Key statistics display the size of the key that was used to encrypt the file.

The time statistics display the encoding timings for ECC, RC6, and MD5, as well as the total processing time needed to produce the cypher text. Customers can access this page to view or clear their download/upload file history.

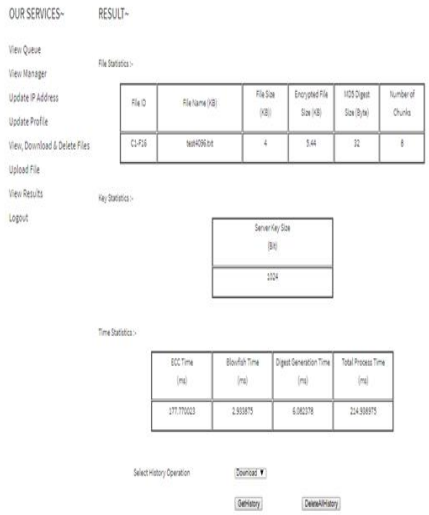

Fig 17. Window for Encrypted File statistics

Figure 18 shows represents the statistics window for the decrypted file.

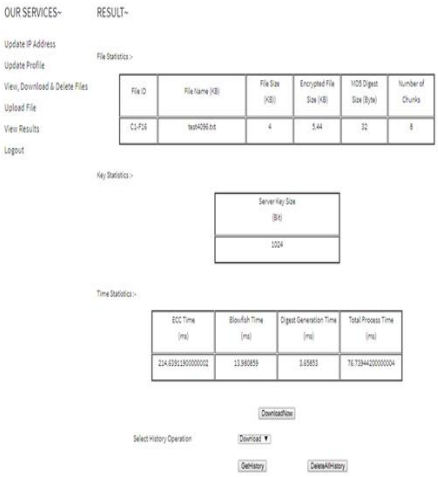

Fig 18. Decrypted File Statistics Window

5. Results Evaluation

5.1 Results Evaluation: Data security, integrity, and authentication in web applications are all ensured by the proposed hybrid model. Compared to other methods, it offers a faster way to encrypt and decrypt data. The intended result is attained using the RC6 and ECC algorithms. The proposed hybrid algorithm's efficiency is measured in terms of the amount of time it takes to encrypt and decode data, as well as the size of the cypher text. The calculation time is calculated with respect to different file sizes. Additionally, the proposed hybrid algorithm and the existing approaches are contrasted.

5.2 Encryption Time: The length of time needed using the algorithm to convert plain text into cypher text is known as the encryption time.

Table 1. Time spent encrypting data overall using the suggested algorithm

Size of plain text(kilobytes)	ECC Time ms	RC6 Time ms	Message Digest Time ms	Total Time Ms
2 kb	19.25	0.37	2.216	30.23
4 kb	45	1.5	3.10	72.20
6 kb	52	1.65	2.35	125.56
8 kb	56.38	1.63	1.67	164.833
10 kb	66.38	3.63	2.36	194.833

The above table 1 demonstrates the time required to encrypt one kilobyte of uncompressed data using different algorithms, including Message Digest, RC6, and ECC. While ECC and RC6 are employed for encrypting and decrypting data to ensure confidentiality, Message Digest is used for verifying integrity. The total time taken to encrypt the file is depicted in Table 1. Additionally, Figure 19 presents these details graphically, offering a statistical perspective.

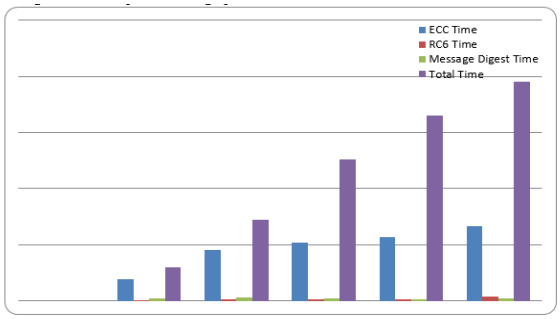

Fig 19. Encryption Time

5.3 Decryption Time:

The decryption time refers to the duration an algorithm requires to convert cipher text back into plain text. This process mirrors the encryption time procedure and is documented in Table 2 in a tabular format. Additionally, its graphical representation is illustrated in Figure 20.

Table 2. Total Decryption Time taken by the proposed algorithm

Size of plain text(kilobytes)	ECC Time ms	RC6 Time ms	Message Digest Time ms	Total Time ms
2 kb	22.25	0.39	2.36	32.36
4 kb	34	1.69	2.45	89.65
6 kb	49	1.98	2.36	136.23
8 kb	64.25	1.85	2.35	175.25
10 kb	69.58	4.23	3.35	215.23

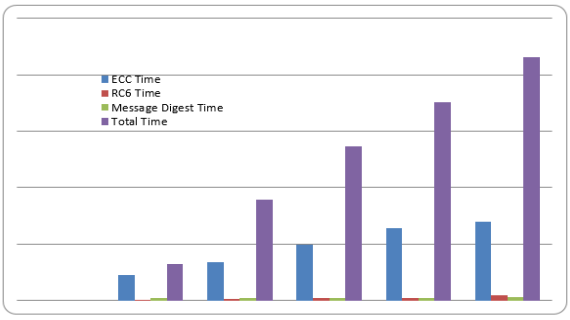

Fig 20. Decryption Time

5.5 Comparison work

Here, a comparison is made between the time needed to encrypt and decrypt files in the proposed and existing work. The comparison involves evaluating the algorithms used in the proposed work against those in the existing work (HCA + THCA). This comparison is detailed in tabular format in Table 3 and visually depicted through a graph in Figure 21.

Table 3. Comparative Table Displaying the Encryption/Decryption Duration of the Proposed Algorithm versus Existing Algorithms

Algorithms	Average Encryption Time / KB ms	Average Decryption Time/Byte ms
Proposed Algorithm	19.25	21.625
Existing Algorithms	76.25	95.36

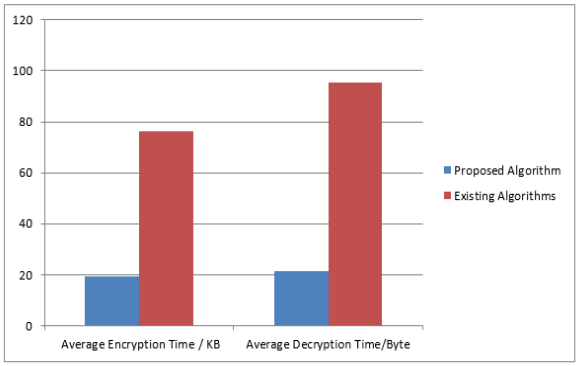

Fig 21. Comparative Table Displaying the Encryption/Decryption Duration of the Proposed Algorithm versus Existing Algorithms

Experimental Analysis of the complete work is described in this section where tables and graphs are plotted to represent the output in statistical form.

6. Conclusion and Future work

6.1 Conclusion: Businesses will be affected by increased Internet usage and automation in conventional sectors. When it comes to running a company these days, many people are shifting their focus to the internet rather of relying only on a brick-and-mortar location. Web applications may help businesses save money, boost productivity, and modernise their procedures. Personal information of customers who use internet applications is always at risk of being accessed by other parties. The existing security paradigm is expected to undergo a transformation that would improve security. The proposed hybrid paradigm aims to provide authentication, confidentiality, and integrity to safeguard data from unauthorised access in online applications. According to the hybrid approach, both ECC (distribution of the key's value) and symmetric key encryption (simpler and faster computation) may be used to assure confidentiality. Hybrid models for securing data in web applications are the best and quickest technique for doing so.

6.2 Future Work : During implementation, we discover that encrypted data is larger than plain text. Encryption and decryption times may be reduced in the future without sacrificing the volume of encrypted data. To apply the hybrid technique to files other than.txt files, such as.mp4 or.doc, would be an option. Military applications, security-conscious hardware and software makers, major websites with enormous databases, mobile apps, and cloud-based applications may all make use of it in the future, as

may many other niche markets.

Author contributions

Kuber Datt Gautam: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Field study. **Dr. Rajeev G Vishwakarma:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] C Akshita Bhandari, Ashutosh Gupta, Debasis D, "A framework for Data Security and Storage in Cloud Computing", International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016, pp. 1-7.

[2] Arora, Rachna, Anshu Parashar, "Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, Vol. 3, pp.1922-1926, 2013.

[3] Wang, Cong, "Privacy-preserving public auditing for secure cloud storage", Computers, IEEE Transactions on Vol 62.2, pp 362-375, 2013.

[4] B. Shereek, "Improve Cloud Computing Security Using RSA Encryption WithFermats Little Theorem", IOSR Journal of Engineering, vol. 4, no. 2, pp. 01-08, 2014.

[5] B. Samanthula,Y. Elmehdwi, G. Howser and S. Madria, "A secure data sharing and query processing framework via federation of cloud computing", Information Systems, vol. 48, pp. 196-212, 2015.

[6] Jin-Mook Kim and Jeong-Kyung Moon,"Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments" published in International Journal of Distributed Sensor Networks by Hindwai Publication Corporation. Volume-1, 2014.

[7] Mrudula Sarvabhatla, Chandra Mouli Reddy M, Chandra Sekhar Vorugunti, "A Secure and Light Weight Authentication Service in Hadoop using One Time Pad", "2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)", Procedia Computer Science 50 (2015) 81 – 86.

[8] TumpeMoyo, and JagdevBhogal, "Investigating Security Issues in Cloud Computing. IEEE Eighth International Conference on Complex", Intelligent and Software Intensive Systems, 2014.

[9]. Nasrin Khanezaei, ZurinaMohdHanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", System, Process and Control (ICSPC), 2014.

[10] Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.

[11] C. Y. Chen and J. F. Tu2, "A Novel Cloud Computing Algorithm of Security and Privacy", Hindawi Publishing Corporation: Mathematical Problems in Engineering, 2013.

[12] G. L. Prakash, M. Prateek and I. Singh, "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science, vol. 3, issue 4, pp. 5215-5223, April 2014.

[13] ChorB,GilboaN,Naor M, "Private Information Retrieval by Keywords", Report 98-03, Theory of Cryptography Library, 1998.

[14] D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Elsevier Journal of Future Generation Computer Systems, vol. 28, pp. 583592, 2012.

[15] F. F. Moghaddam, M. T. Alrashdan and O. Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments", Journal of Advances in Computer Network, vol. 1, No. 3, Sep. 2013.