International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-6, August 2021

Compositional Defence of Application Privacy in Resistant to Physical and Software Attacks in Untrusted Cloud Environment

Mitesh Chanodiya, Manish Potey

Abstract: ***Cloud computing facilities have become an increasing rise in demand for presenting computing sources. Various programs like monetary transactions, fitness care systems, video streaming, IoT programs want on-call for provisioning of cloud sources to guarantee timeliness and excessive availability. A shared culture for data interchange has evolved as a result of the fast progress of networking technology. The data security has become a difficult issue as a result of the vast volume of data that is exchanged via the internet. Thus there is a requirement for security to protect data that is transmitted across an insecure connection. In our proposed work, privacy, confidentiality, availability, integrity, and accountability that contribute to the security of information are ensured by cryptographic technique. This paper also describes an exhaustive study on the usage of hybrid algorithms i.e. the combination of Advanced Encryption Standards (AES) and Elliptical Curve Cryptography (ECC) to protect data leakage and protect the privacy of end-users and SHA256 algorithm to ensure data integrity. This type of hybrid encryption will help not only in concentrating software as well as physical attacks but also provide the model to deal with and prevent the application from these types of attacks; thus making the cloud application system more secure. The implemented web application can be used as a defence system for privacy and security in organizations as well as institutions where members of the organization can share the file or confidential data to other team members or colleagues without data leakage thus providing data privacy and security.***

Keywords: Confidentiality, cryptography, data leakage, data security, integrity, IoT, protect the privacy.

I. INTRODUCTION

In this era of digitization, data privacy and security of confidential information or resources in cloud web applications are important for end-users. Maintainability, flexibility, and uptime are all characteristics of cloud computing. Cloud computing also provides the advantages of budget, carrier on-call, accessibility, internationalization, multi-tenancy, versatility, and durability.

IaaS, PaaS, and SaaS are the three service delivery models of cloud computing service, whereas the patterns include public cloud, personal cloud, hybrid cloud, network cloud, & digital personal cloud. However, while transmitting the data in an untrusted cloud

applications, there is a possibility of data leakage. Thus, there is a need to provide a compositional defence system in cloud applications in order to protect the information or resources present in the application against various kinds of attacks.

The main objective is to concentrate on the attacks which compromise the privacy of user applications which has to be taken into consideration for defence systems. Design the models and methodology or approach against concentrated physical attacks mounted on hardware and software attacks. Providing confidentiality of file that stored in a public cloud storage with the trusted level of security. Enhance the prevention of files against cryptanalytic attacks and brute force at a high level. Creation and analysis of algorithm which best fit for compositional protection of the application privacy even in an untrusted cloud environment. Provide solution; thus creating a compositional defence system to minimize the threat to the privacy of application against respective physical and software attacks.

The privateness safety of cloud computation is usually a warm subject matter in instructional groups. Various authors mentioned 5 safety and privateness attributes (confidentiality, privateness safety, integrity, availability and accountability) and confirmed safety vulnerabilities, danger fashions and protection techniques however lacked a precise overall performance evaluation description.

Fig. 1: Cloud Application Privacy Protection [1]

Manuscript received on July 28, 2021.
Revised Manuscript received on July 31, 2021.
Manuscript published on August 30, 2021.
* Correspondence Author
Mitesh Chanodiya*, Department of Computer Engineering, K.J. Somaiya College of Engineering, Vidyavihar, Mumbai- 400077, India. Email: mitesh.chanodiya@somaiya.edu
Dr. Manish Potey, Department of Computer Engineering, K.J. Somaiya College of Engineering, Vidyavihar, Mumbai- 400077, India. Email: manishpotey@somaiya.edu

Cryptographic techniques provide secure data transmission, but there are some complexities in existing systems. Most of the cryptographic techniques are time consuming processes. Some techniques do not include integrity checks on transmitted data. Another issue is the lack of security during key exchanges. In order to implement an effective cryptographic algorithm, all these aspects have to be considered in order to make it robust. There is a need to implement the technique which helps to overcome such complexities in such an existing system. The Proposed hybrid cryptographic technique uses the best features of symmetric (AES) and asymmetric (ECC) cryptographic technique with a hash function (SHA256). So that, this technique helps to reduce the time complexity. Also, provides authentication and the validation of data integrity.

In order to permit companies and groups to use cloud computation era & supply their very self-records to CV (cloud vendors), it's miles vital to research & resolves privateness and safety, encryption, get right of entry to manage and accept as true with troubles with inside the cloud computing. Overall, the present-day studies and development on cloud computing privateness safety remain in the toddler stage, and an entire studies gadget has now no longer but been formed. A steady envelope presents the safety of foundation and the non- manipulation of the text primarily depending totally on a common mystery key among verbal exchange vendors or clients. But, it's not a standalone safety measure maintaining the security of privacy in cloud applications. Therefore, a way to obtain absolute-grained security and privateness safety inside the system of dynamic records updating is a must to enhance the performance of cloud computing applications.

The scope of this paper is to address the robust risk version, in which cloud vendors, the visitor OS, and VMM aren't always to be relied on. The risk version is in particular applicable to cloud computing due to the fact relied on packages run inside the cloud. Our compositional answer preserves the privateness of the packages simplest by taking an assumption that the hardware is relied on whilst the visitor Operating Systems and VMMs are nonetheless liable for aid administration. Also, to provide file confidentiality to the user, when the user wants to store the file in public cloud storage using hybrid encryption techniques and local PC.

The major goal of the feasibility study is to see if establishing a computerised system is technically, operationally, and economically feasible. A feasibility study is carried out to see if the system is possible to implement so that user needs can be satisfied. The following are the most important factors to consider while doing a feasibility analysis:

- Technical - can be done in current equipment existing software and available
- Operational - user of the system can easily work and interact with the system
- Economical - changes, if required, can be easily made to the system at minimum cost. Hardware, software, storage, operating and maintenance cost are within budget
- Time Feasibility - As a result of applying a planned strategy to task completion, the proposed work can be completed on schedule.

Section I shows the introduction part, Section II contains the literature survey determining the defence system of application privacy, Section III includes methodologies and approach, Section IV explains the design and implementation of different algorithms used to protect the information security, Section V shows the results and Section VI focuses on conclusion.

II. LITERATURE SURVEY

It's frequently assumed that the cloud vendors, as well as the system, can be trustful; the visitor Operating System or the VMMs have efficient security. These assumptions can be questioned given the invention of weakness inside the product VMMs also the truth that OS weakness frequently assists in cyber-attacks.

Fig. 2: Cloud Application System[2]

In 2018, Cloud computing experts mentioned 5 protection and privateness attributes (confidentiality, privateness safety, secrecy, accessibility, accountability) and confirmed protection weakness, danger fashions, and protection techniques however lacked a particular overall performance evaluation description. A comparison of encryption approaches using symmetric and asymmetric key methods is investigated. In terms of cost, security, and construction, the AES algorithm is shown to be superior in symmetric key encryption. In terms of speed and security, the RSA method is superior in asymmetric key encryption. Different types of symmetric and asymmetric algorithms are explained. DES, 3DES, and AES are examples of symmetric algorithms. RSA and Elgamal are two asymmetric algorithms[3]. When compared to asymmetric systems, the performance findings reveal that symmetric techniques are computationally less expensive.

In 2019, cloud experts searched diverse techniques of mystery communicating, inclusive of mystery channel, pass, and fuzzy era. However, those techniques incorporate a form of non-general era and utility, and the utility level maybe not is so broad. Pharmaceutical data in computation of cloud are probably to be exposed[4].

Existing encryption methods are investigated and researched in order to improve the performance of encryption systems while simultaneously ensuring security.

All of the strategies may be used to encrypt data in real-time. Each methodology is distinct in its own manner, and it may be appropriate for a variety of purposes. Different key algorithms such as AES, DES, 3DES, Blowfish, and RSA are examined and compared in this paper. According to the findings, AES and Blowfish are the safest and efficient symmetric encryption methods[5]. These algorithms outperform the others in terms of speed and power usage. Because of its speed and security, RSA is a safe asymmetric encryption method that may be employed for wireless network applications.

Fig. 3: Secure Systems in Cloud Infrastructure[6]

The safety desires of the proposed answer are to guard the statistics privateness of the packages with inside the cloud computing surroundings below the safety version such that the VMMs, the visitor Operating System, and the supplier of cloud each of three cannot get admission to the utility's statistics without permission. The proposed answer does now no longer take into account facet channel assaults towards the execution surroundings. In practice, any development in facet channel prevention techniques may be included in the proposed option to keep away from facet channel threats. Another safety thing that isn't always protected with the aid of using the proposed answer is denial-of-provider assaults. Due to the fact that the VMMs and the visitor Operating Systems are accountable for assets control and challenge timetable and we anticipate those events aren't dependent on with inside the safety version[7].

In 2017, Image encryption and decryption using the ECC algorithm is implemented to ensure authenticity and integrity, the coded picture must be encrypted, decrypted, and digitally signed. The ECC algorithm is proposed to compute the value of a secret key without exposing it to the rest of the network. Encryption and decryption operations are carried out using the coordinate system's block code. The suggested system can protect against plaintext assaults, man-in-the-middle attacks, and other types of attacks. A hybrid cryptography technique using AES and ECC is proposed. The system is designed to protect a wide range of multimedia content, including text documents, photos, audio, and video. A hybrid system is proposed that can encrypt and decrypt sensitive information to protect it from unwanted access and assaults. Also, the cloud scientists confirmed the capacity demanding situations of fog safety and investigated the contemporary answers to protection and privateness weakness. Moreover, the paper in particular displayed the improvement of the IoT, not often mentioned in the studies. Elliptic curve cryptography (ECC) is a relatively recent kind of public key encrypting technique that offers greater security per bit than previous kinds of encryption now in use[8]. Encryption and decryption of text using ECC are explained with the mapping technique. It is concluded that ECC has low power consumption, less memory requirement, small key size, and high security.

In 2018, the Hybrid cryptography approach is implemented using AES and ECC. This system provides encryption to the multimedia data such as text, image, audio, video which resulted in output with 100 percent accuracy without any loss of information. Various text files are used as input and encrypted using a hybrid AES-ECC technique. The analysis of AES encryption with ECC is based on many characteristics such as storage requirements, encryption time, and decryption time. A hybrid approach for encryption technique is implemented over a binary image, all of which improve the encryption process' correctness. The ECC and AES are coupled in a way that sets them apart from other encryption methods. With the rising trend of security, it is more important than ever to properly secure data and information[9].

In 2017, SHA1 and MD5 algorithms are explained in detail. It is concluded that SHA1 is faster than MD5, and SHA2 is even more secure than SHA1 and MD5. Which algorithm is more suitable for the particular message is discussed. The detailed design of hash function MD5, SHA1, SHA2, SHA3 is provided. Different parameters are Hash functions are analyzed by comparing with each other. The working of SHA-256 is explained. SHA-256 is a digital data-encrypting mathematical formula. To ensure the data's integrity, the computed hash is verified to a predicted hash value[10].

III.METHODOLOGY AND APPROACH

There is a requirement for security to protect data that is transmitted across an insecure connection. Cryptography is a Greek term that meaning "hidden writing." The plaintext is the message that will be sent via unreliable media, and it will be encrypted before being sent. The encrypted communication is called code text, and it is received at the opposite end of the medium and decoded to reveal the plaintext message[11].

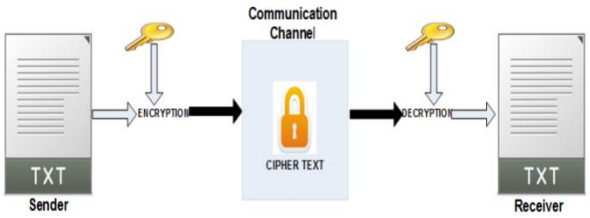

Fig. 4: Encryption-Decryption

The figure above illustrates how encryption and decoding function. The sender encrypts the message with the secret key and sends it across the communication channel, as shown in Figure 1.

The secret key is used by the receiver to decode the message. Cryptography achieves a multitude of security needs, including data privacy, non-alteration, and so on. Cryptography is extensively utilized nowadays due to its significant security benefits. There are two types of cryptography algorithms: symmetric key cryptography and asymmetric key cryptography. E-commerce, chip-based card payments, virtual money, pc password, and mobile surveillance for the military are all examples of cryptography applications.

1. Non abrogation of Origin with Privacy Protection

The existentially unforgeable virtual signatures (however now no longer all) may be considered as usage of non-abrogation proof of foundation in verbal exchange order. Moreover, in everyday virtual signs, the Check set of rules simplest makes use of the signer's key which is public pk to check the expiry of a sign message text combination[12]. Hence, as soon as provided a legitimate sign message text combination beneath neath pk, each person might be satisfied that the text becomes undersigned with the aid of using the proprietor of pk and accordingly discover who's the sender of the message. This ownership, collectively along with the benefit of imitating and addressing virtual signs, may show unwanted in individually or business terms touchy packages wherein the text jobber's privateness is the main task.

The approach is as shown below:-

1.1. Receiver Initialize:-

The receiver choose a number which is random xR from Z multiplied by p and calculate yR = gxR. Let the pair

(pk-R, sk-R) = (xR , yR).

1.2. Sender Initialize:-

The one who is sending choose a number which is random xS from Z multiplied by p and calculate yS = gxS. Let the pair (pk-S, sk-S) =(xS , yS).
Send{pk_R, sk_S, m} ⇔ Receiver{pk_S, sk_R, period}.

- The one who is sending initially calculate sigma = H1(m, period)xS , the CRH (complete realm hashed) one of the variation of variant of Chaum's not deniable sign.
- The one who is sending then generate a dvp ro = (cS , cR ,dS ,dR), stating that one who is sending has the knowledge of secrecy sk:

"sk = DLg [yS] = DLH1(m,time)[σ]" or "sk= DLg[yR]".

In other words, the sender either demonstrates that is a genuine irrefutable signature of pk S or that he or she possesses the recipient's private key. It's worth noting that the evidence can be generated by both the sender and the receiver. The secrecy sk is xS for the sender, and the proof = (cS, cR,dS,dR) is created as follows:

- Chooses three rand integers r, cR ,dR from Z multiplied by p ;
- Calculates cS = H2(gr, H1(m, time)r , gdR ycRR)−cR;
- Calculate dS = (r −cS xS) |p|.

The production is based on Chaum's pseudo 0 knowledge proof, which assures that it is an invalid irrefutable signature, the message sender will not be able to produce the proof.

- The one who is sending transmits the triple (m,,) to the receiver, with the evidence of origin being.
- Given (m,sigma,ro) and = (cS, cR,dS,dR), the recipient accepts (m, pk-S, time) as a valid triple iff H2 gdS ycS S, H1(m, time)dS cS, gdR ycR R = (cS +cR) |p| (1)

The recipient of a valid triple will maintain track of the accompanying proof of origin, i.e. ro.

1.3. Receiver-Simulate:-

This set of rules permits to act as the protocol's receiver Send Recipient and create a proof with the simulation of foundation. To do it in general, for a proof with the simulation of the foundation created with aid of using the set of rules Receiver-Simulate, 1(along sk S) can run a set of rules Creation Proof Public to create a string of bit π so that Check Public output "0". They are actually geared up to outline the privateness of text origin in verbal exchange rules with non-abrogation of foundation [13].

2. The Iterative Approach

The model is divided into six main stages:

2.1. (a) The problem is specified, as are the planned service objectives (goals); and (b) the constraints are recognised during the analysis of requirements phase..

2.2. During the phase of specification, the full definitions of (a) and (b) above are used to create the system specification. The product function should be explicitly defined in this text.

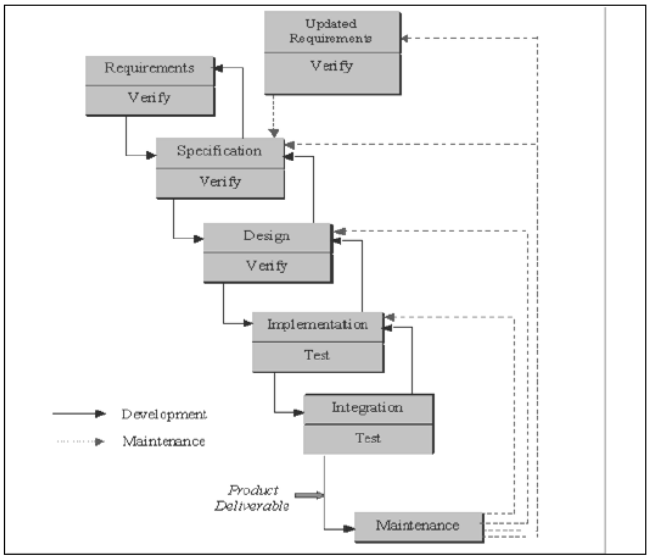

Fig. 5: The Iterative Approach

2.3. Throughout the system and software design process, the system requirements are converted into a software representation. The software engineer is dealing with the following in that level:

- Data structure
- Software architecture

- Algorithmic detail
- Interface representations

The requirements of hardware, as well as a picture of the entire system architecture, are defined at this stage. The developer of software can determine the link between interfaces that are associated, software as well as hardware at the conclusion of this stage. Any flaws in the specifications should preferably not be passed on to the downstream process.

2.4. The designs are transformed into the software realm during the implementation and testing phase.

- Thorough review from the design phase may save a lot of time and work when it comes to coding.
- At this step, testing is focused on identifying any mistakes and ensuring that the programme satisfies its requirements.

2.5. All programme units are combined and tested during the integration and system test phase to check whether the entire design fulfills the requirements of software. [Deliverable - The piece of application is provided to the client for user acceptance.] Following step, the application is provided to the consumer.

2.6. The maintenance of application/software phase is frequently the most time-consuming. The software is changed throughout this phase to:

- Meet evolving client demands
- Adapt to external environmental changes
- Corrected faults and inaccuracy that were previously unnoticed during testing
- Improving the software's efficiency

It's worth noting that loops of feedback enable for model updating that must be implemented. A issue or update in the phase of design, for example, necessitates a visit again to the specs phase[14]. When modifications are done at a point during the process, the corresponding documentation should be changed to showcase those changes.

IV. DESIGN AND IMPLEMENTATION OF ALGORITHMS

This section describes the architecture diagram, control flow graphs, hybrid algorithms i.e. combination of Advanced Encryption Standards (AES) and Elliptical Curve Cryptography (ECC) to secure the confidentiality of the information and protect data leakage as well as SHA256 (Secure Hash Algorithm) to check the integrity of data.

1. *Architecture Diagram*

The architecture design is to create defence system against software attacks mainly cyber-attacks. There can be many software attacks to get the leakage of application privacy; out of which major cyber/software attacks can be as follows:-

The 3 main cyber-attacks which contribute to the world of cybercrime also known as “BIG 3” are-

- Malware – a phrase in usage to showcase software which is malicious, which includes spyware.
- Ransomware – until you pay a ransom amount to hacker, your files are denied to access to your system
- Phishing - the act of duping receivers into revealing sensitive data with an unknown individual may be third party [17].

In our design architecture, we will be mainly dealing with phishing attacks.

Phishing is a form of social engineering assault that is commonly used to steal sensitive data from consumers, may be passwords for login and credit card numbers. When a hacker appears as recuperations and persuades a victim to click on a link of email, instant chat, or text message, this is known as phishing. The recipient is then fooled into opening a malicious program, which could also result in the installation of malware, a systems freezing as part of a data breach, or the exposure of top secret information.

The architecture diagram of proposed thesis to deal with software attacks maintaining a compositional defence system for application privacy is as follows: -

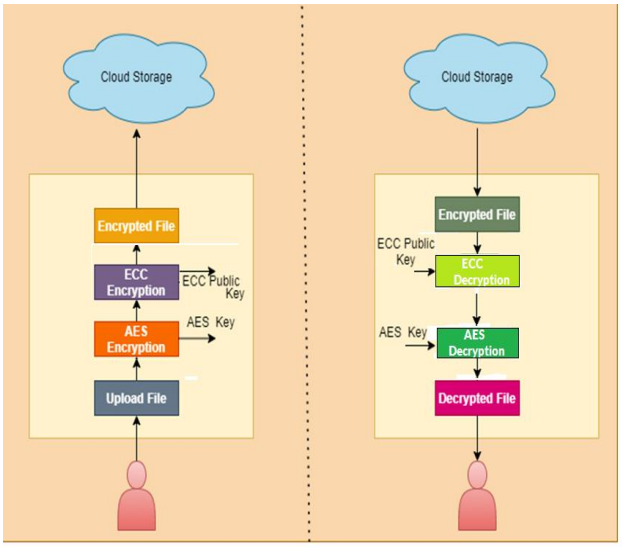

Fig. 6: Architecture Diagram (Control Flow Graph) for Application Privacy

2. *Advanced Encryption Standard (AES)*

AES consists of a symmetric cube code that employs a replaces or facilitates the acquisition to encrypt data. AES's data block and key lengths can be customized to meet specific needs. Three key lengths are used: 128, 192, and 256, with iteration cycles of 10, 12, and 14 rounds, respectively. Rounds change, turns, and key expansion are the three basic features of the AES algorithm. Each round transformation is made up of three layers: a non-linear layer, a linear mixing layer, and the round key layer[15]. The figure below depicts the AES encryption method.

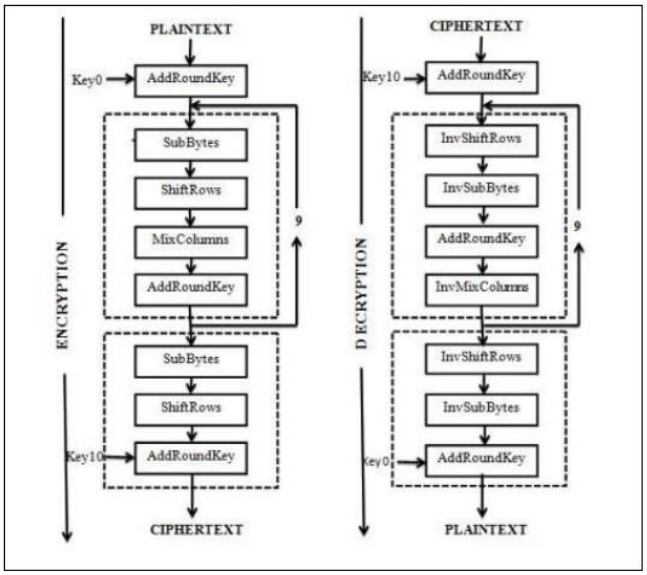

Fig. 7: AES encryption & decryption process[16]

3. *Cryptography using Elliptic Curves (ECC)*

Elliptic curve cryptography (ECC) is a newer kind of public key encrypting technology which offers better security per bit than previous kinds of encryption currently in use. In mathematics, elliptic curves are cube curves that are geometrically identical to tori. They are not connected to the ellipse, unlike their name, although they do obtain their name from the ellipse integral. The Weierstrass normal form, which is the most fundamental universal elliptic curve being used in cryptography, is y2 = x3 + axe + b, as seen in figure 3. Different values for a and b produce curves of this type[17].

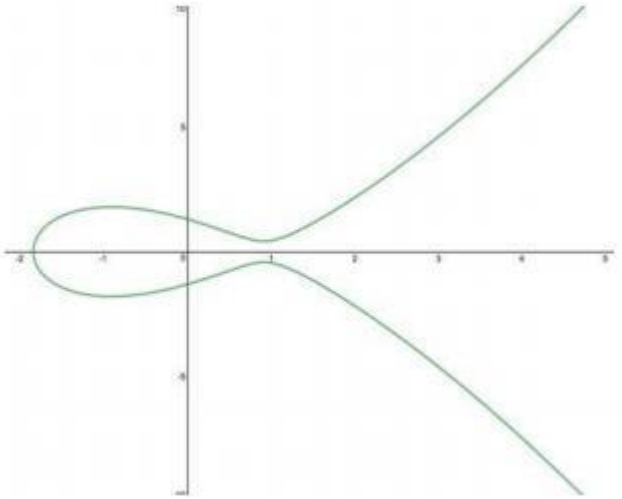

Fig. 8: ECC Curve Graph[17]

4. *Secure Hash Algorithm (SHA256)*

The SHA-2 functions of hash are a series of cryptographic hash algorithms. SHA-2 has several variations, which include SHA-224, SHA-256, SHA-384, SHA-512, SHA512/224, and SHA-512/256. SHA-2 differs significantly from its predecessor, SHA-1, in terms of features. SHA-2 is presently made up of 6 hash algorithms with the intake of 224, 256, 384, or 512 bits. SHA-256 is a digital data-encrypting mathematical formula. To validate the data's integrity, the computed hash is compared to an anticipated hash value[18].

5. *Data Flow Graphs*

The data flow graphs for both sender who is also an Admin in the web application as well as the recipient who will receive the shared file is as follows: -

5.1. *Sender (Admin)*

Admin is a host who controls application by maintaining recipients i.e. the users to whom the admin will be sending the files of various formats such as jpg, png, pdf, docx files etc. Admin will login first, can add recipients, select a file to be sent to receiver after encryption which will be sent to cloud storage management. Cloud Storage Management will split the file, undergoes AES and ECC encryption, generate the key value and upload the files to the database as shown in the figure below.

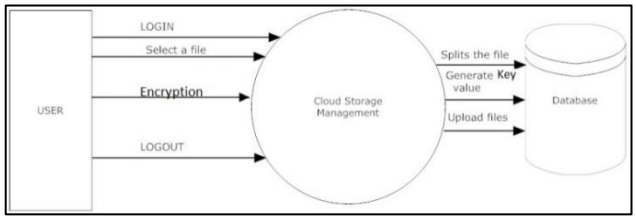

Fig. 9: Data Flow Graph of Admin User and Cloud Storage Management

5.2. *Recipients*

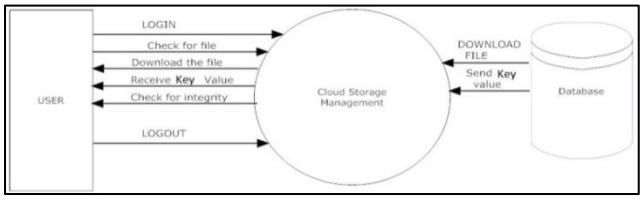

Fig. 10: Data Flow Graph of Recipient User and Cloud Storage Management

The user who will be receiving the data will login using the credentials sent by the admin via mail for the first-time login. Thereafter user can change the password for future use of the application. Then the user will check the file shared by the admin user. To access the file, the receiver will take the key triggered on the mail to download the file. The user can also check for the integrity using the hash value of the received file and original file.

6. *Sequence Diagram (Process flow)*

The sequence diagram explaining the flow of the process for both sender who is also an Admin in the web application as well as the recipient who will receive the shared file is as follows: -

6.1. *Sender (Admin)*

Following is the Sequence diagram to get the process flow of admin to get the knowledge of the overall step by step process to be followed to add user, upload file, and share the file to the respective user

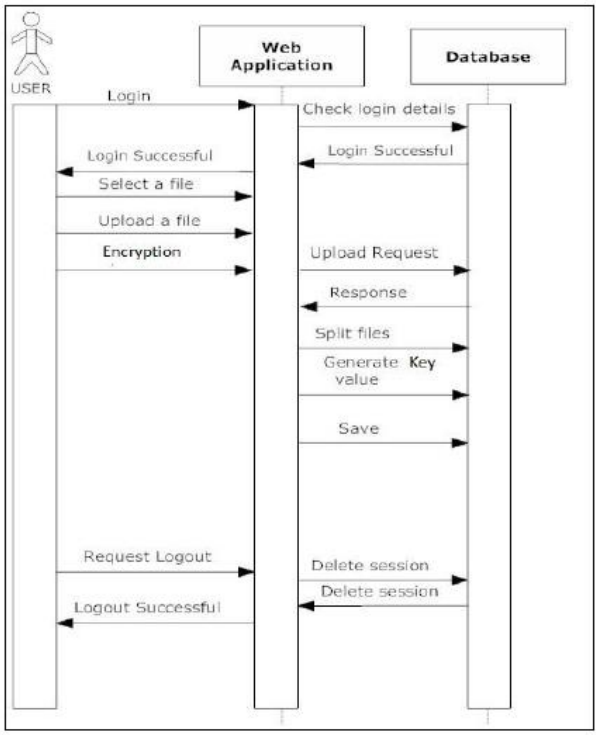

Fig. 11: Sequence Diagram of Admin User

6.2. Recipients

Following is the Sequence diagram to get the process flow of the receiver to get the knowledge of overall step by step process to be followed to check for file, receive key value for particular files, download file, check the integrity, login and logout session.

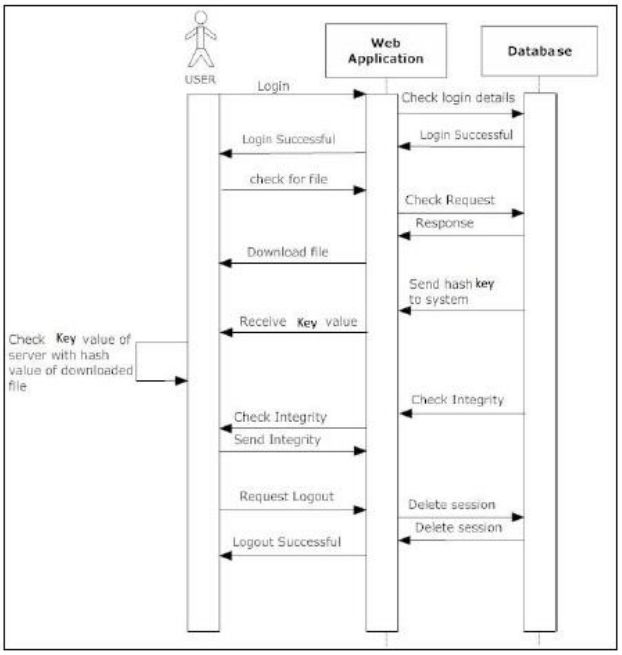

Fig. 12: Sequence Diagram of Recipient User

V. RESULTS

The web application is implemented in the .net framework using C# and SQL Server Management Studio and hosted on Microsoft Azure Cloud Service. These web applications as discussed earlier consist of two versions:-

- One with a single algorithm using symmetric cryptography AES algorithm
- Second with hybrid algorithm i.e. combination of both symmetric hidden AES algorithm and asymmetric ECC algorithm.

Each of these versions of the web application consists of two sessions:-

- One session is for the sender (admin) who will login, register the user to whom he wants to send the file, upload the file and share the file to that respective user.
- The other session is for the receiver (user) who will login, can see the list of shared files, uses the key received on mail to decrypt and download the file and check the hash value to ensure the integrity of the data.

1. Snapshots of Implemented Web Application

Below snapshot describes the home page of the admin after successful login, which consist of multiple tabs that admin can go through such as manage users, manage files and share files.

Fig. 13: Home page of Admin Session of website

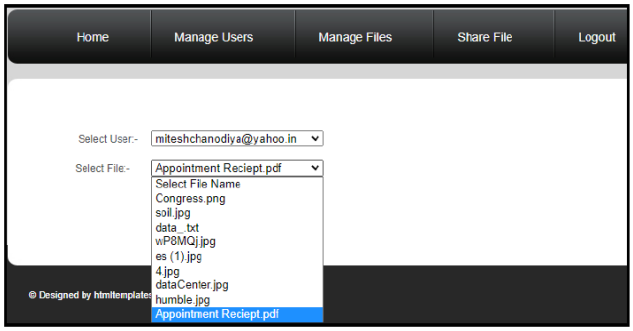

Fig. 14: Window to share file by selecting respective user and particular file from drop down menu

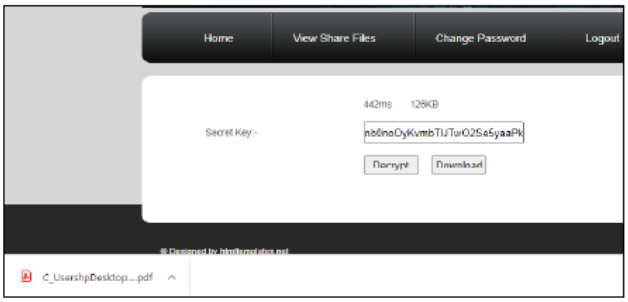

Fig. 15: User Session after decryption of file using hybrid AES and ECC algorithm

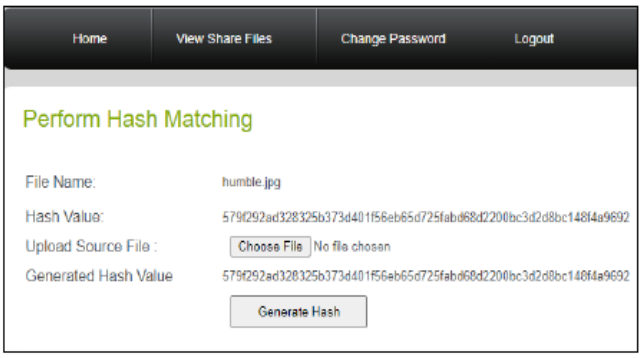

Fig. 16: Window displaying hash value matched of original file and received file to ensure the integrity of the data

2. Comparison of single AES and Hybrid AES-ECC algorithm

Following table shows the overall analysis of different types of files used while uploading and encrypting admin session while the time required to decrypt those respective files in user sessions and thus calculating performance evaluation as follows:-

Table 1: Analysis of different files, time complexity and performance evaluation

File (name.type)	File Size (in kb)	Time (in milli-sec) using AES	Time (in milli-sec) using AES-ECC	Performance Evaluation in %
humble.jpg	80	181	442	59.04
Appointment Receipt.pdf	126	263	654	59.78
Congress.png	268	286	689	58.49
data_.txt	54	87	206	57.76
datacenter.jpg	11	53	122	56.55

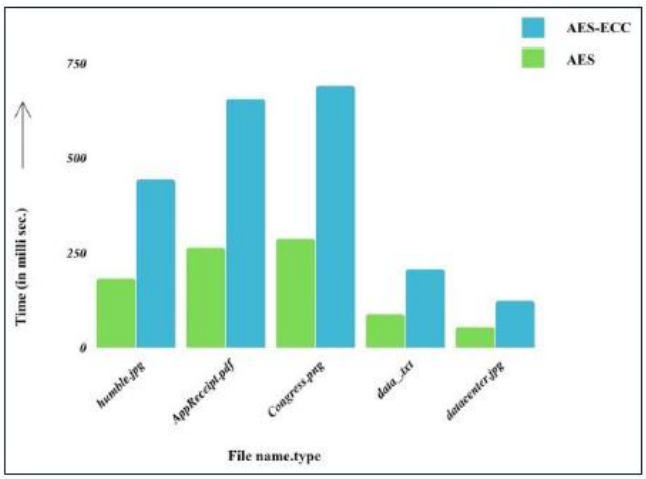

Fig. 16: Graph of Time required for AES and AES-ECC for different file types

VI. CONCLUSION

As per the findings, literature survey, objectives stated and above implementation of hybrid algorithms, the following conclusions are drawn as follows:-

- Based on the literature survey, cloud experts mainly deal with avoiding physical attacks such as on-chip hardware overhead, sealed memory context access, etc.
- The software attacks which are a major threat to cloud computing are phishing attacks which in turn raise both malware and ransomware attacks.
- Cyber-attacks are detected to determine the loop or gaps in cloud applications that pose threats to application privacy in a cloud environment.
- Hieroglyphic inscription which is an AES encryption technique along with hybrid encryption Elliptic Curve Cryptography tackles the problem of leakage of application privacy data in cloud systems.
- UI development of application peers, web server, and cloud storage management is implemented to get connections of end-users, internet via gateway channel and tracking the status of established connections.
- The limitations of various cryptographic techniques are analyzed and a hybrid system with hash function is proposed which is the combination of the AES, ECC, and SHA256. This methodology was implemented for the secure sharing of the data across various applications.
- Text and images with different file sizes are taken as input. Encryption is performed on the original file and is sent to the intended receiver. The receiver decrypted that file using the secret key and then matching of hash is performed.
- The successful hash matching indicates that data is not altered. This system performs encryption and decryption for better security of confidential data.
- It protects sensitive data from unauthorized access and attacks. It provides a hybrid approach to sharing and accessing the data that is secure.

Thus, the combination of more than one algorithm such as AES, ECC and SHA256 etc. makes the compositional defence system to protect privacy of application against software attacks in untrusted cloud environment.

REFERENCES

1. Lei Xu, JongHyuk Lee, Seung Hun Kim, Qingji Zheng, Shouhuai Xu, Taeweon Suh, Won Woo Ro,and Weidong Shi, "Architectural Protection of Application Privacy Against Software and Physical Attacks in Untrusted Cloud Environment", IEEE transaction paper on cloud computing, March 2018.
2. Pan Jun Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions", IEEE Journal of Information Security Special Project, Development and Reform Office, publication-October 9, 2019, current version-October 23, 2019.
3. Wei Wu, Jianying Zhou, Yang Xiangc, Li Xua, "How to achieve non-repudiation of origin with privacy protection in cloud computing", Elsevier Journal of Computer and System Sciences 79 (2013) 1200–1718, China, 2018.

4. Pan Jun Sun, "Security and privacy protection in cloud computing: Discussions and challenges", Elsevier Journal of Network and Computer Applications, 160 (2020) 102642, China, 2020.
5. Jun Feng, Laurence T. Yang, Fellow, Ronghao Zhang, Weizhong Qiang, and Jinjun Chen, "Privacy Preserving High-Order Bi-Lanczos in Cloud-Fog Computing for Industrial Applications", IEEE Journal of Industrial Informatics, 2998086, University of Wollgong, China, 2018.
6. N. G. Nageswari Amma, F. Ramesh Dhanaseelan, "P2CADL : Privacy Preserving in Cloud using Autoencoder based Deep Learning Classifier for Smart City Applications", IEEE Journal of Computer Sciences, Carleton University, India 2018.
7. Benjamin Camus, Anne Blavette, Fanny Dufosse and Anne-Cecile Orgerie, "Self-Consumption Optimization of Renewable Energy Production in Distributed Clouds", IEEE International Conference on Cluster Computing, pp. 2168-9253, IEEE, 2018.
8. Sampa Sahoo, Bibhudatta Sahoo and Ashok Kumar Turuk, "An Energy-efficient Scheduling Framework for Cloud Using Learning Automata", 9th ICCCNT, IISC, Bengaluru, India, July 10-12, 2018.
9. Pingping Xu1, Guilu Wu, Zhifang Gu and Shujun Wang, "Joint Relay Selection and Power Allocation for Energy-limited Networks with Cloud Computing", 17th International Symposium on Distributed Computing and Applications for Business Engineering and Science, China, 2018.
10. Juglul Hasan, Tanjim Ul Haque, Sabab Hasan, "Cloud-Based Automated Power Consumption Optimization, Power management, and Appliance Control", 1st International Conference on Advances in Science, Engineering and Robotics Technology, Dhaka, Bangladesh, 2019.
11. Heba Kurdi, Shaden Alismail and Mohammad Mehedi Hassan, "LACE: A Locust-Inspired Scheduling Algorithm to Reduce Energy Consumption in Cloud Datacenters", King Saud University's Deanship of Scientific Research, IEEE, Volume 6, pp.2169-3536, 2018.
12. M. D. Ryan, "Cloud computing privacy concerns on our doorstep," Commun. ACM, vol. 54, no. 1, pp. 36–38, Jan. 2011.
13. Secunia, "Advisory sa37081 - VMware ESX sever uodate for DHCP, kernel, and JRE," http://secunia.com/advisories/37081/.
14. P. Ferrie, "Attacks on virtual machine emulators," Symantec Security Response, vol. 5, 2006.
15. K. Kortchinsky, "Cloudburst – hacking 3D and breaking out of VMware," in Black Hat USA, 2009.
16. T. Ormandy, "An empirical study into the security exposure to hosts of hostile virtualized environments," in CanSecWest, 2007.
17. R. Wojtczuk, "Subverting the Xen hypervisor," in Black Hat USA, 2008.
18. J. Szefer and R. B. Lee, "Architectural support for hypervisor secure virtualization," in Proceedings of the seventeenth international conference on Architectural Support for Programming Languages and Operating Systems, ser. ASPLOS '12. ACM, 2012, pp. 437–450.

AUTHORS PROFILE

Mitesh Chanodiya, currently pursuing Masters in Computer Engineering from K.J. Somaiya College, Vidyavihar, Mumbai, worked on Streamlining Power Consumption in Data Hubs of Distributed Clouds, GST Billing Software for Business Management System, Completed Bachelors of Electronics Engineering from Ramrao Adik Institute of Technology, Nerul, Navi Mumbai in 2018, worked on projects titled Face Detection and Tracking, Ultrasonic Map Maker, Published the paper titled 'PIC Based Automated Solar Radiation Tracker' in National Level Students' Conference on Frontiers in Engineering and Technology Applications - 2018, worked as IT Backend Production Developer in Godrej Housing Finance Ltd., completed certification courses in Big Data Computing, Python Bootcamp from Udemy, Algorithm- Backtracking from Coding Blocks.

Dr. Manish Potey, presently working as Professor in Computer Engineering Department, Student Branch Counsellor (SBC) Computer Society of India (CSI) KJSCE, Member Local Inquiry Committee, University of Mumbai, Former Head of Department of Computer Engineering, KJSCE, Completed Masters of Engineering (Computer Science & Engineering),Amravati University, Amravati,2002, Completed Ph. D. Computer Science & Engineering, S G B Amravati University, Amravati,2017, research domain – specialization and expertise in Distributed and Cloud Computing, Cryptography and System Security, IPR – Combinatorial Method For Security Cloud, Published papers titled 'Efficient homomorphic encryption using ECC-ElGamal scheme for cloud data' in IET, 2016, Intelligent Transparent Encryption-Decryption as Security-as-a-Service from clouds in IEEE, 2016.