Data security and Confidentiality in Cloud system

[1]Mr. Samiran Maity, [2]Mrs. Kavita Shirsat

[1]Student, [2]Associate Professor
Department of CSE
Vidyalankar institute of Technology, Mumbai, Maharshtra

Abstract**: The present era is said to be an era of information and the period of digitization. The digital information is generated in terabytes daily through various sources like smart phones, social networks, sensors, user generated content. This digitization has raised several issues with respect to data storage on cloud. In the future era of Internet, this explosion of raw data and dependence on data services will grow by four-fold due to storage proliferation of data intensive services and the digital convergence of telecommunication, media and Information Communication Technology (ICT). The next generation data models for storage delivery would migrate to cloud-based infrastructure for storage which will be based on data objects with rich, extensible metadata and elaborated access methods. Such infrastructures will face several research challenges which need to be addressed in order to overcome limitations related to issues like storage access, mobility, cost, energy, security, interoperability, efficiency, etc. The major issue being, data storage security on the cloud**
Encryption is the process of translating plain text data into something that appears to be random and meaningless, Decryption is the process of converting ciphertext back to plaintext.
To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.
The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.

It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

1. INTRODUCTION

Software versus hardware-based mechanisms for protecting data

Software-based security solutions encrypt the data to protect it from theft. However, a malicious program or a hacker could corrupt the data in order to make it unrecoverable, making the system unusable. Hardware- based security solutions can prevent read and write access to data, hence offering very strong protection against tampering and unauthorized access.

Hardware based security or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS#11 may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered (see two-factor authentication). However, dongles can be used by anyone who can gain physical access to it. Newer technologies in hardware-based security solves this problem offering full proof security for data.[citation needed]
Working of hardware-based security: A hardware device allows a user to log in, log out and set different levels through manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as hard disks. Illegal access by a malicious user or a malicious program is interrupted based on the current state of a user by hard disk and DVD controllers making illegal access to data impossible. Hardware-based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on hard disks can be corrupted after a malicious access is obtained. With hardware-based protection, software cannot manipulate the user privilege levels. It is impossible for a hacker or a malicious program to gain access to secure data protected by hardware or perform unauthorized privileged operations. This assumption is broken only if the hardware itself is malicious or contains a backdoor.[3] The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware-based security and secure system administration policies.

2. LITERATURE SURVEY

Concealing the User Identity in Cloud Services:

Cloud computing is a way of providing facility to the users according to their requirements and it also has the ability to fulfil the user’s required necessities. Cloud computation service may have to direct towards three of the most important security related risks which are integrity of user, the confidential needs of a user and the availability of the user needs. In this paper, a proposition is suggested for the user’s management of his/her identification and it’s required protocols along with the question of anything extra that we can do for these already existing protocols, which may be currently engaged for the cloud computation. The integration of confidentiality with the availability of the focused web based services can be said to be the important apprehensions. The newly trending two factor based identity authentication method and technologies that surround the encryption structure may be considered favorable in order to conceal one’s identification in cloud computation amenity

The Method of Ensuring Confidentiality and Integrity Data in Cloud computing:

Cloud computing allows not only to obtain computing resources on- demand but also to store large amounts of data (big data) with a high level of fault tolerance. Nevertheless, data confidentiality for users of hybrid and public clouds is cannot guaranteed in full. Cloud providers have full access to user data, which threatens to compromise the integrity of data. Existing methods of providing security consider methods to increase the speed and reduce the load during authorization and data encryption. The paper proposes a method that describes the use of separate services outside the cloud for authentication, data management and metadata storage to eliminate the possibility of obtaining unauthorized access to data, and the use of metadata to perform integrity control. The developed method is being used to create a stand based on Open Stack and two services on separate servers. The owner of the database limits the access to data that is stored in an encrypted form and does not allow provider to interact with database.

Performance Evaluation of Hybrid Cryptography System:

The spectacular growth of the Internet has make an increased awareness of an interest in security issues. Although Security is measure concern over internet, many applications have been developed and designed without considering main objectives of information security that is confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the importance of an understanding of such security issues will also increase. Cryptography plays important role in secure data communication. First Phase of this paper presents the development of Hybrid Cryptography system which contains Chaffing & Winnowing Algorithm, Diffie-Hellman Key Exchange Algorithm and Advanced Encryption Standard (AES) algorithm and second phase of the paper shows the performance evaluation of AES, Chaffing &Winnowing, Diffie Hellman Key Exchange Algorithm and Hybrid Lastly, Server response generation can be broken down into two categories:

Cryptographic Algorithms. Cryptography algorithms provide a secure data communication over the internet and play key role in any security system. In this paper, different experiments have been conducted to compare these algorithms in term of encryption time, decryption time and throughput over variable concurrency for fixed time and Brute Force attack resistance capability among all algorithm

Performance Evaluation of Hybrid Cryptography System:

The spectacular growth of the Internet has make an increased awareness of an interest in security issues. Although Security is measure concern over internet, many applications have been developed and designed without considering main objectives of information security that is confidentiality, authentication, and privacy. As our daily activities become more and more reliant upon data networks, the importance of an understanding of such security issues will also increase. Cryptography plays important role in secure data communication. First Phase of this paper presents the development of Hybrid Cryptography system which contains Chaffing & Winnowing Algorithm, Diffie-Hellman Key Exchange Algorithm and Advanced Encryption Standard (AES) algorithm and second phase of the paper shows the performance evaluation of AES, Chaffing &Winnowing, Diffie Hellman Key Exchange Algorithm and Hybrid Lastly, Server response generation can be broken down into two categories:

Cryptographic Algorithms. Cryptography algorithms provide a secure data communication over the internet and play key role in any security system. In this paper, different experiments have been conducted to compare these algorithms in term of encryption time, decryption time and throughput over variable concurrency for fixed time and Brute Force attack resistance capability among all algorithm

An Advance Cryptographic Solutions in Cloud Computing Security:

Cryptographically cloud computing may be an innovative safe cloud computing design. Cloud computing may be a huge size dispersed computing model that ambitious by the economy of the level. It integrates a group of inattentive virtualized animatedly scalable and managed possessions like computing control storage space platform and services. External end users will approach to resources over the net victimization fatal particularly mobile terminals, Cloud’s architecture structures are advances in on-demand new trends. That are the belongings are animatedly assigned to a user per his request and hand over when the task is finished. So, this paper projected biometric coding to boost the confidentiality in Cloud computing for biometric knowledge. Also, this paper mentioned virtualization for Cloud computing also as statistics coding. Indeed, this paper overviewed the safety weaknesses of Cloud computing and theway biometric coding will improve the confidentiality in Cloud computing atmosphere. Excluding this confidentiality is increased in Cloud computing by victimization biometric coding for biometric knowledge. The novel approach of biometric coding is to reinforce the biometric knowledge confidentiality in Cloud computing. Implementation of identification mechanism can take the security of information and access management in the cloud to a higher level. This section discusses, however, a projected statistics system with relation to alternative recognition systems to date is a lot of advantageous and result oriented as a result of it does not work on presumptions: it's distinctive and provides quick and contact less authentication. Thus, this paper reviews the new discipline techniques accustomed to defend methodology encrypted info in passing remote cloud storage.

A Study on Data Security and Query privacy in Cloud:

A lot of organizations need effective resolutions to record and evaluate the existing enormous volume of information. Cloud computing as a facilitator offers scalable resources and noteworthy economic assistances as the decreased operational expenditures. This model increases a wide set of security and privacy problems that have to be taken into reflexion. Multi-occupancy, loss of control, and confidence are the key issues in cloud computing situations. This paper considers the present know-hows and a comprehensive assortment of both previous and high-tech tasks on cloud security and confidentiality. The paradigm shift that supplements the usage of cloud computing is progressively enabling augmentation to safety and privacy contemplations linked with the different facades of cloud computing like multi -tenancy, reliance, loss of control and responsibility. So, cloud platforms that deal with big data that have sensitive information are necessary to use technical methods and structural precautions to circumvent data defense failures that might lead to vast and costly harms.

SECURING DATA IN A CLOUD USING AES:

Cloud computing is the new key for the growth of IT Services in the next generation This services are provided to a customer over a network and these services are delivered to the customers by a third party which who owns the infrastructure. The data of the customer is stored in remote sector. Cloud computing provides not only hosting but also storage service on the Internet. Cloud computing is cost effective and location independent when sharing is done on a larger scale. Cloud is classified into three types based on their usage. The three types of cloud are private cloud, public cloud and hybrid cloud. The cloud which is owned by a single organization is known as private cloud. Public clouds are not owned by a single organization and are shared on a large scale. Hybrid cloud is said to be combination of both Private cloud and Public Cloud which is mostly used in the industries. Private cloud provides more flexibility and better control. It provide three levels of "as a service" over the Internet (1) Infrastructure as a Service (IaaS), (2) Platform as a Service (PaaS), (3) software as a service (SaaS). Infrastructure convergence concept is used in development of cloud computing. Cloud computing can be used in all the devices which can be connected to the internet. All the data can be stored in a single location. Hence any extra memory space is not required at our side. The advantages of cloud computing are many and it is very appealing but there are few drawbacks which it needs to tackle. Cloud computing had to face issues in regards to data security. Leakage of critical data of the customers such as bank details, personal information is very harmful. Privacy, Data theft and Data loss are the major issue which cloud computing faces. Security services are provided by cryptography. It concerns with confidentiality, integrity, and authentication. Security is one of the principal challenges of resource sharing on data communication network. The issue of data security becomes critical when data is been shared by two or more computer connected in a same network.

A Review: A Survey on Privacy Preserving for Secure Cloud Storage:

Cloud computing technology provides millions of on demand services to its users on internet ranging from infrastructure, software to storage as a service on cloud. Storage service allows its users to outsource large amount of data without directly controlling it and cloud running on the principle of virtually shared servers do not provide users with the storage location. Therefore, various measures can be adopted for maintaining data integrity, security while entering data in cloud. So here, we are having open audit-ability for distributed storage that shoppers will rely on an outsider examiner (TPA) to test the trait of knowledge. This paper offers the problems known with security whereas golf shot away the client's data to the distributed storage amid the examining. During this paper we'll examine totally different systems to fathom these problems to present protection and security of cloud data. There’s lots of analysis being created to identify problems associated CSPs and security.

Achieving Cloud Security Using Hybrid Cryptography Algorithm:

Clouds are large pools of easily usable and accessible virtualized resources.These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing optimum resource utilization. Cloud Computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services concentrate on security issue. In this paper using SHA- 512 and MAES hybrid algorithm using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using Modify advanced encryption standard, so data is successfully and securely stored on cloud. Proposed system is highly efficient against malicious data an provide high security and higher execution time.

Cloud based Cyber Physical Systems Security Issues - A Survey

Data processing and physical interaction are combined by cyber physical systems (CPSs). CPSs have limited computation and storage capabilities due to their small size and resource constraints. With the emergence of cloud computing there are several new opportunities for these CPSs to extend their capabilities by taking advantage of the cloud resources in different ways. Cloud based cyber physical system (CCPS) is the integration of cloud computing technology with CPSs where complex computations can be transferred to the cloud platform. This paper presents a survey of research done on cloud based cyber physical systems security issues.

Emerging Cyber Security Threats inOrganization:

Cyber-security is a preventive preparation of protecting sensitive information, information systems, computers, servers, critical infrastructure, mobile devices, and computer networks from unauthorized access or hackers. Now a day digital technology takes the most significant role in growth effectiveness and efficiency in the organization. However, new technologies like mobile technologies (5G), IoT and cloud computing are Coming with new information security threats. Employees still using the old software, they didn’t update the software (operating system), they use a permanent password, they are still using weak and default password (Wife name or her phone number) information security literacy and behavior end users or IT staff. They don’t have awareness about proactive cyber-attacks prevention policies and procedures. Because they have not took short and long term training on most serious cyber-attacks like ransom ware, social engineering, malware, DDoS, and phishing. This article attempts to assess or explore the most common and emerging cyber security threats. That the organizations facing. An in-depth literature review is delivered. The main objective of this article is to create awareness about the emerging and the most serious cyber-attacks occurring in the organization. The findings demonstrate that cyber security preparations and trained employees are very low; hackers becoming more sophisticated.

3. DATA SECURITY

- **Backups**

Backups are used to ensure data which is lost can be recovered from another source. It is considered essential to keep a backup of any data in most industries and the process is recommended for any files of importance to a user.

- **Data masking**

Data masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel.[5] This may include masking the data from users (for example so banking customer representatives can only see the last 4 digits of a customer's national identity number), developers (who need real production data to test new software releases but should not be able to see sensitive financial data), outsourcing vendors, etc.

- **Data erasure**

Data erasure is a method of software-based overwriting that completely wipes all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is lost when an asset is retired or reused.

4. EXISTING SYSTEM

Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. Database security is a specialist topic within the broader realms of computer security, information security and risk management.
Security risks to database systems include, for example:

[1] Unauthorized or unintended activity or misuse by authorized database users, database administrators, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations);
[2] Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services;
[3] Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use databases as intended;
[4] Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence;
[5] Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized privilege escalation), data loss/corruption, performance degradation etc.;
[6] Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage

5. PROBLEM DEFINITION

The reason for the massive surge in attacks is slightly more complicated. Ultimately, the problem stems from the historical design of networking. Once upon a time, in the dark ages of the 1980's and 1990's, networking was hard. There were a number of network products and options. Interoperability between networks, even those using the same core technologies, was difficult. The concept of Network Engineers arose, and in reality it did require quite a bit of engineering education and experience.
Networks were designed using the castle model. The electronic ends of the network (i.e. your domain) represent the castle walls. Firewalls, malware detectors and intrusion detectors are the guarded gates toyour domain. Initially those technologies worked well. However, those technologies are all based on the fact that they can recognize an attack, and recognition comes in the form of previous exposure. That was fine when attacks were limited to specific and repeated methods. But hacking is now big business. Where attacks were once the playground for amateurs, today's hackers are far more sophisticated. Not only are attacks often unique against their targets, most often attacks utilize the domain administrators' credentials.
Domain administrators are the resident superpowers. They have full access to everything including the security systems. Unfortunately, when those domain administrator credentials are hacked, stolen or socially engineeredaway from their owners, the hacker gains unrestricted access to everything. Security systems can be turned on and off. Rules can be put in place that create unmonitored back doors. Log files can be edited and any 'footprints' easily erased. Historically, the most common way to detect one of these types of attacks is for a domain administrator to notice that their (or a colleagues) credentials are being used to spawn jobs that they don't recall starting. Once suspicions are aroused, it's often quite simple to trace the attack history retroactively through a number of log files and other forensic methods. However, in far too many cases, the attack isn't discovered until the hacker has made it public.

6. PROPOSED SYSTEM

In this project, we aim to design secured system, which will demonstrate use of hacking technique to know how data is hacked, in which we will encrypt user data in such a way that even after used/hacked data will not lose its value in terms of usability, as we will encrypt our user's data and store in files, consider a case in which user registers on our website or server. Its data will be stored in encrypted format which will be provide a layer of security and it will keep our data safe even after encryption.
As illustrated in flow, data will be in encrypted format while saving and while fetching it will be decrypted, but when someone tries to download it without access it will be sent in encrypted format only

DATA FLOW

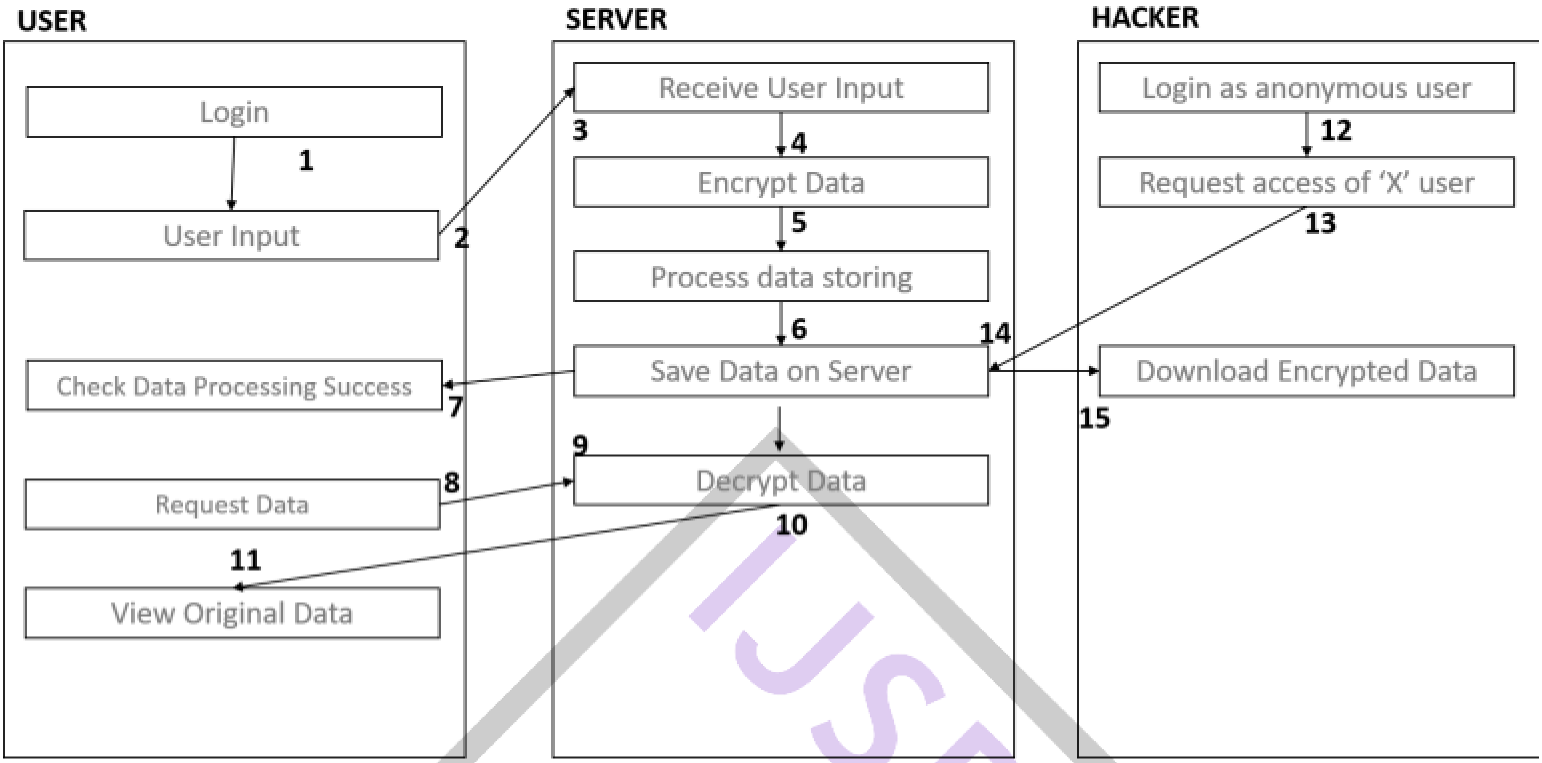

Fig 1.1

7. SYSTEM FLOW

Proposed System Architecture:

This system will be used for storing and accessing data without any data loss, if any data is lost during transmission or stolen from database, it will be completely useless as it will be encrypted and cannot be future processed for any valid meaning without proper decoding or decryption set.

Steps for storing values are :

user need to login in to system where its user id/name and password will be taken as plain text and server will be loaded with algorithms to encrypt password and compare with existing encoded password if both passwords are matched user will be granted access to enter data.

User will then add data (as shown in fig 2.1)

SYSTEM ARCHITECTURE

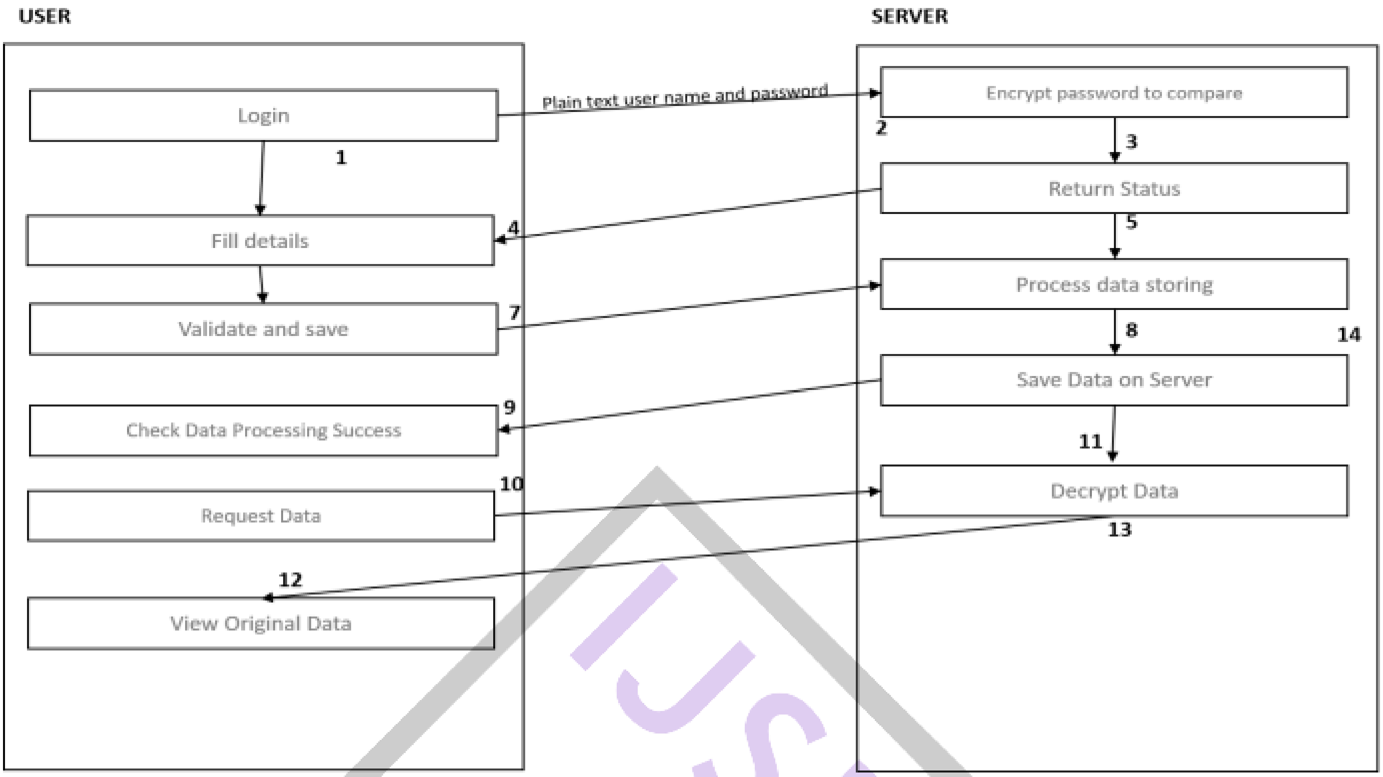

Fig 2.1 User will fill details and save on server (Fig 2.1 step 4)

This data will be validated for some regular expressions such as email must have @ and for FQN (fully qualified names) and hence for data integrity validation must be done before data is store on server Once data is validated and it is ready to process data will be sent on sever for further processing (Step 7,fig 2.1)

Server will then encrypt data and store it on cloud for future request and modifications. Consider user request data (step 10, fig 2.1)

User now has requested for access of data in plain text or original and decrypted form. For this user have to send access request which will be received on sever (step 11,fig 2.1)

System will now decrypted data as user has been authenticated and verified for its ownership this decrypted data will be sent to user for modification and re-encryption iteration will be started again

Hacker System Architecture:

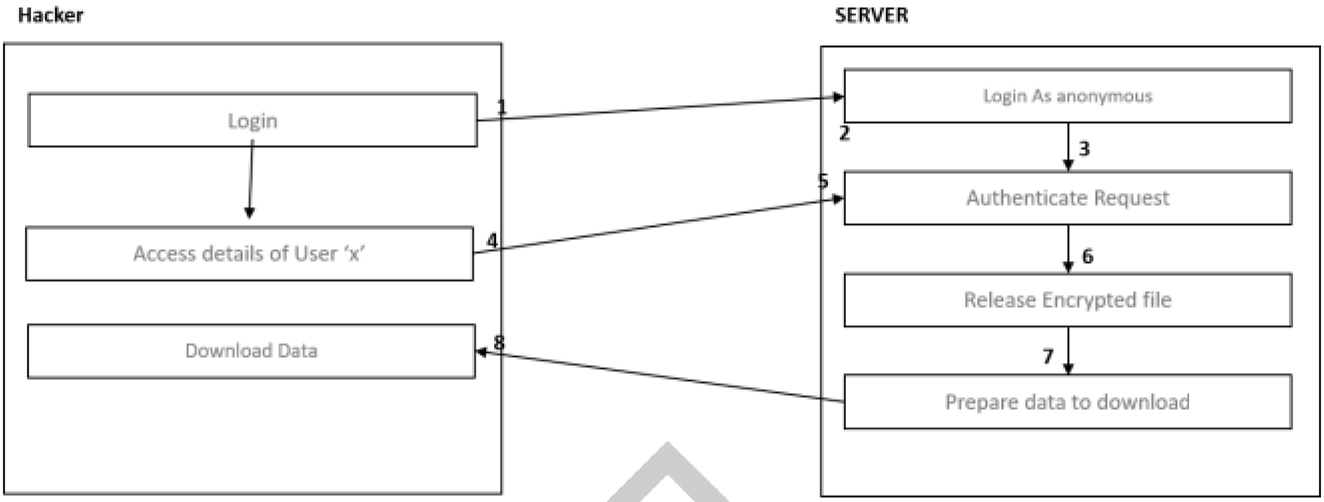

Fig 2.2

System Flowchart (Storing/ Encoding Phase):

In this, user will upload data which will be raw chunk, this raw data cannot be stored as it is without encryption as explain in problem statement, data could be modified without owner's permission, to avoid that data entered by user will be processed and encrypted (as shown in step 5 fig 1.1), once processing is completed user will be notified for data processing status.

Let us understand how data will be decrypted.

Authenticating user process will be same as it was while adding data, user will request data from server which will re-authenticated user for its validity. once user is verified, system will start decrypting file to its original form (plain text) this plain text will be sent to user (step 12 fig 2.1)

System Flowchart (Accessing /Decoding Phase):

In this phase, we believe data will be accessed by some unethical hacker tep 4 fig 2.2) who is not knowing data stored in database is encrypted (fig 2.2) and that person will get data, which will be of no user at will not be decrypted without system algorithms, accessing proper data with decoded will require authenticated user with our system which will verify user and display proper data.

8. SUMMARY

Encryption can help protect data you send, receive, and store, using a device. That can include text messages stored on your smartphone, running logs saved on your fitness watch, and banking information sent through your online account.
Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.
Vast amounts of personal information are managed online and stored in the cloud or on servers with an ongoing connection to the web. It's nearly impossible to do business of any kind without your personal data ending up in an organization's networked computer system, which is why it's important to know how to help keep that data private.

Encryption plays an essential role.

Internet privacy concerns are real
Encryption helps protect your online privacy by turning personal information into "for your eyes only" messages intended only for the parties that need them — and no one else.
You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.
Most email clients come with the option for encryption in their Settings menu, and if you check your email with a web browser, take a moment to ensure that SSL encryption is available.

Hacking is big business

Cybercrime is a global business, often run by multinational outfits.
Many of the large-scale data breaches that you may have heard about in the news demonstrate that cybercriminals are often out to steal personal information for financial gain.

Regulations demand it
The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers to implement security features that help protect patients' sensitive health information online.

REFERENCES

[1] Akanksha Sharma, Dr. Sandeep Mathur, “Concealing the User Identity in Cloud Services” 978-1- 7281-0167- 5/19/$31.00 ©2019 IEEE.

[2] Andrey N. Rukavitsyn, Konstantin A. Borisenko, Ivan I. Holod, Andrey V. Shorov, “The Method of Ensuring Confidentiality and Integrity Data in Cloud Computing:” 978-1-5386-1810-3/17/$31.00 ©2017 IEEE.

[3] Er. Parvin Shaikh, Dr. Sonali Patil, “Performance Evaluation of Hybrid Cryptography System”, International Journal of Engineering Trends and Technology (IJETT) – Volume54 Number 4 -December2017.

[4] Zain Ul Abedin, Zhitao Guan, Asad Ullah Arif and Usman Anwar, “An Advance Cryptographic Solutions in Cloud Computing Security”,978- 1-5386-9509-8/19/$31.00 ©2019 IEEE.

[5] Nagababu Garigipati, Nagababu Garigipati,” A Study on Data Security and Query privacy in Cloud”, 978-1- 5386-9439-8/19/$31.00 ©2019 IEEE

[6] Prof. Mahesh Panjwani, Abhijeet Satpute, Adarsh Kamble , Ninad Ukey, Vaibhav Makde, Yogesh Mehere, “SECURING DATA IN A CLOUD USING AES”, © 2020 IJRAR February 2020, Volume 7, Issue 1.

[7] Areeba Kazim, Ritika Varshney,” A Review: A Survey on Privacy Preserving for Secure Cloud Storage”, International Journal of Computer Applications (0975 – 8887) Volume 177 – No. 13, October 2019.

[8] Tripathi Jyoti, Prof. Gayatri Pandi, “Achieving Cloud Security Using Hybrid Cryptography Algorithm”, IJARIIE-ISSN(O)-2395-4396 Vol- 3 Issue-5 2017.

[9] Yogita Borse, Mohammed Saleh Shaikh, “Cloud based Cyber Physical Systems Security Issues - A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 177 – No. 9, October 2019.

[10] Hailye Tekleselase Woldemichael, “Emerging Cyber Security Threats in Organization”, Volume-7, Issue-6, December 2019 Research Paper,Published:31/Dec/2019.