International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

Significant Permission Identification for Android Malware Detection

Monisha R[1], Mr.E.Sivarajan[2]
[1]M.E, Department of Computer science and engineering, Sri Shanmugha College of Engineering and Technology, Sankari, Salem, Tamilnadu
[2]Assistant Professor, Department of Computer Science and Engineering, Sri Shanmugha College of Engineering and Technology, Sankari, Salem, Tamilnadu

ABSTRACT
With the rapid development of cloud computing, more cloud services are into our daily life, and thus security protection of cloud services, especially data privacy protection, becomes more important. However to perform privacy protection causes huge overhead. Thus it is a critical issue to perform the most suitable protection to decline performance consumption while provide privacy protection. In this project, the Proficient Privacy Protection Scheme (PPPS) is proposed to provide the appropriate privacy protection which is satisfying the user-demand privacy requirement and maintaining system performance simultaneously. At first, the privacy level is analyzed by users those require and quantify security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data.Finally, the simulation results show that the PPPS not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments. The application is designed using Microsoft Visual Studio .Net 2005 as front end. The coding language used is Visual C# .Net. MS-SQL Server 2000 is used as back end database.

1. INTRODUCTION

Cloud computing is emerging as the most suitable paradigm for individuals and organizations to access inexpensive, scalable, ubiquitous, and on- demand computing resources, applications, and data storage services. Cloud storage systems, such as Dropbox, Google Drive, Apple's iCloud, Microsoft OneDrive, etc., enable users to remotely store a large volume of data that can be accessed and shared among users, regardless of time and location constraints. With the growing popularity of cloud computing, the number of enterprises and individuals shifting toward the use of cloud has increased rapidly.As a result, a vast amount of important personal information and critical organization data, such as personal health records, government documents, and company finance data, etc., are transmitted across the Internet and stored in cloud servers. However, outsourcing sensitive data suffers from critical security threats, privacy, and access control problems. These are common concerns of organizations and individuals using cloud services. When data owners migrate their sensitive data to the cloud, they lose an element of control over their data. Cloud users have no guarantee about the way these sensitive data will be treated and protected by cloud providers. Although the cloud provides users with the convenience of data access across multiple devices, by using cloud services, user data are vulnerable to a verity of malicious attacks and threats. Security incidents occur frequently. Even worse, cloud service provider may leak user data to unauthorized entities for illegal profit.One feasible solution to overcome these problems is to use cryptography. All sensitive data have to be encrypted by data owners prior to storing them into the potentially untrustworthy cloud. The strength of the encryption scheme is largely dependent on the strength of the key management technique used. The security of the encryption scheme lies on the secrecy of the keys that are known only to the users authorized to read their respective data, and not only on the secrecy of the encryption algorithm used. Given the amount of data being stored and shared in cloud and the 5 increasing number of data users, designing a cryptographic scheme for cloud storage that meets the requirements of security, efficiency, ease of use, and flexibility is a challenging task. Traditional encryption applications, generally, suffer from limited usability due to the manual solution provided by applications. Data owners must encrypt their data manually prior to uploading to the cloud. Moreover, users have to manually generate,

DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

manage, and store the encryption keys.However, the involvement of data owners in performing multiple encryption and decryption operations is cumbersome and time consuming. Also, it is difficult for users to manage more than a few keys, and if the keys are leaked or otherwise compromised, security will be threatened. Encryption applications are designed to be bandwidth-hungry and latency-sensitive, in which the increased number of outsourced files requiring encryption would significantly affect the system performance and data access response time. Recent works cope with the limitations of the encryption applications by adopting a transparent encryption approach. This type of encryption mechanism isimplemented most effectively with the help of operating system file systems. The common approach is composed of a client application that interacts with the local cryptographic file system, and the encrypted data are synchronized or backup to connected back-end cloud storage servers. In this project, In this scenario, the levels can be seen as the kinds of speed, hybrid, and security.
They are explained as follows.

- Privacy Level 1 (Speed): The requirement of this level presents that no sensitive information in the data. Users want to use the weak encryption composition to obtain more performance for using cloud services.
- Privacy Level 2 (Hybrid): The requirement of this level presents that data include some sensitive information. The data requires weak encryption for partial data (such as address, mail id of corporates') and strong encryption for remaining data (such as account balances and other secure information).
- Privacy Level 3 (Security): In this privacy level, the data contains most important information. In order to protect the data security, more privileged users view most of the data and less privileged users view limited data.

Objectives

- To encrypt/decrypt the data of less importance using weak encryption method so that communication is fast.
- To encrypt/decrypt the partial data using weak encryption method and other partial data in strong encryption method so that communication is fast and security level is raised.
- To encrypt/decrypt the some fields using strong encryption method and some other fields using weak encryption method so that all fields are displayed to high privilege users and some fields are displayed to low privileged users.
- To encrypt/decrypt the watermarked contents with weak encryption method and non-watermarked contents with strong encryption method.

2. LITERATURE SURVEY

In this paper [1], the authors stated that the increasing volume of personal and sensitive data being harvested by data controllers makes it increasingly necessary to use the cloud not just to store the data, but also to process them on cloud premises. However, security concerns on frequent data breaches, together with recently upgraded legal data protection requirements (like the European Union's General Data Protection Regulation), advise against outsourcing unprotected sensitive data to public clouds.

To tackle this issue, this survey covers technologies that allow privacy aware outsourcing of storage and processing of sensitive data to public clouds. Specifically and as a novelty, they reviewed masking methods for outsourced data based on data splitting and anonymization, in addition to cryptographic methods covered in other surveys. They then compared these methods in terms of operations supported on the masked outsourced data, overhead, accuracy preservation, and impact on data management. Furthermore, they listed several research projects and available products that have materialized some of the surveyed solutions. Finally, they identified outstanding research challenges.

Many companies are outsourcing at least some of their information technology to the cloud, from mere data storage to e-mail and other productivity applications. Reduced costs, no need for maintenance, virtually unlimited computational resources and increased availability are the main forces driving this change. Yet,

security and privacy misgivings are still cardinal barriers hindering a franker migration to the cloud.

Security is defined as achieving confidentiality, integrity and availability of the data outsourced to the cloud. Users want to be assured that no intruder can hack the cloud and/or impersonate them to steal or alter their sensitive data, and that no denial of service will occur. In the E.U., 57% of large enterprises using the cloud reported the risk of a security breach as the main limiting factor in the use of cloud computing services [4]; in a survey by the cloud Security Alliance to over 165 information technology and security professionals in the U.S., most of the respondents considered cloud storage as high risk [5]; the European Network and Information Security Agency identified "loss of governance" over the data outsourced to the cloud as a critically deterring factor[6].

Security breaches are, in fact, very real threats. Some well-known examples include the Sony PlayStation Network outage 1 as a result of an external in-trusion, in which personal details from approximately 77 million accounts were stolen, the multi-day outage in Dropbox 2 that temporarily allowed visitors to log into any of its 25 million customer accounts as a result of a misconfiguration, or the leakage of private pictures of a number of celebrities from the Apple iCloud storage service due to weakly protected login 8 credentials[6].

Regarding privacy, its most widely accepted definition in the information society is in terms of informational self-determination, that is, "the claim of individuals, groups or institutions to determine for themselves when, how,and to what extent information about them is communicated to others" [7].

Hence, for a cloud user to store and/or process sensitive data in the cloud,she needs the guarantee that no one other than herself not even the CSP will be able to see or infer her data. Thus, cloud computing needs to increase the user's control on her data, which will decrease the need for users blindly trusting the CSP. Otherwise, a user might be reluctant to outsource sensitive data to the cloud.

Furthermore, when data are personal, the individuals to whom refer subjects— have privacy rights that have recently been enshrined in the new European Union's General Data Protection Regulation (GDPR4). To stay GDPR- compliant, a controller an entity that has obtained consent from subjects to collect,
store and process their data can only outsource subject data to the cloud if she can obtain full control and confidentiality for the outsourced data. The above is a relevant issue because GDPR is also becoming a de facto legal standard outside the European Union, specifically in the USA, Australia, Canada and Japan, and any company wishing to sell information technology solutions to those markets must take it into account. Notice that privacy is even more challenging than security, because it must hold also with respect to (public and, therefore, untrusted) CSPs.

In this respect, the cloud has given CSPs the opportunity to analyze and exploit large amounts of personal data. In fact, a report by the U.S. Federal Trade Commission [5] states that public CSPs regularly collect and analyze the data of their users without the latter's knowledge, and that those analyses could yield sensitive inferences; for example, a CSP could detect individuals that suffer from diabetes because of their interest in sugar-free products and share 9 this information with an insurance company that could use that clue to classify a person as higher- risk (and possibly higher-premium).

One might argue that sensitive data handling in the cloud would be much simpler if the CSP could be assumed to be trusted. However, there are several legal issues here. On the one hand, in many scenarios the data subjects entrust the data controller with their personal data (for example, healthcare data), but this does not mean they allow the controller to further transfer their data to whomever the controller chooses to trust. On the other hand, the CSP may be under a jurisdiction different from the controller's. If, say, the CSP is under U.S. law whereas controller and subjects are under E.U. law, the latter law may be violated.
Finally, many public CSPs offer their services free of charge in return for the possibility of monetizing users' data. For example, a recent privacy policy in Google [8] specifies that whatever information a user decides to

DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

outsource to any Google service can be used, reproduced, modified or distributed by Google with the aim of improving or promoting its services, but also to conduct targeted advertising (e.g., the Gmail filtering system scans the content of our emails to serve personalized ads).

To assuage the above issues and restore the user's control and trust on the protection of the data outsourced to the cloud, several solutions have been proposed in recent years. All of them involve masking sensitive data so that only protected values are stored in the cloud and only the user/controller owning the data is able to unmask the protected values retrieved from the cloud.

However, if the user wants to use not only the cloud's storage but also the cloud's computational power, the challenge is even harder, because data protection should be made compatible with outsourced computations on cloud premises on masked data In this paper we survey the state of the art on security and privacy- enabling solutions towards the cloud, with a focus on those that preserve cloud service functionalities, such as the ability to outsource queries 10 and calculations on protected data to the cloud. In comparison with recent on the ours offers the following contributions:
Most surveys focus on data security vs external attackers [9-12] rather than on privacy versus the cloud. Therefore, they center their analysis on security attacks and on mechanisms to prevent, detect and mitigate them. In contrast, our survey considers mechanisms that protect outsourced data not only against third-party

3. METHODOLOGY

3.1 Problem Definition

The first step in the software development life cycle is the identification of the problem. As the success of the system depends largely on how accurately a problem is identified.
At present, all the data is encrypted/ decrypted with same encryption method, so that all data is given same importance and so existing system is less secure. There is no application with this feature to communicate securely as well as faster.
So, this project identifies that, if helps to solve the problem through the application. In addition, if the new system is able to provide security for text messages as well as image data, then the application can be used in various places where more security is required. The software used to solve the problem and develop the application in Microsoft Visual Studio .Net 2010 and MS SQL Server 2008.
With the rapid development of cloud computing, more cloud services are into our daily life, and thus security protection of cloud services, especially data privacy protection, becomes more important. However to perform privacy protection causes huge overhead. Thus it is a critical issue to perform the most suitable protection to decline performance consumption while provide privacy protection.
In this paper, the Proficient Privacy Protection Scheme (PPPS) is proposed to provide the appropriate privacy protection which is satisfying the user- demand privacy requirement and maintaining system performance simultaneously. At first, the privacy level is analyzed by users those require and quantify security degree and performance of encryption algorithms. Then, an appropriate security composition is derived by the results of analysis and quantified data.
Finally, the simulation results show that the PPPS not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments.The application is designed using Microsoft Visual Studio .Net 2005 as front end. The coding language used is Visual C# .Net. MS-SQL Server 2000 is used as back end database

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.2 Module Description

The following modules are present in the project.

i. MESSAGE SELECTION
ii. ENCRYPTION
SPEED HYBRID SECURITY
iii. DECRYPTION
SPEED HYBRID SECURITY

3.3 Data Flow Diagram

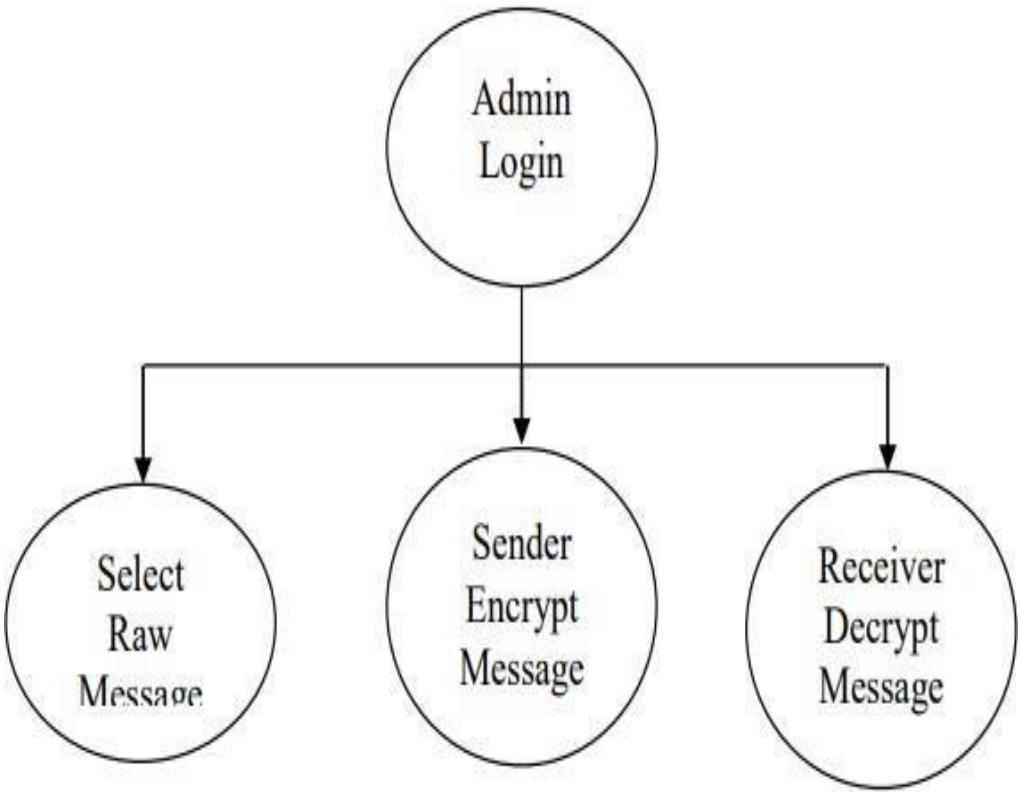


Fig :5 DATA FLOW DIAGRAM (LEVEL 0)

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.4 Encryption Module

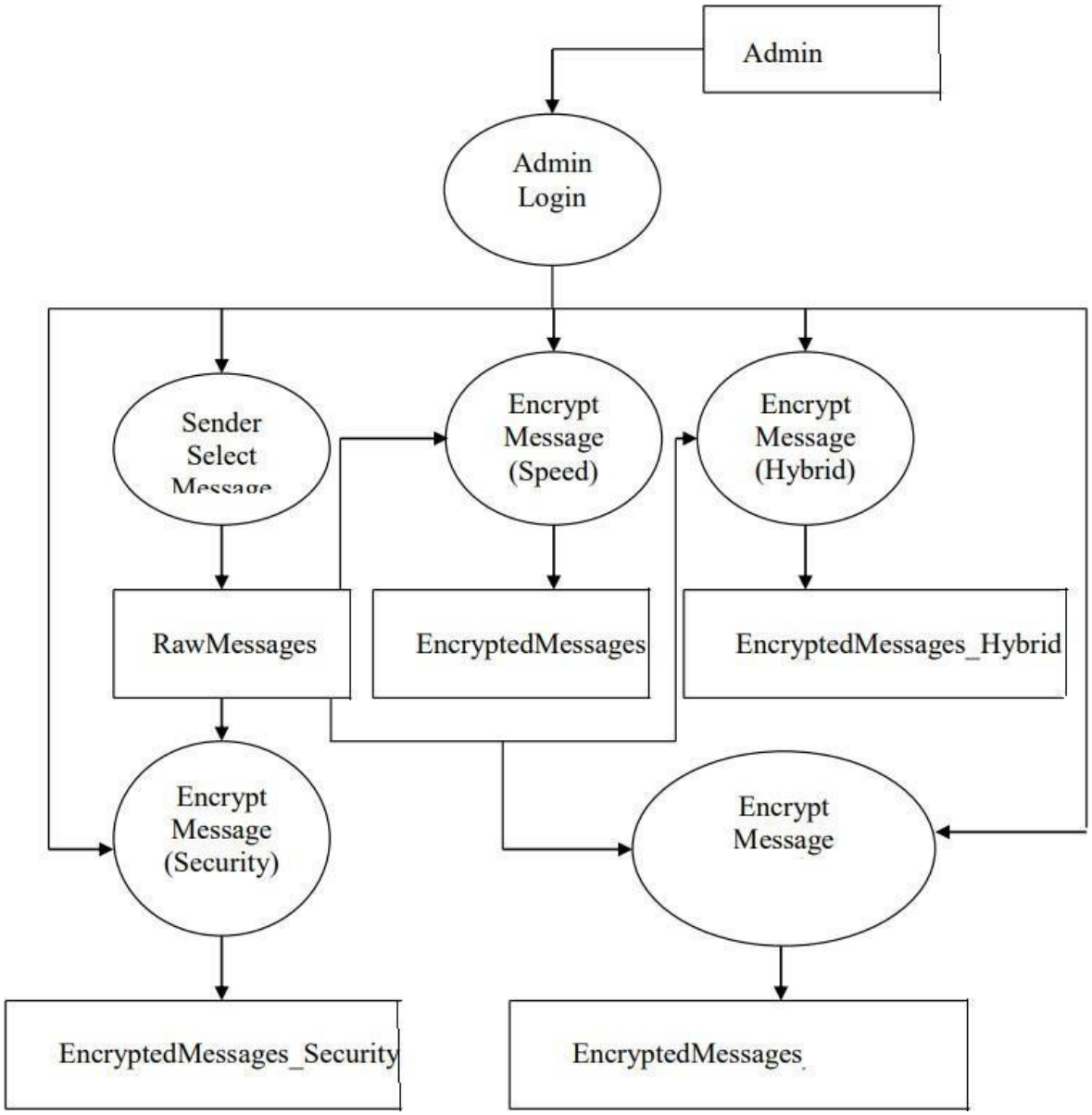


Fig :DATA FLOW DIAGRAM(LEVEL 1) ENCRYPTION MODULE

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.5 Decryption Module

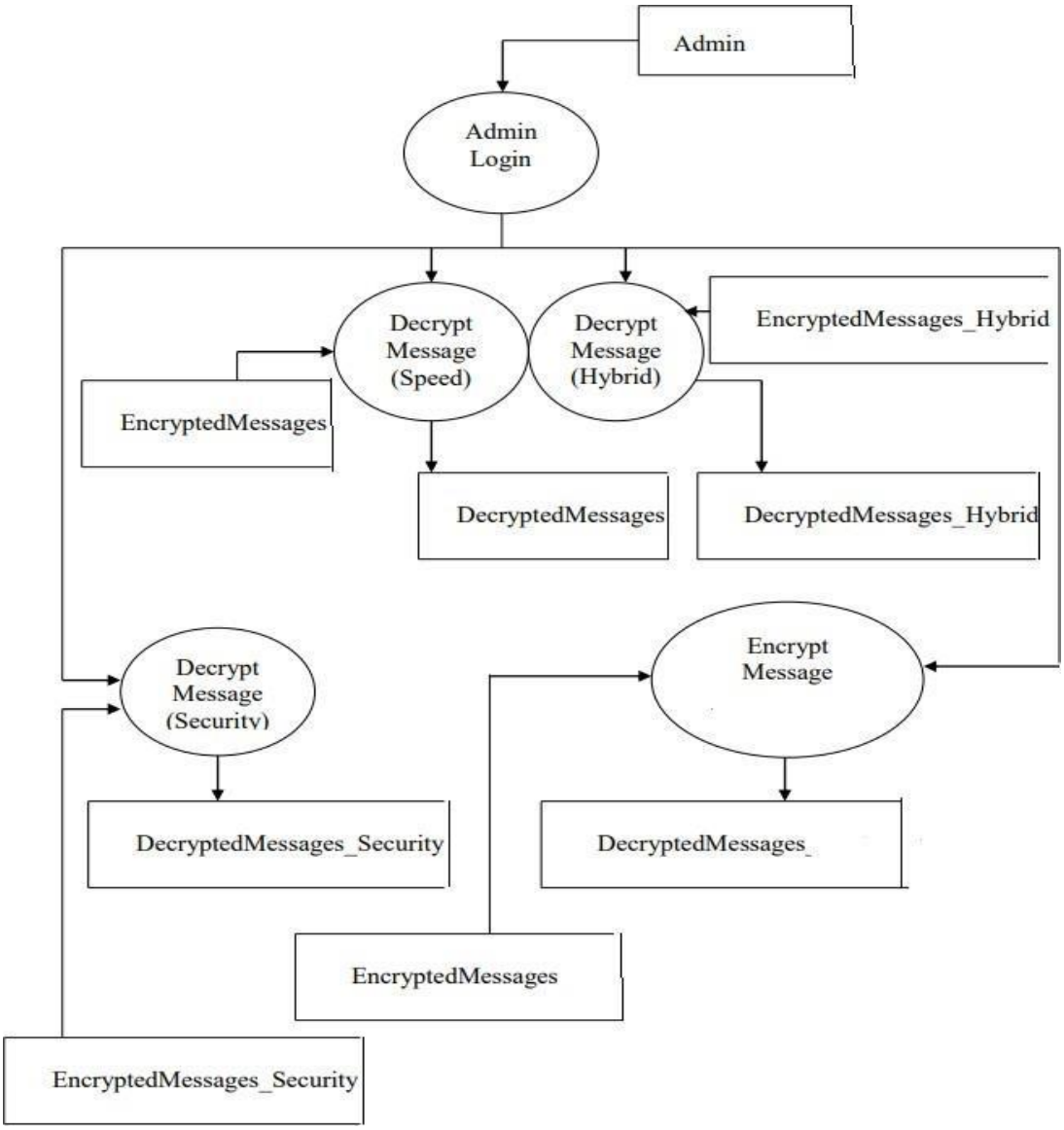


Fig :DATA FLOW DIAGRAM(LEVEL 1) DECRYPTION MODULE

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.6 View Encrypted Values

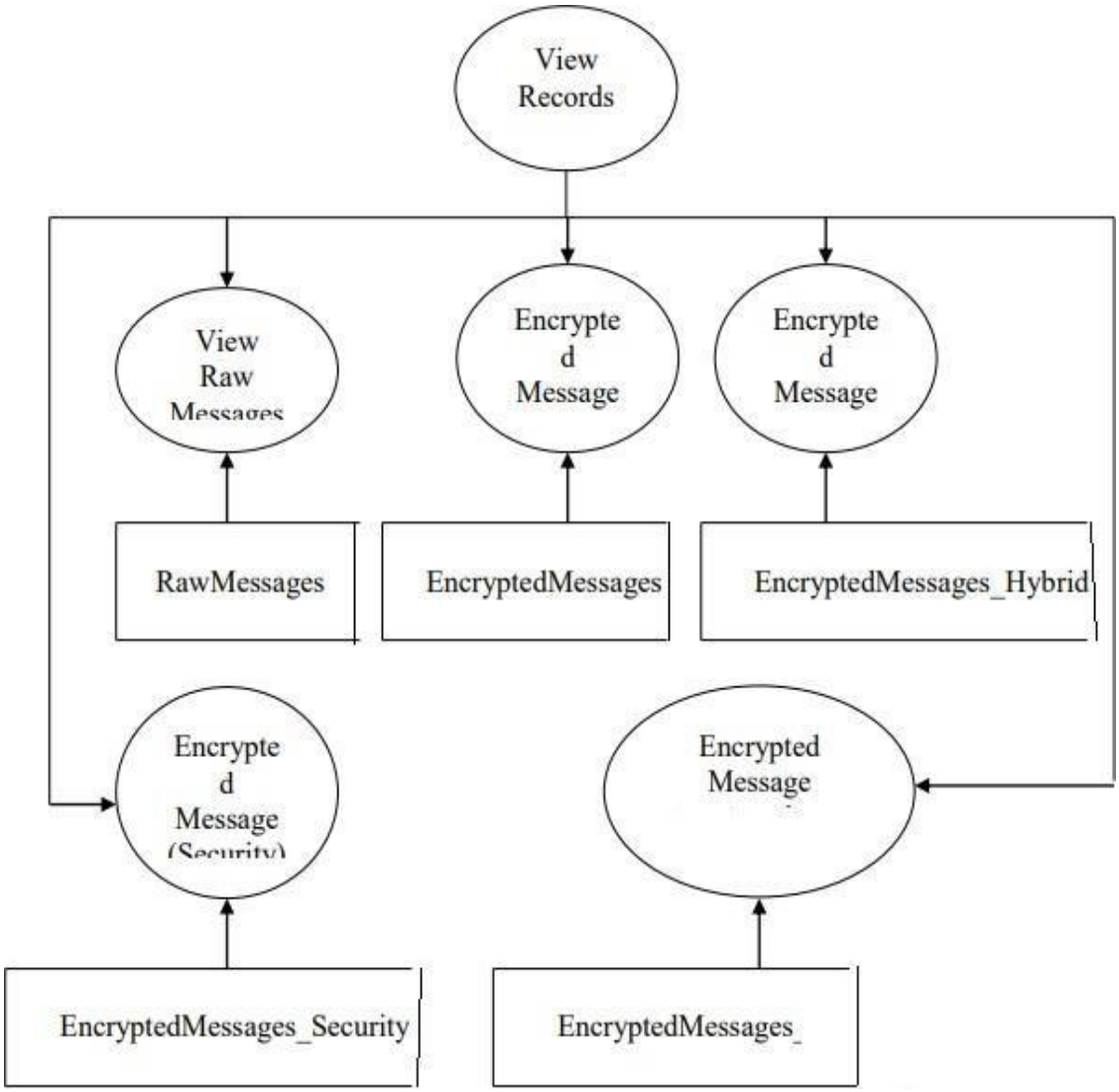


Fig : DATA FLOW DIAGRAM(LEVEL 1) VIEW ENCRYPTED VALUE

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.7 View Decrypted Values

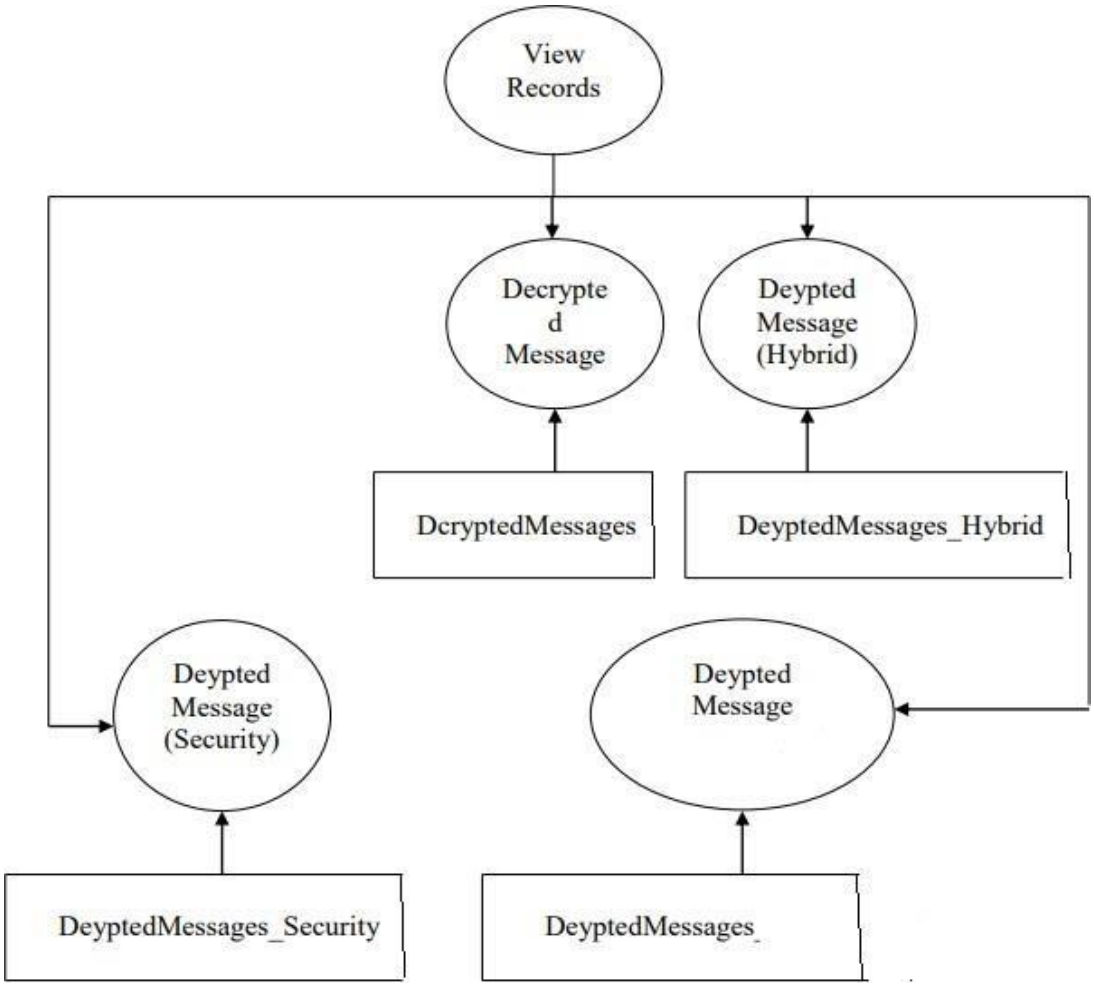
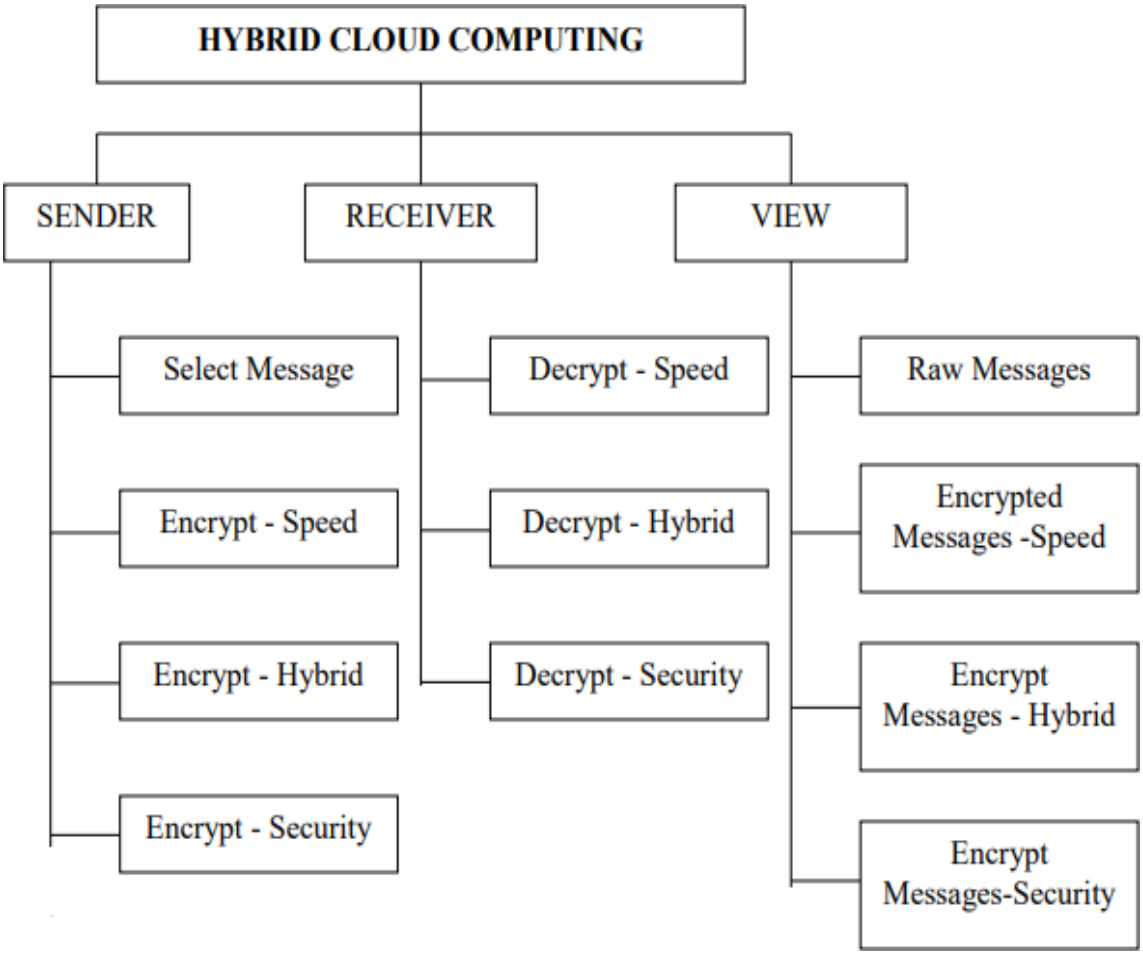


Fig : DATA FLOW DIAGRAM(LEVEL 1) VIEW DECRYPTED VALU

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.8 System Flow Diagram



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.9 Database Design Table Structure

3.9.1TABLE: ADMIN

FIELD NAME	TYPE	SIZE	DESCRIPTION
UserName	VARCHAR	15	Unique
Password	VARCHAR	15	

Unique: UserName
Purpose: This table is used to store the username and password to login to the application.

3.9.2Table: Rawmessages

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
MessageData	VARCHAR	3000	
FileName	VARCHAR	255	
EntryTime	DATETIME	8	

Primary Key: SNo
Purpose: This table is used to store the raw messages which are to be encrypted.

3.9.3Table: Encrypted Messages

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
RawMessageSNo	VARCHAR	3000	Foreign Key
EncryptedMessage	TEXT	-	
EntryTime	DATETIME	8	
Password	VARCHAR	15	

Primary Key: SNo
Purpose: This table is used to store the encrypted messages which are used in (Speed) Mode.

3.9.4Table: Encrypted Messages Hybrid

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
RawMessageSNo	VARCHAR	3000	Foreign Key

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

EncryptedMessage1	TEXT		
EncryptedMessage2	TEXT	-	
EntryTime	DATETIME	8	
Password	VARCHAR	15	

Primary Key: SNo
Purpose: This table is used to store the encrypted messages which are used in (Hybrid) Mode.

3.9.5Table: Encrypted Messages Security

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
EncryptedField1	VARCHAR	3000	
ShowHighPrivilegeUserOnly1	BIT	1	
EncryptedField2	VARCHAR	3000	
ShowHighPrivilegeUserOnly2	BIT	1	
EncryptedField3	VARCHAR	3000	
ShowHighPrivilegeUserOnly3	BIT	1	

Primary Key: SNo
Purpose: This table is used to store the encrypted messages which are used in (Security) Mode.

3.9.6Table: Decrypted Messages

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
EncryptedMessageSNo	INT	4	Foreign Key
DecryptedMessage	TEXT	-	
EntryTime	DATETIME	8	

Primary Key: SNo
Purpose: This table is used to store the decrypted messages which are used in (Speed) Mode.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

3.9.7Table: Decrypted Messages Hybrid

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
EncryptedMessageSNo	INT	4	Foreign Key
DecryptedMessage1	TEXT		
DecryptedMessage2	TEXT	-	
EntryTime	DATETIME	8	
Password	VARCHAR	15	

Primary Key: SNo
Purpose: This table is used to store the decrypted messages which are used in (Hybrid) Mode.

3.9.8Table: Decrypted Messages Security

FIELD NAME	TYPE	SIZE	DESCRIPTION
Sno	INT	4	Primary Key
EncryptedMessageSNo	INT	4	Foreign Key
DecryptedField1	TEXT	-	
DecryptedField2	TEXT	-	
DecryptedField3	TEXT	-	

Primary Key: SNo
Purpose: This table is used to store the decrypted messages which are used in (Security) Mode.

4. INPUT DESIGN

Input design is the process of converting user-originated inputs to a computer understandable format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system. A large number of problems with a system can usually be tracked backs to fault input design and method. Every moment of input design should be analyzed and designed with utmost care. The design of the input should be made the input as the over to the numerous networks in the reliable area that should be passed as the installation in the remote network. It has the following constraints in the input database.

1. All the files from the disk should be acquired by data.
2. It is suitable to more available data clearance and made
3. The menu of design should be understandable

The system takes input from the users, processes it and produces an output. Input design is link that ties the information system into the world of its users. The system should be user friendly to gain appropriate

DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

information to the user. The decisions made during the input design are,
The application gives the low time consumption to make the sensitive application made simple. When applying the project it provides the low man-power attrition with the reasonable output. The amount of fund that the company can spend into the research and development of the system is limited.
System analysis decide the following input design details like, what data to input, what medium to use, how the data should be arranged or coded, data items and transactions needing validations to detect errors and at last the dialogue to guide user in providing input. Input data of a system may not be necessarily is raw data captured in the system from scratch. These can also be the output of another system or subsystem.
The design of input covers all the phases of input from the creation of initial data to actual entering of the data to the system for processing. The design of inputs involves identifying the data needed, specifying the characteristics of each data item, capturing and preparing data for computer processing and ensuring correctness of data.
The following forms are implemented.

5. OUTPUT DESIGN

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application the output is designed in such a way that it is attractive, convenient and informative. Forms are designed in C# .NET with various features, which make the console output more pleasing.
As the outputs are the most important sources of information to the users, better design should improve the system's relationships with user and also will help in decision-making. Form design elaborates the way of output is presented and the layout available for capturing information.
The following output forms can be implemented.

5.1.1DECRYPTION

Three forms are provided in which, three types (speed, hybrid, security) of decryption work is carried out and the original messages are displayed in text box

6. SYSTEM TESTING

Testing is vital to the success of the system. System testing makes a logical assumption that if all parts of the system are correct, the goal will be successfully achieved. In the testing process we test the actual system in an organization and gather errors from the new system operates in full efficiency as stated. System testing is the stage of implementation, which is aimed to ensuring that the system works accurately and efficiently.
In the testing process we test the actual system in an organization and gather errors from the new system and take initiatives to correct the same. All the front-end and back-end connectivity are tested to be sure that the new system operates in full efficiency as stated. System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently.
The main objective of testing is to uncover errors from the system. For the uncovering process we have to give proper input data to the system. So we should have more conscious to give input data. It is important to give correct inputs to efficient testing.
Testing is done for each module. After testing all the modules, the modules are integrated and testing of the final system is done with the test data, specially designed to show that the system will operate successfully in all its aspects conditions. Thus the system testing is a confirmation that all is correct and an opportunity to show the user that the system works.

6.1 UNIT TESTING

Unit testing verification efforts on the smallest unit of software design, module. This is known as "Module Testing". All the modules are tested separately. This testing is carried out during programming stage itself. In these testing steps, each module is found to be working satisfactorily as regard to the expected output from the module.

6.2 ACCEPTANCE TESTING

Acceptance testing is performed after system testing is done and all or most of the major defects have been

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.8 July - August – 2024
DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

fixed. The goal of acceptance testing is to establish confidence in the delivered software system that it meets the end user/customers requirements and is fit for use. Acceptance testing is done by user/customer and some of the project stakeholders. Acceptance testing is done in production kind of environment. For Commercial off the shelf (COTS) software's that are meant for the mass market testing needs to be done by the potential users, there are two types of acceptance testing for COTS software's.

7. SYSTEM IMPLEMENTATION

In the System development life cycle, the system implementation and maintenance will be occurring after the completion of analysis and system design. The term implementation is ranging from the conversion of a basic application to a complete replacement of a computer system. In other term, implementation is used to process of converting a new or a revised system design into an operational one.Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization.The implementation process begins with preparing a plan for the implementation of the system. According to this plan, the activities are to be carried out in these plans; discussion has been made regarding the equipment, resources and how to test activities. Thus a clear plan was prepared for the activities.
The implementation phase is less creative then system design. It is primarily concerned with,

- User Training
- Site preparation

User Training
Analyst user training focus on two factors, which is user capabilities and the nature of the system being installed in the system. Users range from the naïve to the highly sophisticated. Development research provides interesting insights into how naïve computer users think about their first exposure to a new system.
Site Preparation
The review team prepares a formal review plan around the objectives of review, the type of evaluation to be carried out and the time schedule required.
Types Of Implementation
There are three types of implementation,

- Implementation of a computer system to replace a manual system.
- Implementation of a new computer system to replace an existing one.
- Implementation of a modified application to replace an existing one, using the same computer.

During the final testing, user acceptance is tested followed by user training. Depending on the nature of the system, extensive user training may be required. Conversion usually takes place about the same time the user is being trained or later. The implementation of the project is done through the following steps,

- Install NET framework.
- Create the folder with project name and bin, obj folders are copied into that project folder.

CONCLUSION

Through this project, the problem of secure communication is eliminated. In addition, the application required less working experience in systems to run the software. The application is tested well so that the end users use this software for their whole operations.It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the project is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The project effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

DOI:10.46647/ijetms.2024.v08i04.013 ISSN: 2581-4621

REFERENCES

[1] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, ‘‘Privacy- preserving cloud computing on sensitive data: A survey of methods, products and challenges,’’ Comput. Commun., vols. 140–141, pp. 38–60, May 2019.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ‘‘A survey on IoT security: Application areas, security threats, and solution architectures,’’ IEEE Access, vol. 7, pp. 82721–82743, 2019.

[3] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, and Y. Zhou, ‘‘Identity- based encryption transformation for flexible sharing of encrypted data in public cloud,’’ IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3168–3180, 2020.

[4] Eurostat, Cloud computing - statistics on the use by enterprises (Dec. 2016 (Accessed 14 February 2019)). URL http://ec.europa.eu/eurostat/statistics- explained/index.php/ Cloud_computing_-_statistics_on_the_use_by_enterprises

[5] C. S. Alliance, Cloud usage: Risks and opportunities report (Sep. 2014 (Accessed 14 February //downloads.cloudsecurityalliance.org/initiatives/collaborate/netskope/Cloud_Usage_Risks_and_Opportunities_Survey_Report.pdf

[6] A. Westin, Privacy and Freedom, Atheneum, 1967.

[7] E. Ramirez, J. Brill, M. K. Ohlhausen, J. D. Wright, T. McSweeny, Data brokers: A call for transparency and accountability, U.S. Federal Trade Commission (May 2014).

[8] M. A. Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications 71 (2016) 11–29.

[9] S. Singh, Y.-S. Jeong, J. Park, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications 75 (2016) 200–222.

[10] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications 79 (2017) 88–115.

[11] P. Praveen-Kumar, P. Syam-Kumar, P. Alphonse, Attribute based encryption in cloud computing: A survey, gap analysis, and future directions, Journal of Network and Computer Applications 108 (2018) 37–52.

[12] Z. Shan, K. Ren, M. Blanton, C. Wang, Practical secure computation outsourcing: A survey, ACM Computing Surveys 51 (2) (2018) Article No. 31.