Journal of Computer Science & IT Research and Review Volume-1, Issue:1- September -2025

VISWAM PUBLICATIONS

Journal of Computer Science & IT Research and Review

https://viswampublications.com/journals/index.php/jcsitrr



EFFICIENT UTILIZATION OF STORAGE MANAGEMENT POLICY WITH SECURITY OF HYBRID CLOUD IN SOCIAL NETWORKING

Mrs M. Saraswathi[1] Research Scholar Sri Meenakshi Vidiyal Arts and Science College, Paluvanchi, Tiruchirappalli,Tamilnadu,India (Affiliated to Bharathidasan University) E-Mail:sarascssmvc@gmail.com

Dr R.Sugumar[2] Professor & Deputy Director Christhuraj College, Royal Nagar, Panjappur, Tiruchirappalli,Tamilnadu,India E-Mail:rsugusakthi1974@gmail.com

ARTICLE INFO

Received : 08.03.2025
Revised : 25.05.2025
Accepted : 19.08.2025
Published : 26.09.2025

Corresponding author:
Mrs M. Saraswathi
sarascssmvc@gmail.com

Keywords:
Hybrid cloud ,
Social media ,
Security threat.

ABSTRACT

Nowadays, in over the world everyone connected via social networking. The Online social media network has become big part of human life in every day. In social networking the human beings shared resources trough cloud computing. The formation of social networks and the cloud computing technology has led to the registration of large number of online users into the networks. In social media the peoples are transforming the way of users and make new social relations or relate with family and friends. Cloud computing has therefore the freedom of relations on social media that has made most users to freely share personal information via social media it leads the security threat. and we eradicate the security threat in social networking, who the users are shared their own personal resources and also another difficulty in social media is storage management .because social networking it store the massive amount of user information like text,images, audio, video and so on and to reduce the storage space and security threat of hybrid cloud in social networking.

This article is licensed under Creative Commons Attribution-Non-commercial 4.0 International License.
Copyright ©2025 Author(s) retains the copyright of this article. DOI:

1. INTRODUCTION

A social network may be a network of persons associated by interpersonal relationships. The relationships between these users have variety of dissimilar names across different social networks like friends, or followers. Through these relationships users share messages and media among themselves. There are many online social networking websites like Face book, LinkedIn Twitter and so on. These social networking sites have overflow 100 million active members. Social networking has become an everyday a part of many peoples' lives as evidenced by the large user communities. Some communities even exceed the population of huge countries, for instance Facebook has over 400 million active users. With such an excellent number of users using these services.

Cloud refers to a Network or Internet. In other words, we will say that Cloud are some things, which is present at remote location. Cloud can provide services over public and personal networks, i.e., WAN, LAN or VPN. Applications alike e-mail, web conferencing, customer relationship management (CRM) execute on cloud. Cloud Computing states that operating, constructing, and accessing the hardware and software resources remotely. It deals online data storage, infrastructure, and application.

Cloud computing and social networking has intermingled during a sort of ways. Most obviously social networks are often hosted on cloud platforms or have scalable applications within the social networks. Modern research has also offered cloud based applications using social networks for user management and authentication during a system called social clouds (Chard, 2010). Cloud environments typically provide low level abstractions of storage. Social networks storing heavy multimedia content in cloud storage systems. Videos and pictures are the foremost popular content on social media, which essentially spend the utmost space allocated to them. They need the capacity to hamper applications and servers with all of their resource demands. Except for data storage, the social networks are now also using clouds for various other tasks. So during this paper, we examine the safety and enhance the storage management policy of cloud computing in social networking

In cloud trouble related to data security that has impelled the need for maintain personal data private and improvement of the trust towards the service provider. This study investigates the security concerns that arises from the use of cloud technology in social networks and provides a proposal on the measures that needs to be enforced to secure personal information stored over the cloud.

Basic Concepts in Cloud

There are certain services and models working behind the scene making the cloud computing feasible and accessible to end users. There are two working models for cloud computing:

- Deployment Models
- Service Models

1. DEPLOYMENT MODELS

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid, and Community.

Types of clouds

Cloud computing is typically classified in the following three ways:

Private cloud:

The computing infrastructure is committed to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real models of cloud computing. Private clouds are more expensive and more secure when compared to public clouds The private cloud allows systems and services to be accessible within an organization. It is more protected because of its private nature.

Public cloud:

In public cloud the computing infrastructure is accommodated by the cloud vendor at the vendor premises. The customer has no visibility and switch over where the computing infrastructure is hosted. The computing infrastructure is public between any organizations. The public cloud allows systems and services to be easily available to the general public. Public cloud may be fewer secure because of its openness.

Hybrid cloud:

Organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud using services like Salesforce cloud computing for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully. The hybrid cloud is a mixture of public and private cloud, in which the critical activities are performed using private cloud while the non-critical activities are performed using public cloud.

2. Service Models

Cloud computing is based on service models. These are categorized into three basic service models which are -

- Infrastructure-as–a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)
- Infrastructure-as-a-Service (IaaS)

IaaS provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.

- Platform-as-a-Service (PaaS)

PaaS provides the runtime environment for applications, development and deployment tools, etc.

- Software-as-a-Service (SaaS)

SaaS model allows using software applications as a service to end-users.

2. OBJECTIVE OF THE PAPER

This paper concentrates on subject in cloud Security and the cloud storage management policy in social networking. The major objective of this research work is to enhance a storage management in a cloud environment with secured data access and protect ownership of information, does not allow unauthorized access in social networking. Even though an encryption scheme can ensure the confidentiality within Personal information in social networking. We still should make stronger the valid users when using the system, because of accidental or malicious operation that would guide to private information's to other illegal users. So to achieve this objective, we have to generate a User Authorized Pin (UAP) from Password Credential Identity (PCI), this symmetric encryption technique and proof of data ownership and provide keeping signing rights.

In this paper mainly concentrate the reduce the storage space when the user upload the content text, images, audio, video using the framework Content Compress Storage Framework (CCSF). This technique involves the encryption with user data and a User Profile Key (UPK).

3. LITERATURE REVIEW

Gizealew Alazie Dagnaw, et al [2019] discussed a social network, because the name suggests may be a network of people created for social communication. it's a huge platform where people interact with others anywhere within the world online supported some relationship. The connections are often friendship, family membership or others with some shared interests. Despite these significant benefits, there are serious concerns and challenges about this new technology. The most vital issue is said to security and privacy subjects in cloud-based environments. Accordingly, challenges and concerns associated with cloud based environments are identified and most appropriate current solutions for every challenge are described. In overall, it is anticipated that cloud computing are going to be the foremost important and challenging issue in IT industry. As regarding the significance of this technology, we hope this paper will contribute to a better understanding of the vision of cloud computing and therefore the challenges ahead for further researches. Likewise, social networks have seen enormous growth, with many Internet users actively participating across various social networking websites.

Jaydip Kumar [2019] discussed need to secure the data which may in the form of text, audio, video, etc. There are various algorithms designed by the researchers for securing the data on the cloud. This paper mainly focused is an attempt to elaborate some of the important algorithms for the security of data for this purpose, exhaustive literature has been conducted.

C.Veni [2018] discussed about the basic concepts of clouds computing and also model available in cloud , security threats of cloud computing.

Karunakar Reddy et al[2018] discussed Cloud computing is related to other research areas like distributed and grid computing, Service-Oriented Architecture, and virtualization, as cloud computing inherited their limitations and advancements. It is possible to exploit latest opportunities for security. This paper objective is to discuss and analyze how attain mitigation for cloud computing security risks as a basic step towards obtaining secure and safe environment for cloud computing. The results exposed that, using a simple decision tree model Chaid algorithm security rating for classifying approach is a robust technique that enables the decision-maker to measure the extent of cloud securing, and the provided services. It was demonstrated throughout this paper that policies, standards, and controls are critical in management process to safeguard and protect the systems as well as data. The management process should evaluate and understand cloud computing risks for protecting systems and data from security exploits.

B.Jagadhesan et al[2016] discussed how we store information and run applications. Rather than running programs and data on an individual desktop computer, everything is held in the cloud. A cloud service provider offers the services for the data request in a remote server. virtualization aspect of cloud computing in Social network felicitatesbetter utilization of resources. The industry needs to address the foremost security risk in the underlying technology. The cloud computing environment in Social networking aggravated with various security problems. This paper addresses challenges in securing data in cloud for Social networking.

Adnan Majeed[2016] discussed to highlight the importance of social network big data with mobile cloud. The primary data is collected from questionnaire, interviews, and previous research paper.

Auwal S. I et al (2015) discussed online social network (OSN), people has to easily communicate with one another. All user generated data with the help of OSN does not allow the hackers. Privacy issues in OSN.

Tadepalli [2015] discussed the millions of people are connected through internet and also connected on Social networking. Social networks are more than just a place for social interactions and personal relationship.

R. Velumadhava Rao et al [2015] discussed Cloud service providers such as Amazon IBM,Google's Application, Microsoft Azure etc., provide the users in emerging applications in cloud environment and to access them from anywhere. Cloud data are stored and retrieved in a remote server with the help of services provided by cloud service providers. Providing security is a main concern as the data is transmitted to the remote server over a channel (internet). Already implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we focused data related security challenges in cloud based environment and solutions to overcome.

Harshali Sonawane et al[2014] discussed dynamic Social Cloud and to enable users to share heterogeneous resources

within the context of a social network we have proposed leveraging of the social relationships. We consider that combining trust relationships with suitable incentive mechanisms could provide much more sustainable resource sharing mechanisms. We have presented a business application as a means of regulating sharing, due to the unique nature of the Social Cloud. The business application is new as it uses both social and economic protocols. In today's world, social community credentials are being used for authentication purpose on many other websites (e.g. Facebook). Here we outline our vision of creating a Social Storage Cloud, looking especially at possible market mechanisms that could be used to create a dynamic Cloud infrastructure in a Social network environment.

Kyle Chard et al. [2014] in this paper author has to explore new ways to interact with, and

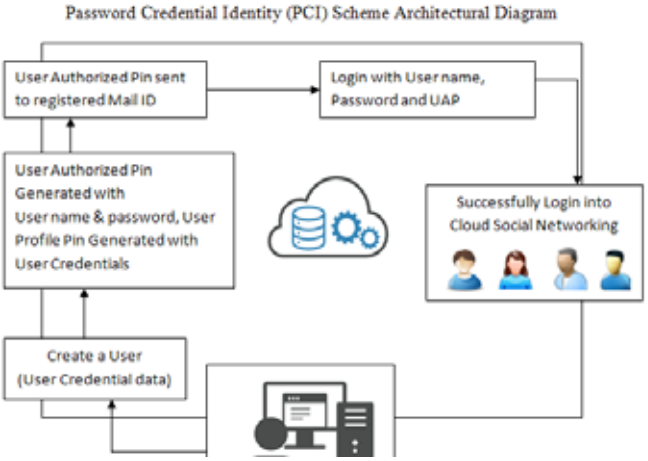
exploit these developing paradigms. Social networks are used to real world relationships that

allow users to share information and form connections between one another, We propose pre-

well-known trust formed through friend relationships within a Social network to form a

dynamic "Social Cloud", allowing friends to share resources within the context of a Social

network. Finally is to create a dynamic Cloud infrastructure in a social network environment.



4. METHODOLOGY

4.1 Proposed PCI Scheme

This section thoroughly explores the idea and the architecture of the two main cryptosystems, such as Password credential identity(PCI), and Content compress storage framework(CCSF), that are used to define secure and efficient storage access control techniques of Hybrid Cloud in social networking.

In this paper first to propose the Password credential identity is to communicate securely and verify the signatures of users. The PCI scheme is constructed based on a User Password Credential. We are generate a User Authorized Pin (UAP) from PCI Scheme.When the user login into the social networking first they login with user name and password then the User Authorized Pin is generated from user Password credential and sent to the User mail id. The user receive the secret key (UAP) and finally the user enter the UAP it verify the user is authorized or not authorized. The PCI scheme must be protected against user's attack. If the user is authorized then the users enter the home of social networking.

Steps in the process flow of Proposed Password Credential Identity (PCI)

1. The social networkingUsers request to register as a user for use cloud storage space in different types of cloud.
2. The User Profile Pin (UPP) is generated from the user given user credentials (first name, last name, phone number, mail id,date of birth,gender).the UPP is used to after in second phase for compress the storage data in cloud.
3. The User Authorized Pin (UAP) is generated, when the users login to the cloud social networking.
4. The UAP is generated from the users Login Credentials like User name and Password.
5. Generated UAP is send through the Users E-mail.
6. Successfully the user's login with UAP to Enter the User's home page, then the user's upload their Data(Text,Image,Audio,Video) in the Public or Private Cloud.
7. Supposed the user's UAP is not matched in cloud Data Base, then the user's failed to login their cloud social networking.

The Password Credential Identity (PCI) is strappingly protects the data from unauthorized access. The PCI ensures that the user is valid or not valid in the cloud social networking. The PCI generated every time when the user login into the cloud social networking and send trough the users email. The PCI does not allow the unauthorized user to upload the data content in the cloud social networking.

Procedures to generate a UAP from the User Password Credential

Step 1. Get a four random letters in User Password Credential(Username ,Password)

Step 2. Encrypted data is considered as input for tag generation

Step 3. Merge the each four letters and form a plain text

Step 4. The plain text is converted to ascii code

Step 5. The ascii code converted into binary 0 and 1

Step 6. Find the size of the total bits.

Step 7. Divide the total bits by each 8 bits blocks.

Step 8. Find the one's complement for each 8 bits block

Step 9. Find the reverse of each 8 bits block

Step 10. Merge to all the 8 bits block.

Step 11. Divide the all bits block by each 32 bits block.

Step 12. Merge the each 32 bit block as a single 32 bit block.

Step 13. Split a 32 bit block to each eight bit block.

Step 14. Convert each eight bit binary to ascii value.

Step 15. Convert the ascii decimal value to ascii character produce the User Authorized Pin(UAP)

Procedures to generate a User Profile Pin (UPP)

Step 1.Get a sixteen random letters from the user Credential (first name, last name
Address, phone number, mailed, date of birth, gender, city)

Step 2. Merge the sixteen letters and form a plain text

Step 3. The plain text is converted to ascii code

Step 4. The ascii code converted into binary 0 and 1

Step 5. Find the size of the total bits

Step 6.Divide the total bits by each 8 bits block.

Step 7.Rotate the each eight bits blockleft to right 7 times

Step 8. Find the one's complement for each 8 bits block

Step 9. Convert each bit binary to ASCII value

Step 10.Convert the ascii decimal value to ascii character produce the User Profile Pin(UPP).

Procedures for Content Compress Storage Framework (CCSF)

Step 1. User uploaded data is converted to binary (Text,Image,Audio,Video)

Step 2. Count the number of bits in the User Uploaded Binary Data

Step 3. Divide the binary data into into each 128 bit block

Step 4. Find the two's complement in each 128 bit block

Step 5. Reverse the each 128 bit block

Step 6. Get the ASCII value of User Profile Pin (UPP)

Step 7. ASCII value of User profile Pin is converted to binary

Step 8.Find the XOR operation each 128bits block with generated user profile pin

Step 9.Merge each 128 bits block into single block

Step 10. Divide the binary block into eight bit block

Step 11 . Remove the bits in the first and last place, if the bit is '1'in the each eight bit block

Step 12. Finally compressed Binary data is stored in the cloud storage Pseudo code for Proposed PCI Scheme

Algorithm:-encryption_UAP(UCT)

Inputs:- Users' Credential data

```
UCT   ←User Credential Text
NT    ←Size of PT
AC    ←ASCII codes of PT
BIN   ←Binary code for AS
TB    ←Total No.of Blocks
EBK   ← Split eight bit Blocks with binaries
OCM   ← one's Complement
REV   ← Reverse the bits
MER   ← Merge th bits
L     ← Number of 8bits binary
SP    ← split 8bits Binary
DEC   ←Decimal value of 8bit binary
CT_Mem← Buffer Variable to append the decimal values
UAP   ←User Authorized Pin
OEBK← Ones complement 8 bit block

1.    start
2.    NT      ←sizeof(UCT) // find the size of the UCT
3.    for i   ← 1 to NT
Ac[i]←ASCII(UCT[i]) //convert into ASCII
BNY[i]←BINARY(AC[i]) //convert into 8bits binary
Temp←APPEND(BNY[i]) // temp variable for combine all the
      binaries
next i
4.    for i← 1 to NT
count←temp[i) // temp variable for combine all the binaries
count++;
next i
5.    TB=count // calculate total no.of blocks
6.    Sp=0
7.    While(Sp<=TB)
EBK[i]←SPLIT(temp) //method to split the binaries into block
Sp++
loop
// find one's complement for each eight bit block
8.    for i ← 1 to TB
for j ← 1 to K1
OEBK[j]←One_comp(EBK[j])
next j
next i
9.    Rev=0
10.   While(Spt<=E)
Rev_block[i]←Reverse(OEBK) //Reverse the each One's Com-
      plement 8bits block
Sp++
loop
11.   for i← 1 to N
DEC[i]←DECIMAL(DIV[i]) // convert the 8bits into decimal
CT_BUF←APPEND(ASCII(DECI[i]))
next i
12.   CT←CT_BUF
```

13. end

Pseudo code for Proposed Content Compress Storage Frame-work (CCSF) Scheme

Algorithm:-encryption_ CCSF(UUC)

Inputs:- Users' Uploaded data

UUC ←User Uploaded Content
UBD ←Convert uploaded data to binary data
NB ←count the number of bits
128_bit_block ←split 128 bit block
REV_128_bit_block← Reversed 128 bits block
UPP_ASCII← User Profile Pin Ascii value
UPP_bin← User Profile Pin binary value

XOR_VAL← REV_128_bit_block with UPP_bin
128_Merge←merge the all 128 bit blocks
EBK← Split eight bit Blocks with binaries
COM_Blcok← Compressed Bit Block

1. start
2. UCC←convert the user uploaded content to binary
3. for i← 1 to UCC
UBDA[i]←ASCII(UCT[i]) //convert into ASCII
UBD[i]←BINARY(AC[i]) //convert into 8bits binary
Temp←APPEND(BNY[i]) // temp variable for combine all the binaries
next i
4. for i← 1 to UBD
count←temp[i) // temp variable for combine all the binaries
count++;
next i
5. TB=count // calculate total no.of blocks
6. Sp=0
7. While(Sp<=UBDS)
128_bit_block[i]←SPLIT(SP) //method to split the binaries into block
Sp++
Loop
8. While(Sp<=TB)
EBK[i]←SPLIT(temp) //method to split the binaries into block
Sp++
Loop
9. While(bit<=128_bit_block)
REV_128_bit_block [i]←reverse(128_bit_block) //method to split the binaries into block
Sp++
loop
// find one's complement for each eight bit block
10. for i ← 1 to REV_128_bit_block
for j ← 1 to K_1
XOR_VAL←=REV_128_bit ^ UPP_bin
next j
next i
11. for i ← 1 to XOR_VAL
for j ← 1 to K_1
128_Merge =128_Merge + XOR_VAL [i]
next j
next i

12. or i← 1 to 128_Merge

EBK =split(128_Merge)

next i

13. Rev=0
14. While(Spt<=BKE)
15. If(sbk[o] and sbk[7]==1)
COM_Blcok =bke[i] //remove the bits if 0 and last place is "1" 8bits block
Sp++
loop
16. CT←CT_BUF
17. end

Sample output

Generate User Profile Pin (UPP)

1. USER CREDENTIAL INPUT:

SNO	INPUT FIELD	VALUES
1.	First Name	saraswathi
2.	Last Name	smvcollege
3.	Phone Number	8124675865
4.	Mail Id	saraswathy@gmail.com
5.	Date	25.11.1985
6.	Gender	Female

2. Get a Random sixteen letters from User Credential Input

Fn=sara
Ln=coll
Ph=24
Mid=wa
Date=11
Gen=ma
Plain Text=saracoll24wa11ma

3. ASCII Code equivalent plain text

s=115	a=97	r=114	a=97	c=99	o=111	l=108	l=108
2=50	4=52	2=119	a=97	1=49	1=49	m= 109	a=97

4. ASCII Value Equivalent Binary

115=01110011	**97**=01100001	**114**=01110010	**97**=01100001
99=01100011	**111**=01101111	**108**=01101100	**108**=01101100
50=00110010	**52**=00110100	**119**=01110111	**97**=01100001
49=00110001	**49**=00110001	**109**=01101101	**97**=01100001

5.Total number of bits=128

01110011011000010111001001100001011000110111011110110110001101100001100100011010001110111011000010011000100110000101101101100001

6. Split 8 bit block

01110011	01100001	01110010	01100001	01100011	01101111	01101100	01101100
00110010	00110100	01110111	01100001	00110001	00110001	01101101	01100001

7. Left to right Bit rotation (left rotation) 7 times bit rotation

10111001	10110000	00111001	10110000	10110001	10110111	00110110	00110110
00011001	00011010	10111011	10110000	10011000	10011000	10110110	10110000

8. Ones complement of rotation bits

01000110	01001111	11000110	01001111	01001110	01001000	11001001	11001001
11100110	11100101	01000100	01001111	01100111	01100111	01001001	01001111

9. Binary equivalent ASCII CODE

70	79	198	79	78	72	201	201
230	229	68	79	103	103	73	79

10. ASCII CODE Equivalent ASCII TEXT

FOÆONHÉÉæåDOggIO

Experimental OUTPUT(UPP)

FOÆONHÉÉæåDOggIO
Experimental Input /Output
Password Credential Identity (PCI)
Generate a UserAuthorized Pin (UAP) from the User Password Credential:

1. USER PASSWORD CREDENTIAL INPUT:

SNO	INPUT FIELD	VALUES
1.	User Name	saraswathi
2.	Password	saraswathy@gmail.com

2. Get a Random 8 letters from User Password Credential Input
User Name=arsa
Password=srwt
Plain Text=arsasrwt

3. ASCII Code equivalent plain text

a=97	r=114	s=115	a=97
s=115	r=114	***w=119***	***t=116***

4. ASCII Value Equivalent Binary

97=01100001	**114**=01110010	**115**=01110011	**97**=01100001
115=01110011	**114**=01110010	**119**=01110111	**116**=01110100

5.Total number of bits=64
01100001 01110010 01110011 01100001 01110011 01110010 01110111 01110100

6. split8 bit block

01100001	01110010	01110011	01100001
01110011	01110010	01110111	01110100

7. 1's Complement of 8 bit block

10011110	10001101	10001100	10011110
10001100	10001101	10001000	10001011

8.Reverse the each 8 bit block

01111001	10110001	00110001	01111001
00110001	10110001	00010001	11010001

9.Merge the 8 bit block into single block
0111100110110001001100010111100100110001101100010001000111010001

10. Split the 32 bit block

First 32 bit Block	01111001 10110001 00110001 01111001
Second 32 bit Block	00110001 10110001 00010001 11010001

11.Xor Operation

First 32 bit Block	01111001 10110001 00110001 01111001
Second 32 bit Block	00110001 10110001 00010001 11010001
XOR Binary Value	01001000 00000000 00100000 10101000

12. Split a XOR 32 bit block to each eight bit block

01001000	00000000	00100000	10101000

13.Binary equivalent Ascii Code

72=01001000	**0**=00000000	**32**=00100000	**168**=10101000

UserAuthorized Pin (UAP)

72	**0**	**32**	**168**

Experimental Input /Output

Procedures for Content Compress Storage Framework (CCSF)

1. Uploaded data
   HIHELLOIAMSARASWATHIASIAMWORKING
2. Uploaded data converted into binary

01001000	01001001	01001000	01000101	01001100	01001100	01001111	01001001
01000001	01001101	01010011	01000001	01010010	01000001	01010111	01000001
01010100	01001000	01001001	01000001	01010011	01001001	01000001	01001101
01010111	01001111	01010010	01000001	01001011	01001001	01001110	01000111

3. Divide the binary data into into each 128 bit block

01001000	01001001	01001000	01000101	01001100	01001100	01001111	01001001
01000001	01001101	01010011	01000001	01010010	01000001	01010111	01000001

01010100	01001000	01001001	01000001	01010011	01001001	01000001	01001101
01010111	01001111	01010010	01000001	01001011	01001001	01001110	01000111

4. Find the two's complement in each 128 bit block

10110110	10110111	10111000	10111011	01001101	10110100	10110001	10110111
10111111	10110011	10101101	10111111	10101110	10111111	10101101	10101001

10111111	10101100	10111000	10110111	10111111	10101101	10110111	10111111
10110011	10101001	10110001	10101110	10110101	10110111	10110010	10111001

5. Reverse the each 128 bit block

01101101	11101101	00011101	11011101	10110010	00101101	10001101	11101101
11111101	11001101	10110101	11111101	01110101	11111101	10110101	10010101

11111101	00110101	10111000	10111011	01001101	10110100	10110001	10110111
10111111	10110011	10101101	10111111	101011101	10111111	10101101	10101001

6. Get the ASCII value of User Profile Pin (UPP)

115	97	114	97
99	111	108	108
50	52	119	97
49	49	109	97

7. ASCII value of User profile Pin is converted to binary

01110011	01100001	01110010	01100001
01100011	01101111	01101100	01101100
00110010	00110100	01110111	01100001
00110001	00110001	01101101	01100001

8. Find the XOR operation each 128bits block with generated user profile pin

128	01001000	01001001	01001000	01000101	01001100	01001100	01001111	01001001
UPP	01110011	01100001	01110010	01100001	01100011	01101111	01101100	01101100
XOR	00111011	00101000	00111010	00100100	00101111	00100011	00100011	00100101
128	01000001	01001101	01010011	01000001	01010010	01000001	01010111	01000001
UPP	00110010	00110100	01110111	01100001	00110001	00110001	01101101	01100001
XOR	01110011	01111001	00100100	00100000	01100011	01110001	00111010	00100000

128	01010100	01001000	01001001	01000001	01010011	01001001	01000001	01001101
UPP	01110011	01100001	01110010	01100001	01100011	01101111	01101100	01101100
XOR	00100111	00101001	00111011	00100000	00110000	00100110	00101101	00100001
128	01010111	01001111	01010010	01000001	01001011	01001001	01001110	01000111
UPP	00110010	00110100	01110111	01100001	00110001	00110001	01101101	01100001
XOR	01100111	01111011	001001011	00100000	01111010	00111000	00100011	00100110

9. Merge each 128 bits block into single block

00111011001010000011101000100100001011110010001100100011001001010111001101111001001001000010000001100011
11100010011101000100000001001110010100100111011001000000011000000100110001011010010000101100111011110011001
00101100100000011110100011100000100011001001 10

10. Divide the binary block into eight bit block

00111011	00101000	00111010	00100100	00101111	00100011	00100011	00100101
01110011	01111001	00100100	00100000	01100011	01110001	00111010	00100000
00100111	00101001	00111011	00100000	00110000	00100110	00101101	00100001
01100111	01111011	001001011	00100000	01111010	00111000	00100011	00100110

11.Remove the bits in the first and last place, if the bit is ‘1’in the each eight bit Block

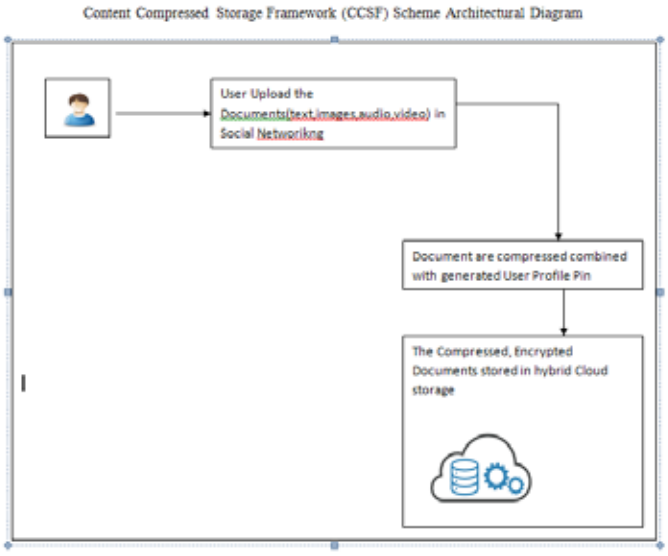
0011101	00101000	00111010	00100100	0010111	0010001	0010001	0010010
0111001	0111100	00100100	00100000	0110001	0111000	00111010	00100000
0010011	0010100	0011101	00100000	00110000	00100110	0010110	0010000
0110011	0111101	00100101	00100000	01111010	00111000	0010001	00100110

12. Finally compressed binary data is stored in the cloud storage.

0011101	00101000	00111010	00100100	0010111	0010001	0010001	0010010
0111001	0111100	00100100	00100000	0110001	0111000	00111010	00100000
0010011	0010100	0011101	00100000	00110000	00100110	0010110	0010000
0110011	0111101	00100101	00100000	01111010	00111000	0010001	00100110

4.2 Proposed CCSF Scheme

n this Content Compress Storage Framework (CCSF) scheme involves two phases. In the first phase, generate the User Profile Pin (UPP).The User Profile Pin is generated with the help of user credential such as (first name, last name, phone number, mail id, date of birth , gender) etc. In the second phase, the user uploaded data (text, image, audio, video) with User Profile Pine and get the compressed data. Finally the compressed data stored on hybrid cloud.



5. CONCLUSION

Even though cloud computing is the new emerging technology that provides user has to work with social networks. In this paper, it faces security challenges and storage utilization on cloud as well as provide solution to overcome the risk involved in cloud computing. To provide secure data access in cloud, the PCI technique can be used for storing and retrieving data from cloud and also Content Compress Storage Framework (CCSF) scheme used for reducing storage space on cloud.

References

[1] C.Veni A Study on Social Networks and Cloud Computing International Journal of Engineering Trends and Applications (IJETA) – Volume 5 Issue 1, Jan-Feb 2018.

[2] Tadepalli A Survey on the Role of Cloud omputing in Social Networking Sites International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1509-1512.

[3] Gizealew Alazie Dagnaw Challenges and Opportunities of Cloud Computing in Social Network; Survey Internet of Things and Cloud Computing. Vol. 7, No. 3, 2019, pp. 73-79.

[4] B.Jagadhesan Cloud Computing in Social Networking for Security Policy Enhancement

International Journal of Web Technology Volume: 05 Issue: 01, June 2016, Pages: 51-54.

[5] Adnan MajeedMobile Cloud Computing & Big Data Social Network Scientific

Research Journal (SCIRJ), Volume IV, Issue I, January 2016 20 ISSN.

[6] Harshali Sonawane Social Cloud Computing Using Social Network IOSR Journal of

Computer Engineering (IOSR-JCE) Volume 16, Issue 3, Ver. II (May-Jun. 2014), PP 15-18.

[7] Jaydip Kumar Cloud Computing Security Issues and Its Challenges: A Comprehensive

Research International Journal of Recent Technology and Engineering (IJRTE) ISSN:

2277-3878,Volume-8, Issue-1S4, June 2019.

[8] Karunakar Reddy Data Mining Technique in Securing the Cloud Int. Journal of

Engineering Research and Application ISSN : 2248-9622, Vol. 8, Issue3, (Part -2)

march2018, pp.01-09.

[9] D.Sakthipriya Security issues in cloud computing Journal of Analysis and Computation

(JAC) (An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861.