A Model To Ensure Business Ethicsin Social Networks

Neethu. MR, Harini.N

Abstract: Social networking sites generally push aside trust issues to maximize social interaction. One of the barriers to trust in online environment is privacy because Internet by design lacks a unified method for identifying who communicates with whom. Privacy concern is a person's awareness and assessment of risks related to privacy violations. Violation to privacy happens mostly because users themselves don't understand the consequences of sharing their personal data with peers. Context aware systems like cameras, accelerometers, microphones etc. affect privacy to a larger extent. Individuals are more likely to be concerned about their privacy when information is used without one's knowledge. In this paper, a privacy preservation scheme that safeguards users from online social networks selling data to third parties, based on distributed ledger technology is presented. The proposed scheme uses IPFS to store the digital content with high integrity thus making it available to all.

Index Terms: Social Networking Sites, Internet, Information sharing Privacy, Distributed ledger technology, IPFS

1. INTRODUCTION

Today, web has become more personal with the existence of social networking sites that offers web based services using which users connect with their peers and make their visibility in their network. Popular social media sites include Classmates, DeviantArt, Facebook, Google+, LinkedIn, Mastodon, Mix, MySpace, Pinterest, Reddit, Tumbler, Twitter, Yik Yak, YouTube etc (De Salve, Mori, and Ricci 2018). Researchers have explored many sides of social media like its usage for obtaining feedback from stakeholders by organizations; reviews written by consumers related to quality of products, communities successfully connecting based on common interests and goal etc. Studies show that with a plethora of applications being offered through social media platforms, today around 50 million businesses are active on Facebook business pages. The reach of these business pages in social networking sites are tremendous and their popularity is evident with the number of likes, shares, messages, posts etc to those pages.Social networking sites implement a wide variety of technical features for exchange of information with their backbone consisting visible profiles that could be used as a means for self-introduction in the network. The existences of these profiles which are to be made available to only passive receivers are now made available to active gatherers of information. Profiling specific characteristics like age, gender, academic levels etc. are exploited by these information harvesters thus causing hindrance to the privacy of users. The access to the stored information causes problems like fraud vandalism, etc. in the web environment. A fully filled out Facebook profile contains around 40 personal information including name, birthday, relationship status, favorite movie, educational history, employment history, photos etc. The exponential growth in the number of users associating themselves with popular social networks as shown in graph (Figure 1) demands a security frame work that enhances privacy concerns of individual participants in social networking sites. The results of experimentation clearly brought out the ability of the schemes in terms of preserving privacy concerns from evil eyed business applications. The rest of the paper is organized as follows: Section 2 consist of review of literature in the field of security in social media, section 3 depicts the proposed architecture, Section 4 presents the results of experimentation and discussion and finally section 5 presents conclusion and directions for future extension of the work.

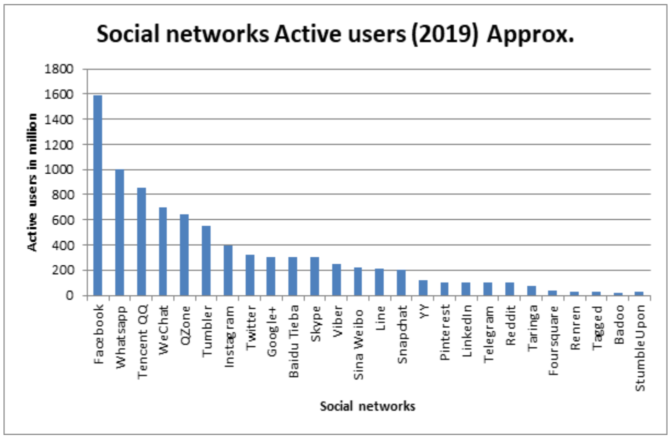


Fig. 1. *Active users in social networking sites*

2 LITERATURE REVIEW

2.1 Popularity of social media

Humans are by nature socially active. It can be observed that some of them are very active and some are less active. When people become more eager for connectivity and networking, the age of digitization facilitates this with the advent of many social networking websites and applications. As stage progresses, relationships grow but unfortunately the security flaws in this medium make relationships end in social media itself. As per the statistics, approximately 2 billion users used SNS and applications in 2015 and with the advent of mobile phones, the number of users touched 2.6 billion mark by 2018.

2.2 Impact of social media

Being a handy means for users to keep in touch with friends and family, social networks evolved to have a real impact on society(Benkhelifa and Laallam, 2018).. It is used in many ways to contour politics, business, careers, world culture, innovation, education etc. Participants share information on social media for many reasons like to voice out their support

- *Neethu. M R, Research Scholar, Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India . E-mail: cb.en.d.cse17014@cb.students.amrita.edu.*
- *Harini. N, Assistant Professor, Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India . E-mail: n_harini@cb.amrita.edu*

an issue or cause that they feel strong, exchange one views and valuable information, build an image to showcase themselves, nurture relationships and involve in happenings around the world(Bahri, Carminati, and Ferrari 2018). There are many negative impacts for the society from social media like cyber bullying, lack of privacy, depression and anxiety, fear of missing out, unrealistic expectations, general addiction (leading to out of focus, attention and lowered motivational levels)(Rathore et al. 2017). These psychological impacts have been found to lead to many physical problems and negative impacts in life and society. Reports show that some people even commit suicide due to either breakage of relationship that is built in social networks or due to leakage of their private information in the social media (Alves, Fernandes, and Raposo 2016). Even a tight secured system may leak personal information if privacy preserving policies are not well set.

2.3 Business and social media

Today every business enterprise needs to rely on social media to announce their existence and for becoming popular. It is important that every business enterprise pay careful attention to correctly choose the social media that suits them(Alalwan et al. 2017). Latest surveys show that 70% of business to customer marketers has acquired consumers through Facebook. Instagram and pinterest also plays their role in increased consumers through social media (Godey et al. 2016). Marketing through social media can carry significant success to the business as the consumers even tend to recommend the online brand to their friends thus increasing the business. Goals that can be achieved through social media marketing are not just limited to increased sales, hovering brand awareness, creating a brand identity and positive brand association, refining communication and interaction with important onlookers etc. These goals also induce severe privacy concerns like account hacking and impersonation, stalking and harassment, being compelled to turn over passwords, walking a fine line between effective marketing and privacy intrusion and privacy downside of location-based services. Although there exists many privacy protection tips and tricks provided by social web sites, most of the users do not know the importance of privacy settings and many who know do not care to keep proper settings to their account.

2.4 Privacy concerns

The marketing strategies used in social networking sites lead to many privacy concerns. The concerns are mainly about unauthorized access to the consumers data from SNS. This lead to reuse of user's personal data such as sharing the data with third parties, whose applications the users have installed or given access permission unknowingly. In brief, the users allow these applications to access in their personal authentication token (Mobile phone).

- View the contact list, initiate phone conversations or push message notifications.
- Make modifications in device calendar.
- Location access.
- Camera permission allows the company to click pictures, record videos.
- Audio permission allows to record audio
- Internal storage permissions give access to files and even allow them to delete it.

In case of social networks like Facebook also, the scenario is the same and hence third parties gain access to personal data. In response to privacy concerns, Facebook allow the user to logon to third party applications(De Salve, Mori, and Ricci 2018). When the user log in to multiple sites using single-sign-in feature, it makes the account more vulnerable with the lowest security. So-called daisy-chained accounts can also make identity theft easier for would-be scammers. Whether Facebook, Google or any other account, being a trusted source of identity, becomes a weak link in the chain, it gets targeted by the attackers (Feng et al. 2018). The possibility of less scrupulous websites may do anything with the user's data that the user agreed for. For example, they can even sell the data to another third party or fourth company that the user may not even be aware of. (Figure 2) summarizes the three-step process of application installation for Android apps.It is very common to observe users installing applications from playstore using ones social network account information. This process triggers social network websites to share basic information about the user that are publically available to be shared with the owner of the app downloaded form the store. The shared features includes simple information like user name to extended properties like activities performed, stories published, location, personal likes etc.

2.5 IPFS

Interplanetary File System (IPFS) is a versioned record system that stores files and related path information along with version information over time(Chen et al. 2017). This distributed file system defines a methodology that could be adopted for converting a file content to a distributed format and managing its distributions in a networked environment(Giang Do and Ng, 2017). IPFS combines these two properties and enables a new web that is permanent and augments the existing internet protocols. IPFS requests are structurally similar to http requests with prefix ipfs/ instead of http:/.

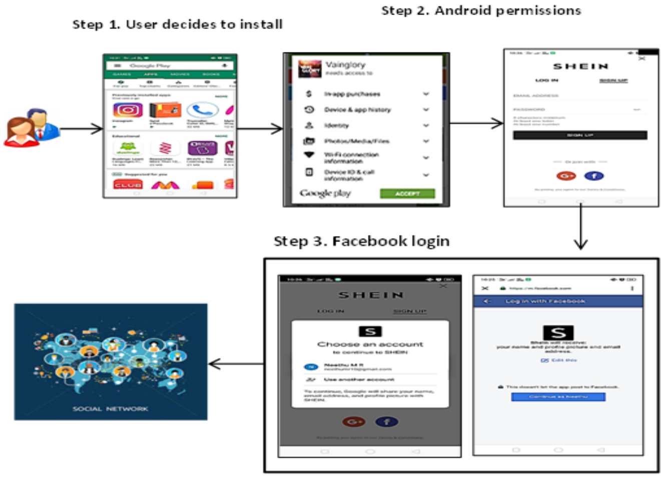


Fig. 2. Three step procedure for application installation

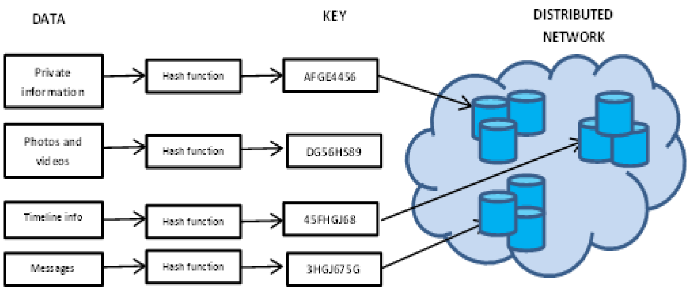


Fig. 3. *Hashing in IPFS*

IPFS facilitates content based search, similar to the access procedures used by associative memories. The output of applying a cryptographic hash function generally represents a root object using which other objects in its path can be found. The server in the network is eliminated and instead, direct access to the "starting point" of data is given to the user. The person who is close to user get direct communication with the user instead of routing through a central server. Distributed hash table with key/value pair is used to store information(Ali, Dolui, and Antonelli 2017). The hashed file is stored and is downloaded directly from the node. Similarly, if the private content of social media is stored in such a platform, only if the user has direct link with the third party websites (cryptographic key), the stored hash file of the personal information will be visible to the requestors, thus making security feature strong(Chen et al. 2017) (Giang Do and Ng 2017). The key IPFS components includes a data trading module responsible for managing efficient block distribution, a decentralized transparent key management system, a decentralized look up service that facilitates efficient retrieval of the value associated with the key and a directed graph whose nodes contain cryptographic hashes. IPFS uses a mathematical function SHA2 256(Gowthaman and Sumathi 2015) to condense data to a fixed size using a base58 multihash format. The result of encrypting the text "hello world" in this IPFS uses the procedure elaborated in algorithm A1(Rachmawati, Tarigan, and B C Ginting 2018).

A1 Algorithm for SHA 256:

```
              Input: attributes
              Output: message digest
              Initialization:
Step:   1.    M ← padded with bits
Step:   2.    Length(M) 448 modulo 512
Step:   3.    64-bit of Length(M) is appended to the result
Step:   4.    Final m is parsed to N 512 MESSAGE BLOCKS by appending 64-bit block.
Step:   5.    $H^{(0)}$,Initial hash value is set.
Step:   6.    Message schedule←      Sixty four 32 bit words. W0,W1,...W63
Step:   7.    Initialize Eight working variables (p,q,r,s,t,u,v,w) with the (j-1)th hash value.
                  For i=0 to 53:
              {
              $T_1 = w + \sum_{1}^{256} t + ch(t,u,v) + K_1^{256} + W_i$
              $T_2 = \sum_{0}^{256} p + Maj(p,q,r)$
              W=V; V=U; U=T; T=s+$T_1$; S=R; C=Q; Q=P; P=$T_1$+$T_2$
              }
              Where:
              $\sum_{1}^{256} t = (t\ ROTR\ 6) \oplus (t\ ROTR\ 11) \oplus (t\ ROTR\ 25)$
              $\sum_{0}^{256} p = (t\ ROTR\ 2) \oplus (t\ ROTR\ 13) \oplus (t\ ROTR\ 22)$
              $Ch(t,u,v) = (t \wedge u) \oplus (t \wedge v)$
Step:   8.    Output (Repeat steps 1 to 4, N times)
              $H_0^N \parallel H_1^N \parallel H_2^N H \parallel_3^N \parallel H_4^N \parallel H_5^N \parallel H_6^N \parallel H_7^N$
```

The obtained hash from the above procedure is then encoded with Base58 encoding as it makes the hash unreadable. Encoding eliminates redundancies thus preventing third parties access to data unless they breach the algorithm used. Multihash and Base58 encoding causes the output message digest be prefixed with Qm. (For eg: QmcaHpwn3bs9DaeLsrk9ZvVxVcKTPXVWiU1XdrGNW9hpi3) Block distribution in IPFS is performed using a bittorrent inspired protocol: Bitswap(Chen et al.2017). It operates as market place with a notion of barter system. Bitswap nodes have to provide keys in exchange for the data. This exchange of keys between the peers is for a particular period of time until the connection between the two closes. This can be done from any side. Bitswap helps in the decentralized transparent key management for IPFS.Merkle DAG , a combination of Merkle tree and Directed Acyclic Graph,ensures the exchange of data blocks in the network of peers without any alteration, damages or corrections. For this, cryptographic hashes are used. Also versioned File system is also incorporated with IPFS as it is the strongest feature of merkle DAG, and helps for permanent storage of data in IPFS. In summary, IPFS is a self-certifying file system based on public key cryptography for secured exchange of data. OpenPGP encryption standard is used for this purpose in the system. Kleopatra, used in the system that enables openPGP encryption for files.

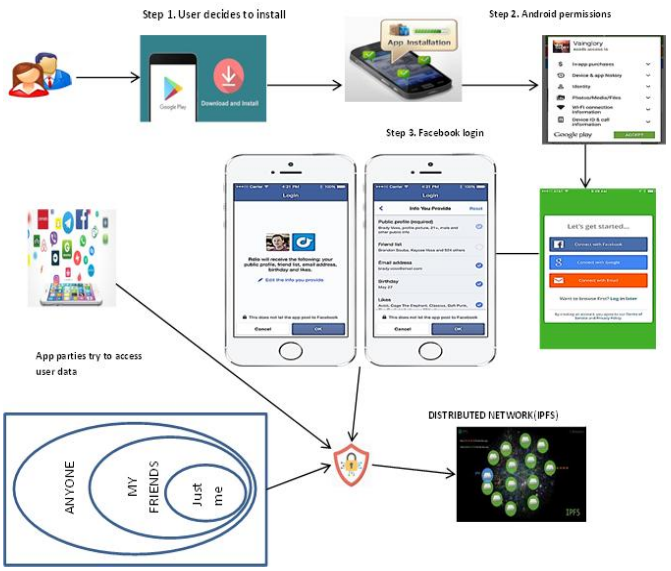


Fig. 4. *Framework for proposed architecture*

3 PROPOSED ARCHITECTURE

It is a common procedure to allow users install applications from app store by verifying his/her credentials using the details provided from their existing personal accounts with sites like Google, Facebook etc. Most of the users ignore to read terms and conditions related to privacy preservation policies , thus granting full access rights on personal information to third parties. The newly installed application gains access to the profile information of the user(Golbeck and Mauriello 2016). If the information in these accounts is stored in a protected way, it is clear that only those who possess authentication tokens can gain access to profile information. The work (Figure 4) proposes a scheme to enhance privacy preservation in which the profile information of the user in social networks is stored securely in IPFS and reveal based on the key value. A centralized Certificate Authority is responsible for managing and distributing the keys. Certificate Authority distributes the key to the other connects of the user in social network depending on the metrics (reliability, credibility and trust score) computed and stored by trust manager component. The certificate Authority classifies the user into three groups namely close friends, friends and public. Calculation of the mentioned metrics is based on factors like user's total number of transactions in Social Networking Sites, classification and tone analysis on shared posts(M.Neethu and Harini 2018) (M. R. Neethu and N. Harini 2018).. The system classifies all the profile information associated with the user as public and private.The private information is stored in IPFS and given access only to those in possession of the right key value. A detailed experimentation process was carried out to collect profile information of users from social networks, categorize peers based on their sensitivity and store them in distributed ledger. The procedure also included creating sub groups of profile information, generating message digest and encrypting them using public key cryptosystem. These generated keys for different subgroups are managed and distributed by a centralized CA. The usage of the keys to obtain information prevents the leakage of private information of users profile to any third parties, knowingly/unknowingly linked with the user profile.

4 RESULTS AND DISCUSSIONS

A rigorous procedure was adopted to collect data from social network. Data collected from the social network included the following 42 attributes: Comments, Likes, Shares, Number of comments under an image, Comments under an image, Number of likes in an image, Friends phone number, Interests based on Facebook activity, Advertisers Who Uploaded a Contact List With Your Information, Advertisers whose ads you've clicked on Facebook, Pages that you are admin of, Photos and videos (you have posted), Posts : other people posts on your timeline, your posts, Profile information, Apps installed using Facebook credentials, Posts from the apps you've given permission to post on your behalf, Call logs: A log of calls made and received on your device that you've chosen to share in your device settings, Message logs:, Event log, Following, Friends: received, rejected, removed, sent, Groups: activity, posts and comments in group, Likes: pages , post and comments, Messages, Saved video, Search history, Security login information: IP Addresses, Other activity : pokes.

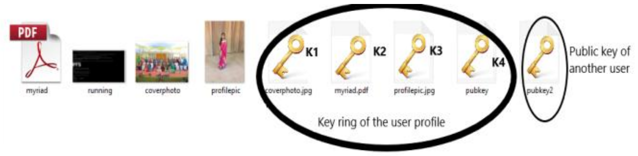
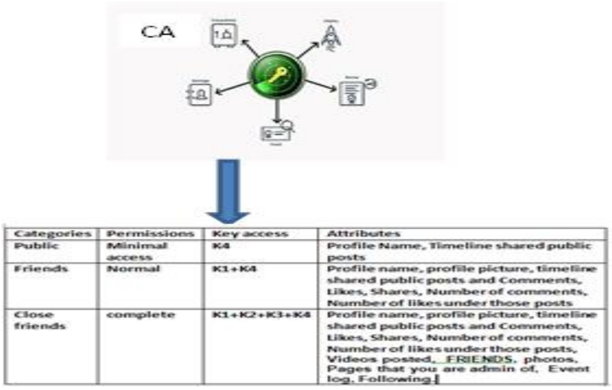


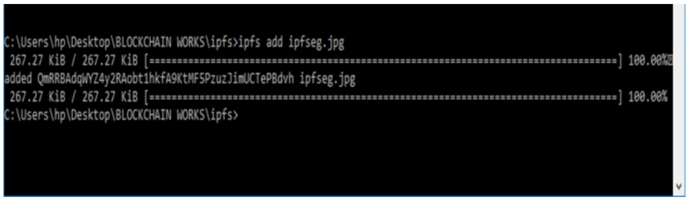
Fig. 5. *Requirements for GPG encryption*

These attributes are grouped based on their sensitivity and each subgroup is protected by a unique key. These keys are created, distributed and managed by the Certificate Authority. The other peers in the network on request would be provided by the key based on the trust score as computed by the trust manager component. The identified private information for experimentation included Profile information, saved video, Search history, Security login information: IP addresses, friends, photos and videos.The results of experimentation with respect to generation of key pairs, Message Digest of profile information and their storage in IPFS are depicted in Figures 5 to 11 . Figure 5 depicts the keys generated for a user profile in social network using gpg. Figure 6 shows the procedure for key distribution by the Certificate Authority. it is important to note that these keys serve as basis for gaining access to various private attribute associated with the user. Figure 7 and Figure 8 clearly show the process of storage and decryption in IPFS. The provision of right key results in successful decryption thus granting revelation of data to the requestor.



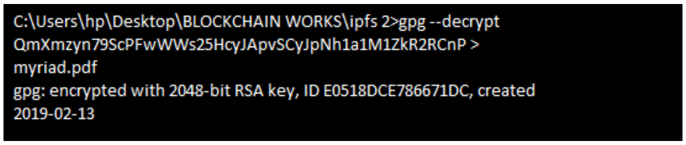
Categories	Permissions	Key access	Attributes
Public	Minimal access	K4	Profile Name, Timeline shared public posts
Friends	Normal	K1+K4	Profile name, profile picture, timeline shared public posts and Comments, Likes, Shares, Number of comments, Number of likes under those posts
Close friends	complete	K1+K2+K3+K4	Profile name, profile picture, timeline shared public posts and Comments, Likes, Shares, Number of comments, Number of likes under those posts, Videos posted, FRIENDS, photos, Pages that you are admin of, Event log, Following

Fig. 6*. Allocation of keys by Certificate authority.*



```
C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs>ipfs add ipfseg.jpg
 267.27 KiB / 267.27 KiB [================================================================================] 100.00%
added QmRRBAdqWYZ4y2RAobt1hkfA9KtMF5PzuzJimUCTePBdvh ipfseg.jpg
 267.27 KiB / 267.27 KiB [================================================================================] 100.00%
C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs>
```

Fig. 7*. Adding a file to distributed storage.*



```
C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs 2>gpg --decrypt
QmXmzyn79ScPFwWWs25HcyJApvSCyJpNh1a1M1ZkR2RCnP >
myriad.pdf
gpg: encrypted with 2048-bit RSA key, ID E0518DCE786671DC, created
2019-02-13
```

Fig. 8. *Decryption using key.*

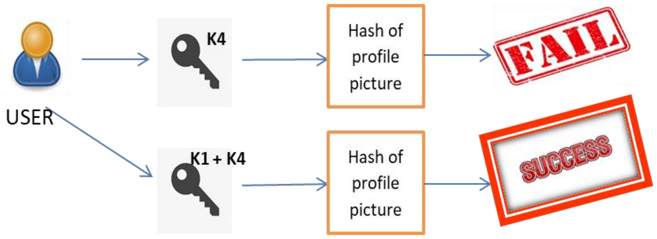
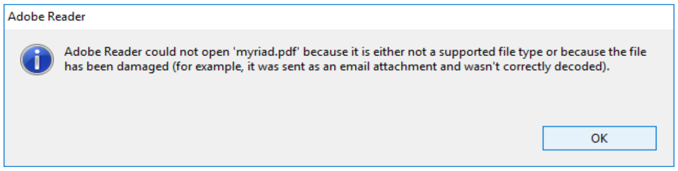


Fig. 9. *Success and Failure cases using different keys.*



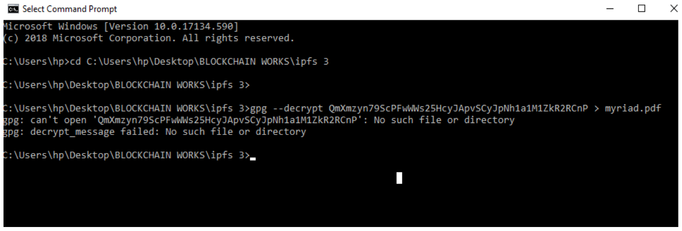
Adobe Reader could not open 'myriad.pdf' because it is either not a supported file type or because the file has been damaged (for example, it was sent as an email attachment and wasn't correctly decoded).

Fig. 10. *Failed case when peer don't have key.*

Failing to provide appropriate key leads to failure of decryption process which in turn restrict the revelation of selected attributes to the requestor. The failure scenario is depicted in Figure 9, 10 and 11. Figure 9 clearly imparts that a user will be able to view the private information only if a valid key is available with that peer. Otherwise the case fails and the peer is not given access to the information. K1 + K4, being the key for normal access, the user is able to view the profile image whereas the user with only K4 with minimal access permission fails to view the image. Figure 10 and 11 shows the failed cases with wrong key.

5 CONCLUSION

The popularity and the wide spread use of social networking sites for day today communication and the stories concerning the privacy and security issues of popular social media demands a special access control paradigm that preserves privacy of information. Although social networking sites offer access control mechanism that are typically coarse grained and binary visible. The present scenario demands a sophisticated access control mechanism that is fine grained and capable of offering wide range of access control abstractions. The work presented in this paper aims at providing a privacy model based on distributed storage mechanism and offering privacy preservation on profile item, posts and friendship articulation using IPFS. The results of the model carried out on privacy preservation strategy for restricting access to private data of the user by third parties particularly when a social account of the user is used to install an app in his/her mobile phone presented and discussed in section (4) confirms the efficiency of the proposed scheme in terms of privacy preservation (M. R.Neethu and N. Harini 2018).



```
Microsoft Windows [Version 10.0.17134.590]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\hp>cd C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs 3

C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs 3>

C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs 3>gpg --decrypt QmXmzyn79ScPFwWWs25HcyJApvSCyJpNh1a1M1ZkR2RCnP > myriad.pdf
gpg: can't open 'QmXmzyn79ScPFwWWs25HcyJApvSCyJpNh1a1M1ZkR2RCnP': No such file or directory
gpg: decrypt_message failed: No such file or directory

C:\Users\hp\Desktop\BLOCKCHAIN WORKS\ipfs 3>_
```

Fig. 11. *IPFS failure when user is not given access.*

5.1 Future direction: IPFS and Blockchain

The linking of IPFS with blockchain technology can be a better platform for storage as smart contracts can also be incorporated with the system. Incorporating blockchain would allow user to own and control his/her data in a better fashion. The decentralized nature of block chain allows user to store data in nodes and own them fully. The blockchain is integrated with self-executed and self-verified (Wang, Yinglong Zhang, and Yaling Zhang 2018) smart contracts(Feng et al. 2018). Smart contracts are written in solidity language which is a high level language that is influenced by C++, Javascript and Python(Kosba et al. 2016). IPFS utilize the concept "Distributed Hash Table" on Peer to Peer decentralized network similar to decentralization concept in blockchain. Blockchain combined with IPFS is expected to provide superfast, secure and unalterable transfer of data among nodes. Hence, as a future direction (Hao, Sun, and Luo 2018). to this work, it is planned to integrate a smart contract based trust model capable of working out trust relations and frame dynamic policies based on the score. So this is a very clear statement that, when one implement Blockchain with IPFS, then the transferring of data among nodes will be super-fast, secured, and unalterable (M. Neethu and Harini 2018).

6 REFERENCES

[1] Alalwan A., Rana N., Dwivedi Y., Algharabat R.: Social Media in Marketing: A Review and Analysis of the Existing Literature. In: Telematics and Informatics, 2017.

[2] Ali M.S.,Dolui K.,Antonelli F.:IoT data privacy via blockchains and IPFS.,2017.

[3] Alves H., Fernandes C., Raposo M.: Social Media Marketing: A Literature Review and Implications: IMPLICATIONS OF SOCIAL MEDIA MARKETING. In: Psychology Marketing, vol. 33, pp.1029-1038, 2016..

[4] Bahri L., Carminati B., Ferrari E.: Decentralized privacy preserving services for online social networks. In: Online Social Networks and Media, vol. 6, pp. 18–25, 2018.

[5] Benkhelifa R., Laallam F.Z.: Exploring demographic information in online social networks for improving content classification. In: Journal of King Saud University-Computer and Information Sciences, 2018.

[6] Chen Y., Li H., Li K., Zhang J.: An improved P2P file system scheme based on IPFS and Blockchain. In: 2017 IEEE International Conference on Big Data (Big Data), pp. 2652–2657. IEEE, 2017.

[7] De Salve A., Mori P., Ricci L.: A survey on privacy in decentralized online social networks. In: Computer Science Review, vol. 27, pp. 154–176, 2018.

[8] Feng Q., He D., Zeadally S., Khan M.K., Kumar N.: A survey on privacy protection in blockchain system. In: Journal of Network and Computer Applications, 2018.

[9] Giang Do H., Ng W.K.: Blockchain-Based System for Secure Data Storage with Private Keyword Search. pp. 90–93.2017.

[10] Godey B., Manthiou A., Pederzoli D., Rokka J., Aiello G., Donvito R., Singh R.: Social media marketing efforts of luxury brands: Influence on brand equity and consumer behavior. In: Journal of Business Research, vol. 69, 2016.

[11] Golbeck J., Mauriello M.: User perception of Facebook app data access: A comparison of methods and privacy concerns. In: Future Internet, vol. 8(2), p. 9, 2016.

[12] Gowthaman A., Sumathi M.: Performance Study of Enhanced SHA-256 Algorithm.In: International Journal of Applied Engineering Research, vol. 10(4), pp.10921–10932, 2015.

[13] Hao J., Sun Y., Luo H.: A Safe and Efficient Storage Scheme Based on BlockChain and IPFS for Agricultural Products Tracking. In: Journal of Computers, vol. 29(6), pp. 158–167, 2018.

[14] Kosba A., Miller A., Shi E., Wen Z., Papamanthou C.: Hawk: The blockchain model of cryptography and privacy preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP), pp. 839–858. IEEE, 2016.

[15] Neethu M., Harini N.: Safe sonet: A framework for building trustworthy relationships. In: International Journal of Engineering Technology, vol. 7, p. 57, 2018.

[16] Neethu M.R., Harini N.: Securing Image Posts in Social Networking Sites. In: D.J. Hemanth, S. Smys, eds., Computational Vision and Bio Inspired Computing, pp. 79–91. Springer International Publishing, Cham, 2018.

[17] Rachmawati D., Tarigan J., B C Ginting A.: A comparative study of Message Digest 5(MD5) and SHA256 algorithm. In: Journal of Physics: Conference Series,vol. 978, p. 012116, 2018.

[18] Rathore S., Sharma P.K., Loia V., Jeong Y.S., Park J.H.: Social network security: Issues, challenges, threats, and solutions. In: Information sciences, vol. 421, pp. 43–69, 2017.

[19] Wang S., Zhang Y., Zhang Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. In: IEEE Access, vol. 6, pp. 38437–38450, 2018.