ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 2, January 2018

CLUSTERING BASED APPROACH USING FINGERPRINT AUTHENTICATION FOR IDENTIFYING FAKE PROFILES IN ONLINE SOCIAL NETWORKS

Dr.M. Geetha[1], Raymond.M[2], Sabareesh.A[3], Rohit.J[4], Raghavendar.S[5]
[1]geetha.m@ritchennai.edu.in , [2]raymond7in@gmail.com , [3]sabareeshvijay07@gmail.com ,
[4]j.rohit.mail@gmail.com , [5]raghathelion@gmail.com
[1]Prof, Department of Computer Science and Engineering,
[2.3.4.5]UG Scholar, Department of Computer Science and Engineering,
Rajalakshmi Institute of Technology.

Abstract: Cybercrime attacks have become a major problem in online social networks. Many mechanisms have been developed in providing network security to the social network users. But the advancements made in providing network security has considerable drawbacks in certain cases that includes security to user data, authentication methods like Password recognition, OTP methods, secured URL login had not provided maximum level of security. This paper mainly focuses the ways to overcome the cybercrime attacks on social networks with a view of providing a better method for the usage of online social networks. New mechanisms have been proposed in this project with the view of providing a secured way of authentication through biometrics, and data security to users.

This paper also focuses in providing secured storage space for user data in cloud which has become prone to intruders. This helps in accessing the account securely from anywhere and anytime across the world. Finally, this paper provides the properties of the existing projects, their drawbacks and the enhancements to be made for the existing projects.

Keywords: Fingerprint Authentication, Cloud Security, Data Mobility, Online Social Networks.

I INTRODUCTION

In recent years internet has grown into a wide ocean of information, some crucial and important. Cyber security has become more reliable since cybercrimes has also been increased. Cybercrimes like cyber bullying and spam messages that can act as a pipeline to send ransom wares or other such malwares that can defect, steal or even destroy a user's device. The level of Data Security has also become a threat due to the increased cybercrime activities. Encrypting the data at backend cloud servers by providing a low-level of authentication cannot provide much security to the data. So, to hopefully remove such crimes from internet, the project has been developed to decrease both

Even though illegal, this kind of feature helps in providing maximum security because online social networks have become a tool for all virtual and real-time crimes. Initially all users are in need of an online social network, which is user friendly and more secured. In the view of providing these features as an inbuilt feature for all the social networks, we have enhanced the networks with an additional layer in signing up and logging up process.

Fingerprint Authentication layer becomes the most preferred and an important layer of security for accessing the account. For signing up the account the fingerprint of the user gets recorded and will be cross checked with the existing fingerprints in the database. Identical Fingerprints will all the basic information of the user will be backtracked without the user knowledge when the user tried to duplicate the account.

the terrorists. So, this helps in analysing the user activities and identifying anything different apart from the actual activities.

II MOVING TOWARDS BIOMETRICS

Adding fingerprint authentication to your project is a multi-step process, so to help you decide whether it's worth the initial time and effort, let's look at some of the ways in which fingerprint authentication can improve the user experience:

It's a quick and convenient way of authenticating the user's identity. While a traditional PIN, pattern or password is an effective security feature, there's no denying that requiring the user to input a password does add some friction to the user experience. Touching your fingertip to a sensor is far easier than entering a PIN, pattern or password, making fingerprint authentication an effective way of striking a balance between keeping your users safe and providing a frictionless user experience. Major advantages of using Biometrics are,

1) **You can't forget a fingerprint!** Most of us have a long list of passwords we need to remember on a day-to-day basis. Plus, if you follow best practices for creating secure passwords (never use the same password more than once; always use a combination of symbols, numbers, plus upper and lowercase characters) then chances are these passwords aren't particularly easy to remember! Fingerprint authentication can provide your users with all the security of a password, without actually adding to the list of passwords they need to remember on a day-to-day basis.
2) **No more struggling with mobile keyboards.** Not only are long, complex passwords difficult to remember, they're also difficult to type on the smaller screen of a mobile device. Even if your app only requests the user's password once per session, navigating the awkward mobile keyboard can make this feel like one time too many. Also, consider that many mobile users interact with their apps on the go – and no-one wants to be messing around trying to type out a long, complex password when they're stood up on a busy commuter bus! Fingerprint authentication gives users a way of confirming their identity without them having to go anywhere *near* the mobile keyboard.
3) **No more annoying password recovery or reset.** There's never a good time to forget your password, but forgetting a password for a mobile app can be particularly painful as users tend to interact with mobile apps on the go. If you're out and about then the *last* thing you want to do is sit down and navigate an app's password recovery or reset procedure. By adding fingerprint authentication to your app, you can ensure that your users never have to see your app's password recovery or reset screens again.
4) **Your fingerprint is unique and impossible to guess.** Even if your users follow best practices for creating a secure password, there's no guarantee that someone won't be able to guess their password anyway, or even manipulate the user's device into leaking their password via tools such as spyware. While nothing is ever 100% secure, a fingerprint cannot be guessed or stolen in the same way a password can.

III CATEGORISING PEOPLE USING OSN:

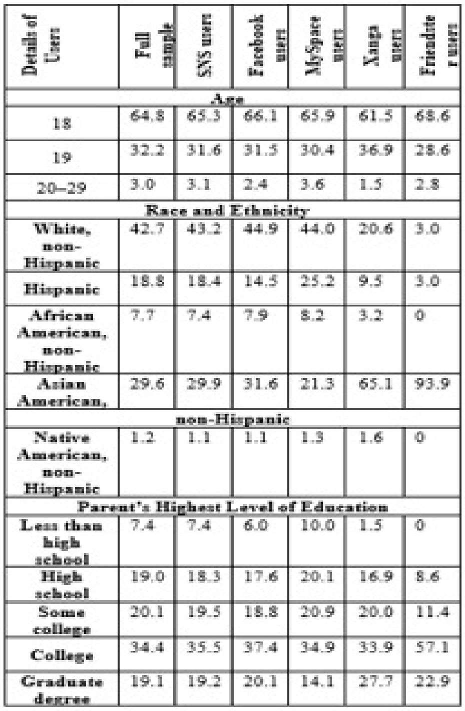
Network Security can be achieved to the fuller extent only when we are able to categorise people using OSN among various sectors and circumstances. Since the project involves in analysing and tracking all user activities, it is mandatory for to categorise all sectors of people.

A detailed study has been made by Ezster Hargittai published on October 2007 categorising all the users may or may not using OSN for an year. The way of categorisation is done by using the following features,

1) Differences in Social Network Site Usage

People who uses SNSs, and are different students equally likely to use the various services available in this realm? The survey included questions about six SNSs: Bebo, Facebook, Friendster, MySpace, Orkut, and Xanga. For each, respondents were first asked to report whether they had ever heard of the site. Next, they were asked to indicate their experiences with it, using the following options: “no, have never used it,” tried it once, but have not used it since,” yes, have tried it in the past, but do not use it nowadays,” yes, currently use it sometimes,” and “yes, currently use it often.” Overall, 88% of respondents are SNS users, and 74% report using at least one SNS often. Only one student claims not to have heard of any of the six SNSs included on the survey, so non-use is not a result of not being familiar with these services. Rather, despite knowing about such sites, over 12% of the sample does not use any of them.

Table 1 shows the proportion of SNS users by specific site.

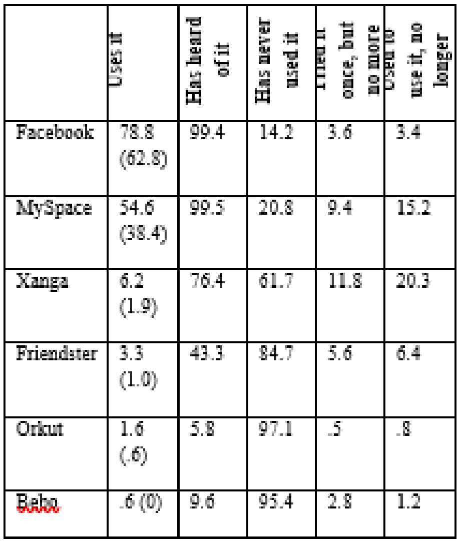


Details of Users	Full sample	SNS users	Facebook users	MySpace users	Xanga users	Friendste r users
Age						
18	64.8	65.3	66.1	65.9	61.5	68.6
19	32.2	31.6	31.5	30.4	36.9	28.6
20–29	3.0	3.1	2.4	3.6	1.5	2.8
Race and Ethnicity						
White, non-Hispanic	42.7	43.2	44.9	44.0	20.6	3.0
Hispanic	18.8	18.4	14.5	25.2	9.5	3.0
African American, non-Hispanic	7.7	7.4	7.9	8.2	3.2	0
Asian American,	29.6	29.9	31.6	21.3	65.1	93.9
non-Hispanic						
Native American, non-Hispanic	1.2	1.1	1.1	1.3	1.6	0
Parent's Highest Level of Education						
Less than high school	7.4	7.4	6.0	10.0	1.5	0
High school	19.0	18.3	17.6	20.1	16.9	8.6
Some college	20.1	19.5	18.8	20.9	20.0	11.4
College	34.4	35.5	37.4	34.9	33.9	57.1
Graduate degree	19.1	19.2	20.1	14.1	27.7	22.9

Table 1 shows the proportion of SNS users by specific site. Facebook is the most popular service among these students, with almost four in five using it, and over half of the overall sample doing so frequently. MySpace is used by more than half of the sample, although just over one-third uses it often. The other four sites (Xanga, Friendster, Orkut, and Bebo, in that order of popularity) are significantly less widespread in this group, with each used by less than 10% of the sample.

2) Categorising users by Social Networks:

Table 2: Descriptive statistics for the sample demographics (percentages).



	Uses it	Has heard of it	Has never used it	Tried it once, but no more	Used to use it, no longer
Facebook	78.8 (62.8)	99.4	14.2	3.6	3.4
MySpace	54.6 (38.4)	99.5	20.8	9.4	15.2
Xanga	6.2 (1.9)	76.4	61.7	11.8	20.3
Friendster	3.3 (1.0)	43.3	84.7	5.6	6.4
Orkut	1.6 (.6)	5.8	97.1	.5	.8
Bebo	.6 (0)	9.6	95.4	2.8	1.2

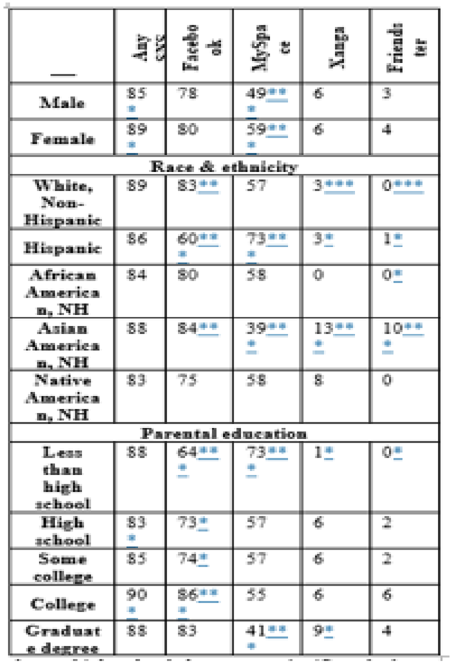
Table 2 reports the demographic breakdown of SNS users, first in the aggregate (second column) and then by site (columns 3–6). Orkut and Bebo are excluded from the table due to their extremely low levels of use in this group.

The differences among the user populations of these services are not particularly pronounced on most variables. Some trends, nonetheless, are notable. First, the percentage of Asian/Asian American users fluctuates considerably, depending on the service. In particular, Asian/Asian American students in the sample are least represented on MySpace, whereas Xanga and Friendster are especially popular with this group. Second, students of Hispanic origin make up a considerably larger segment of MySpace users than their representation in the sample as a whole. Third, there is a relationship between parental education and use of some SNSs. In particular, students who have at least one parent with a graduate degree are more represented on Facebook, Xanga, and Friendster than they are in the aggregate sample, while students whose parents have less than a high school education are disproportionately users of MySpace. This rather simple look at the data shows that social network site usage in the aggregate attracts a diverse set of students across services, but that certain groups are more represented on some sites than others. The important methodological take-away point here—in addition to the substantive ones about specific groups of users—is that when studying users of one SNS, researchers should exercise caution in generalizing the findings to users of another social network site.

3) Probability of User Activities:

Another way to look at the data is to consider the levels of SNS popularity by type of user attribute.

Table 3 Percentage of different groups of people who use any SNS and specific social network sites



—	Any SNS	Facebook	MySpace	Xanga	Friendster
Male	85*	78	49***	6	3
Female	89*	80	59***	6	4
Race & ethnicity					
White, Non-Hispanic	89	83**	57	3***	0***
Hispanic	86	60***	73***	3*	1*
African American, NH	84	80	58	0	0*
Asian American, NH	88	84**	39***	13***	10***
Native American, NH	83	75	58	8	0
Parental education					
Less than high school	88	64***	73***	1*	0*
High school	83*	73*	57	6	2
Some college	85	74*	57	6	2
College	90*	86***	55	6	6
Graduate degree	88	83	41***	9*	4

Table 3 shows significant differences according to type of user. When it comes to aggregate SNS usage, women are more likely to use such services than are men, but once disaggregated by type of site, depending on the service, the differences all but disappear. That is, while female students in the sample are much more likely to use MySpace, there is little difference between young women and young men in the group when it comes to Facebook, Xanga, or Friendster use.

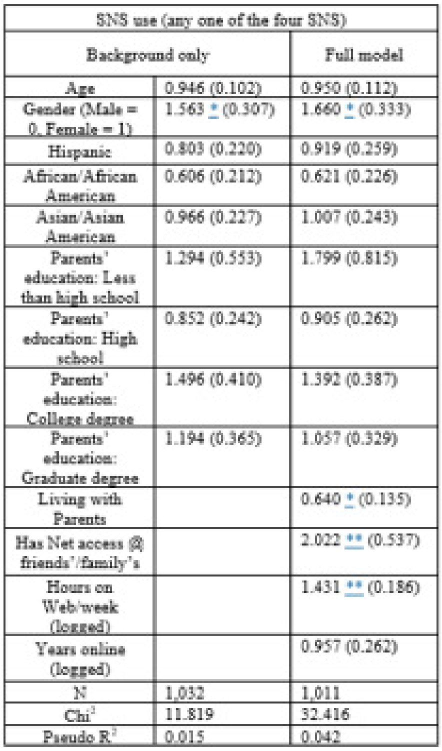
Regarding race and ethnicity, the most pronounced findings concern students of Hispanic and Asian origin. Hispanic students are significantly less likely to use Facebook (60% compared to 75% or more for other groups), whereas they are much more likely than others to use MySpace (73% among Hispanic students compared to 58% or less among all others). In contrast, like White students, Asian and Asian American students are much more likely to use Facebook than others, but they are significantly less likely to use MySpace. Additionally, this group of students is especially active on Xanga and Friendster compared to others.

There are also significant differences according to parents' level of education. The most pronouncedfinding is that students whose parents have less than a high school degree are significantly less likely to be on Facebook and are significantly more likely to be MySpace users. In contrast, those who have at least one parent with acollege education are significantly more likely to be Facebook users, while those who have at least one parent with a graduate degree are considerably less likely to spend time on MySpace. Xanga also seems to appeal more to those whose parents have higher levels of education. However, since there is a relationship between parental education and a student's race and ethnicity, it is best to look at these associations using more advanced statistical techniques that allow other factors to be controlled while the relationship between the various background variables and SNS usage is examined. The next section does this by considering what predicts SNS use on the whole and with regard to specific sites when controlling for other factors in the model.

4) Explaining Any SNS Use

The findings presented in Table 4 suggest that numerous factors influence whether a student uses social network sites, while the results in Table 5 suggest that the predictors are not uniform across different services. The figures presented in both tables are "odds ratios," meaning that any number greater than 1 constitutes a higher propensity to engage in SNS usage, whereas a number less than 1 suggests that the type of characteristic lowers the likelihood of social network site usage. First, I consider the findings for overall SNS usage, followed by an examination of specific site uses separately.

Table 4. Results of logistic regression analyses explaining SNS use (standard errors in parentheses)



SNS use (any one of the four SNS)		
Background only		Full model
Age	0.946 (0.102)	0.950 (0.112)
Gender (Male = 0, Female = 1)	1.563 * (0.307)	1.660 * (0.333)
Hispanic	0.803 (0.220)	0.919 (0.259)
African/African American	0.606 (0.212)	0.621 (0.226)
Asian/Asian American	0.966 (0.227)	1.007 (0.243)
Parents' education: Less than high school	1.294 (0.553)	1.799 (0.815)
Parents' education: High school	0.852 (0.242)	0.905 (0.262)
Parents' education: College degree	1.496 (0.410)	1.392 (0.387)
Parents' education: Graduate degree	1.194 (0.365)	1.057 (0.329)
Living with Parents		0.640 * (0.135)
Has Net access @ friends'/family's		2.022 ** (0.537)
Hours on Web/week (logged)		1.431 ** (0.186)
Years online (logged)		0.957 (0.262)
N	1,032	1,011
Chi^2	11.819	32.416
Pseudo R^2	0.015	0.042

IV LITERATUE SURVEY:

Some views of authors undergoing similar projects are,

A technique suggested by Aditi et al. [1] for detecting fake accounts in a social network is by using user given data and analysing the data with facts for real and fake accounts. It employs the use of classifiers, 12 classifiers employed for detection. The efficiency of the proposed model is only 78%, as given by the author. But this model does not satisfy the privacy rules of a social network, thus it becomes a major drawback. This work can only be applied if the user of a social network accepts in sharing data.

According to Pietro et al. [14], cloud computing needs to be secure for data privacy and protection in personal data. And it's a major challenge for securing data in cloud services. So the use of biometrics authentication, such as fingerprint authentication, is used for better security. But for using biometrics data for logical access to IT services, is a more challenging and

Farzam Kharaji et al. [5], suggested that for a biometric authentication, the inner knuckle print recognition is used. The inner knuckle print

still an unsolved problem. Yet using biometrics authentication for securing cloud services is more effective in security and is being adopted widely.

Shan-Hung Wu et al. [18] proposed a technique to solve identity fraud in Social Networking Services (SNSs), which is to extend the use of continuous authentication to detect the in-situ identity fraud incidents, which occurs when the attackers use the same accounts, the same devices, and IP addresses as the victims. The proposed model has proven that it is possible to detect such incidents by analysing SNS users' browsing behaviour. The detection accuracy is 80% after 2 minutes and 90% after 7 minutes. One more drawback of the model is that it uses continuous authentication and is behavioural driven model, i.e., the data is formed according to the user's behaviour.

Cloud security is one of the main issues in cloud computing, open and distributed architecture as well as internet access, have caused cloud environments to be risky and vulnerable. Privacy, confidentiality, and authentication are some of security concerns which need to be addressed. Hamid Roomi et al. [9] adopted a technique using Kerberos 5 protocol that is one of the best-known authentication and key distribution systems. Further the Kerberos 5 is improved by using Strong Diffi-Hellman-DSA key exchange algorithm and the user's fingerprint samples.

In reference to Muhammad Yaasir et al. [12], it is concluded that biometric authentication is widely used for cloud services as security measures. Even though there are areas which biometrics method provides benefits, it is at risk of attacks. The model uses B.O.X (Biometrics Operational Security-X), which is created as the application interface and GrFinger, which is a recognized SDK for fingerprint implementation. Cancellable Biometrics increases the confidence in biometric authentication devices. The technology permanently shields biometric templates versus unauthorized access or perhaps disclosure by providing biometric comparisons within the encrypted domain. It also ensures the conservation of privacy regarding biometric characteristics.

is one of the reliable physiological characteristics among different approaches that exist in biometrics. In this model, the image of the inner surface of the middle and ring fingers are used for human verification. Considering the inner knuckle print as a texture two types of feature extraction methods are applied, namely Gabor wavelet filters and wavelet energy. Among all feature that is extracted by these approaches, fifty superior features selected by the forward feature selection algorithm.

A technique proposed by Feng Fujun et al. [6] for Identity Authentication System Based on Fingerprint Recognition and Cryptography is well used and secure. The model uses MD5 algorithm to encrypt and decrypt the user's data and fingerprint. Fingerprints as one of the biological properties can uniquely authenticate the identity of a "person". For balancing the restrictions of FRR and FAR, the username/password is encrypted with MD5, and a double identity authentication system based on fingerprint recognition and cryptography is proposed in this paper. The False Accepted Rate is 0% which means that the proposed model does identify illegal fingerprints. FRR denotes the false rejection rate which considers the same fingerprints to the different. Because the different outside conditions, the fingerprints become incomplete and fuzzy, which make the detecting fingerprints not match to the registered ones.

Anshuman et al. [3] stated that using Elliptic Curve cryptography for encryption can secure the cloud against eavesdropping attacks. As it is based on Elliptic Curve Cryptography, subsequent results obtained show that it reduces the computational overhead incurred in the encryption of data. The performances of other traditional security scheme such as RSA are also compared with the proposed encryption scheme. It is observed that the proposed scheme outperforms the other schemes in terms of the chosen performance characteristics. The results show that ECC is a light weighted and effective method for encryption in cloud than RSA encryption scheme.

Even though ECC provides more security than RSA Cryptography scheme in cloud security, as proposed by George et al. [8], Enhanced RSA Algorithm with varying Key Sizes is also an effective cloud security method. The Key size can be varied to make the encryption process strong. Hence it is difficult for the attackers to intrude the data. Increasing key size correspondingly increases the time taken for encryption and decryption process. The proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size. This strength paves the way to store data in cloud by the users without any inconvenience. The usage of prime numbers instead of random numbers in the proposed system improves the speed of encryption and decryption. Apart from increasing the speed, the implementation of ERSA algorithm also makes the computation complex one and increases the strength of security. In future, the time spent for encryption and decryption can still be improved by using the concept of Addition chaining.

According to Ahmed Abouollo et al. [2], we can identify fake accounts in a social website using HTML Canvas fingerprint. The model demonstrates how the "<canvas>" HTML tag can be used to draw some text and obtain fingerprints which are used later as a detection mechanism of fake accounts by checking whether the fingerprint created at the registration time and stored in the database matches any of the fingerprints created at the registration of other accounts, and then raising a flag to online social network operators to investigate further. This technique showed to be effective as long as the user uses the same browser, which limits the user's ability to create accounts more than the number of browsers installed in the device before getting detected. In our experiment, 6.67% of the raised flags were false positives, whereas 7.44 were missed flags. The Index of Similarity, a score that is calculated to represent the extent to which two accounts could belong to the same person. This model is more effective since it can be combined or adopted for future models in network security.

TABLE 5 : Provides the conclusions made from the survey.

Algorithm/Techniques Used	**Authentication**		**Data security (Data mobility provided)**	**Level of efficiency achiev**		**Advantages**	**Limitations/ Future Implementations**
	Network Security provided	**Biometrics used**		**Response Level***	**Complexity***		
Gathering user feed and evaluation using **Learning Classifiers [1]**	Fake user accounts are found in Online Social Networks(OSN)	×	×	L	M	Identifies fake users by just using user's activities	The efficiency is 78% and employs a minimum of 12 classifiers. Privacy policy is also affected.
Biometrics is obtained by a model using **Scale Invariant Feature Transform(SIFT)** [14]	Biometrics security for cloud services	✓	×	M	L	Every individual has unique fingerprint	Fingerprint authentication is complicated and can also be encrypted for better security.
Behavioural patterns are found using **Role-Driven Behavioural Diversity [18]**	Identity Fraud in social networks are found using behavioural patterns	×	×	M	H	Accuracy is more than 80% within 2 minutes of surfing	Cannot be applicable if the attackers can change their IP address frequently
Cloud Computing Authentication Using **Biometric-Kerberos** scheme based on **Strong Diffi-Hellman-DSA Key Exchange [9]**	Cloud security further using Kerberos 5 and Strong Diffi Hellman DSA with user's fingerprint	✓	×	M	H	Strong Diffi-HellmanDSA Key Exchange overcomes the vulnerability in Kerberos 5 protocol	Multiple fuzzy vaults are constructed for one fingerprint, which is a limitation for large number of users
Biometrics Operational Security-X, GrFinger is a recognized SDK for fingerprint Implementation [12]	Cancellable Biometric Authentication in Cloud computing	✓	×	H	H	Cancellable Biometrics increases the confidence in biometric authentication devices	More common use of biometrics can often be considered as a threat to level of privacy
Extraction methods, **Gabor wavelet filters and wavelet energy** are used [5]	Network security can be enhanced using inner knuckle print authentication	✓	×	L	L	Human finger inner print is used as biometric characteristic for verification	Such biometric authentication can be used for several security services, like network security

Cryptography method: **MD-5**, Algorithms: **FRR, FAR, ERR [6]**	User's identification using fingerprint authentication and encryption using MD5	✓	×	H	H	Uses double authentication, which includes username/password and fingerprint recognition.	Even though it secure and strongly reliable, the time taken is more for a single user
It is based on **Elliptic Curve Cryptography [3]**	ECC based encryption scheme for securing the cloud against eavesdropping attacks	×	×	H	M	ECC is way better than Traditional security schemes like RSA	It can be further Utilized for larger number of users in Cloud Computing
Enhanced RSA Algorithm with varying Key sizes for Data Security [8]	Cloud Security using ERSA with varying Key sizes	×	×	H	M	ERSA key algorithm uses two different keys for encryption and decryption processes.	Dividing the file into several blocks for large number of users in difficult
HTML Canvas Fingerprint to identify what accounts belong to the same person or entity [2]	Fake accounts in Social Networks can be found using HTML Canvas Fingerprint	✓	×	L	L	Web tracking method such as Canvas Fingerprinting are the most recent and effective method used	6.67% of the raised flags were false positives, whereas 7.44 were missed flags

LOW (L) : 0 - 40 %, MEDIUM(M) : 41 - 70%, HIGH (H) : 71 - 100%

V OBSERVATIONS MADE FROM TABLE 5:

Even though the projects discussed satisfies some factors in network security, it does not come across all lines of security mechanisms. The paper **Accessing Cloud Services through Biometrics Authentication** [14] has provided maximum level of security for securing cloud data, but it does not relate with the Online Social Networks. So, integrating Biometrics as a step for authentication and for accessing user data is the major factor to be enhanced.

1) PROVIDINGMOBILITY TO DATA BETWEENDIFFERENT CLOUD STORAGES:

Since all the user data are stored on a stable cloud storage, identifying the cloud's IP address and the database location becomes extremely hard for the intruders from being accessing the user data. Even-though this kind of process takes large workload and processing, this helps in ensuring better security of the personal data.

Mobility between the cloud storages can be achieved by many third-party applications in case of our project (Eg. MultCloud). Moving to the implementation of this project into all the social network applications, these third-party apps will never come into play. This is because all these social applications will be having their cloud storages and databases separately for their personalised use. So, mobility of data between the databases and cloud storage will become easier for these kinds of applications.

2) ACHIEVING DATA MOBILITY:

Providing a routine check of these user data helps in making sure that they do not follow a regular chain of mobility. This can be achieved by providing an algorithmic pattern of mobility to the data. Comparing to the past developments that had been made, the mobility will follow a sequential pattern or a pattern that is easy to track and find. But this kind of pattern will also make the task harder for intruders from being accessing the data. Allowing the data to freely move between the cloud following a timely basis and algorithmic nature of movement between the database will help in ensuring that the data was not stable at a particular cloud or database. Once the data is moved to another cloud, the cloud which previously had the data will be filled with some other data from other databases.

VI CONCLUSION:

Online Social Networks are widely used Public platform, where users communicate with each other. The threats faced by OSN users have increased in the recent years; this is due to more users joining an OSN. When an OSN becomes widely popular and is used by millions of users, it becomes a victim to cybercrime. Even though much advancement have been done for achieving network security, they do not provide more secured way of authentication and storing user data.

In the proposed paper, the user's details and fingerprint are encrypted using Cryptographic methods and stored in cloud storages, which are not publicly accessible. The model doesn't introduce new strategies for Network security, rather it enhances the security by introducing biometric authentication in Network Security. Using biometrics rather than behavioural patterns we can obtain a more relevant and precise observation if the user is a bot or not. It also helps to identify Identity Theft and Fraud Users. Another metric of the model, is that we can keep track of users and easily identify any threats committed by a user. So hopefully this provides maximum level of network security for users.

VII REFERENCES:

[1] Aditi Gupta and Rishabh Kaushal"**Towards Detecting Fake User Accounts in Facebook**", Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India,2017.

[2]Ahmed Abouollo, Sultan Almuhammadi"**Detecting Malicious User Accounts Using Canvas Fingerprint**"College of Computer Science and Engineering King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia, 2017.

[3] Anshuman Chhabra and Shivam Arora"**An Elliptic Curve Cryptography based Encryption Scheme for securing the Cloud against Eavesdropping Attacks**",Division of ECE, Netaji Subhas Institute of Technology, University of Delhi, India,2016.

[4] Anil K. Jain, Arun Ross and Salil Prabhakar, "**An Introduction to Biometric Recognition**",IEEE Transactions on circuits and

systems for video technology, VOL.14, NO.1, January 2004.

[5] Farzam Kharaji Nezhadian, Saeid Rashidi,]"**Inner-knuckle-print for human authentication by using ring and middle fingers**",Faculty of Biomedical EngineeringIslamic Azad University, Science and Research branch Tehran, Iran,2016.

[6]Feng Fujun, Li Xinshe,"**Design and Implementation of Identity Authentication System Based on Fingerprint Recognition and Cryptography**",Wang Litao Elementary Command CollegeRocket Force University of Engineering Xi'an, China,2016.

[9] Hamid Roomi Talkhaby, Department of Computer Engineering Amirkabir University of Technology Tehran, Reza Parsamehr, Department of Computer Science and Information Technology Institute of Advanced studies in Basic Science Zanjan,"**Cloud Computing Authentication Using Biometric-Kerberosscheme based on Strong DiffiHellman-DSA Key Exchange**", IRAN,2016.

[10] A.K. Jain, P. Flynn, and A.A.Ross, eds., "**Handbook of Biometrics**", Springer, 2007.

[11] H.C.Lee and R.E.Gaensslen. eds., "**Advances in Fringerprint Technology", **2nd., CRC press 2001.

[12] Muhammad Yaasir Khodabacchus, KrishnarajMadhavjee Sunjiv Soyjaudah,Gianeswar Ramsawok Faculty of Engineering University of Mauritius Reduit, Mauritius"**Fingerprint Code Authentication Protocol on Cloud", **2016.

[13] S. Pankanti, S. Prabhakar, and A.K. Jain, "**On the Individuality of Fingerprints**", IEEE Trans. Pattern Analysis and Machine Intelligence, Aug. 2002, pp.1010-1025.

[14] Pietro Ruiu*, Giuseppe Caragnano, Giovanni L. Masala†, Enrico Grosso†, *Istituto Superiore Mario Boella (ISMB), Torino, Italy † Department of Political Science, Communication, Engineering and Information Technologies Computer Vision Laboratory, University of Sassari, Sassari, ITALY,"**Accessing CloudServices through Biometrics Authentication**", 2016.

[15] Qing-Yun Li and Lei Zhang," The **Public Security and Personal Privacy Survey**" July/August 2016, 1540-7993/16/$33.00 © 2016 IEEE.

[16] A.A. Ross, K. Nandakumar, and A.K. Jain, "**Handbook of Multibiometrics**", Springer,2006.

[17] Rui LIU "**Chaos-Based Fingerprint Images Encryption Using Symmetric Cryptography**" 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012).

[18] Shan-Hung Wu, Man-Ju Chou, Chun-Hsiung Tseng, Yuh-Jye Lee, and Kuan-Ta Chen,"**Detecting In-Situ Identity Fraud on Social Network Services: A Case Study with Facebook**", Senior Member, IEEE,2015.

[19] TanishaAggarwal ,Dr.Chander Kant Verma, "**Fake Fingerprint Detection Methods**", IJITKMSpecial Issue (ICFTEM-2014) May 2014 pp. 61-69 (ISSN 0973-4414).

[20] Toshighige Shimamura, Hiroki Morimura, Nobuhiro Shimoya, Tomomi Sakata, Satoshi Shigematsu, Katsuyuki Machida Mamoru Nakanishi, "**A Fingerprint Sensor with Impedance Sensing for Fraud Detection**", Solid-State Circuits Conference, 2008. ISSCC 2008. Digest of Technical Papers. IEEE International.

[21] Walairach Nunsong, Kuntpong Woraratpanya" An **Improved Finger-Knuckle-Print Recognition Using Fractal Dimension Based on Gabor Wavelet**" 2016 13th International Joint Conference on Computer Science and Software Engineering (JCSSE).