I.J. Education and Management Engineering, **2018, 4, 50-60**
Published Online July 2018 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2018.04.05

Available online at http://www.mecs-press.net/ijeme

Threats, Consequences and Issues of Various Attacks on Online Social Networks

Gururaj H L[a], Swathi B H[b], Ramesh B[c]

[a]*Vidyavardhaka College of Engineering, Mysuru 570002,India*
[b]*Vidyavardhaka College of Engineering, Mysuru 570002,India*
[c]*Malnad College of Engineering, Hassan 573201,India*

Received: 06 December 2017; Accepted: 15 March 2018; Published: 08 July 2018

Abstract

Security is an important factor of life, which varies from home network to all aspects of our life. Data security is one of the challenges research areas where we can't provide 100% security for any data and network. Initially the data were secured with Passwords and extended up to biometrics, eventually attackers also becoming stronger to heal the data. In this paper critical review has been done starting from the passwords for securing data to various biometric methods. By using modern tool the data are securing using biometric methods.

Index Terms: Security, Biometric Recognition Systems, Finger Print Recognition System (FPRS), Face Recognition System(FRS), Palm Recognition System (PRS), Iris Recognition System (IRS), Voice Recognition System (VRS).

1. Introduction

Security is one of the prominent features for each aspect of day today life. If we want to keep the jewellers safe, we will keep in secret locker. This conventional method of securing has waved off because duplicate locker keys will be used to unlock it. After many decades, pin codes or passwords were emerged. These passwords are associated with each user and initially it was four letters alphabets or numbers. Later it was typically associated with a string of six to ten characters, a shared secret between the user and the machine. Each user is capable of committing to memory those who want keep the data safe and secure. There are certain rules bound to construct a password[3]. The length of the password should be minimum of eight characters and

* Corresponding author.
E-mail address:

maximum of twelve characters. These passwords should comprises of at least one uppercase, one numeric and one special character and that password should not be the username nor found in online. Moreover, users are restricted to change the password to lifetime of 30 to 90 days periodically. This process called password aging [2].

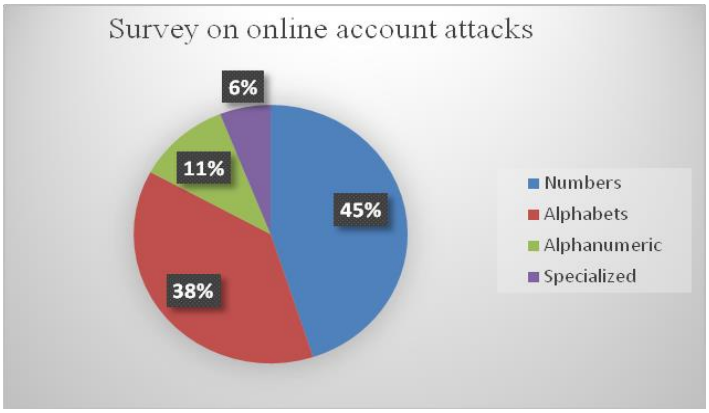

Fig.1. Survey on Online Account Attacks

There were many tools and mechanisms, which extract the passwords and these passwords, are vulnerable to brute force attack. Human intervention is not required for the password to check the legitimacy of a person [1]. To overcome this major pitfall biometric authentication mechanisms are on focus. According to the survey, online accounts are masquerade by interveners are analyzed as shown in the Fig. 1.

2. Biometric Recognition System

Providing authentication for an individual, Biometric Recognition outset its operation as depicted in Fig. 2. There are various biometric methods. They can be categorized into two main divisions

i. Physiological Biometric Recognition System (PBRS)
ii. Behavioural Biometric Recognition System (BBRS)

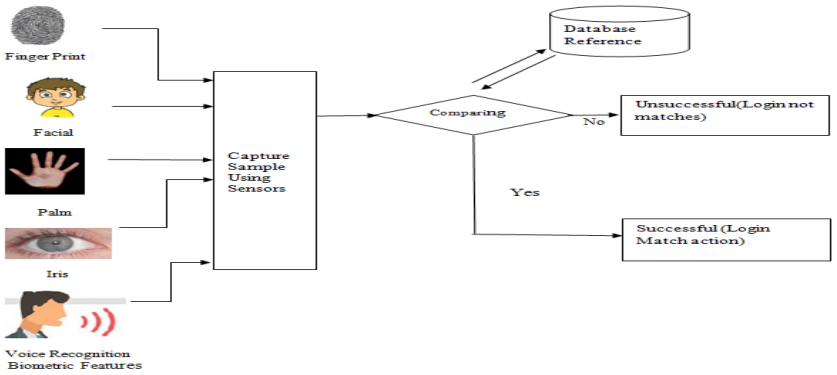

Fig.2. Biometric Recognition Systems

In PBRS, physiological features which may include DNA, Fingerprints, Face, Hands, Retina and Ear features. In BBRS, behavioural characteristics that are related to behaviour of a person[7][8].

Physiological Biometric Recognition System (PBRS) are of different types:

- Finger Print Recognition System (FPRS)
- Face Recognition System(FRS)
- Palm Recognition System (PRS)
- Iris Recognition System (IRS)
- Voice Recognition System (VRS)

Finger Print Recognition System (FPRS):

FPRS is one of the biometric physiological system uses a light sensitive microchip or optical sensors which scans the lines on the finger as shown in the Fig. 3. FPRS works with following steps:

1. Fingerprint Template formation (Minutiae Extraction)

Light sensitive microchip scans original 15 to 20 minutiae greyscale image of a finger. Template is an array of minutiae of 240*320 pixels. Each template is in the range of 200 to 500 bytes.

2. Finger Print Matching

Matching is done in two ways 1:1 matching and 1: N matching. In 1:1 matching saved template in database is mapped with one captured template but in 1: N matching many saved template are mapped with captured template[1].

Pros- FPRS has human intervention to give the sample on the device where it achieves authentication and more advantageous over classical passwords. Physical contact is mandatory.

Cons- If the finger is wet, dry, scratches and abrasions.
Spreads gems / bacteria very easily.
Attackers use silicon fingers, puppets and toys.

Application Areas of Fingerprint Recognition System:

- Aadhar ID registration and identification.
- Border control and passport verification by using fingerprint based biometrics.
- Population census can be easily done by using biometrics.
- Driving license and professional ID card verification will get done with the help of biometric identifiers.

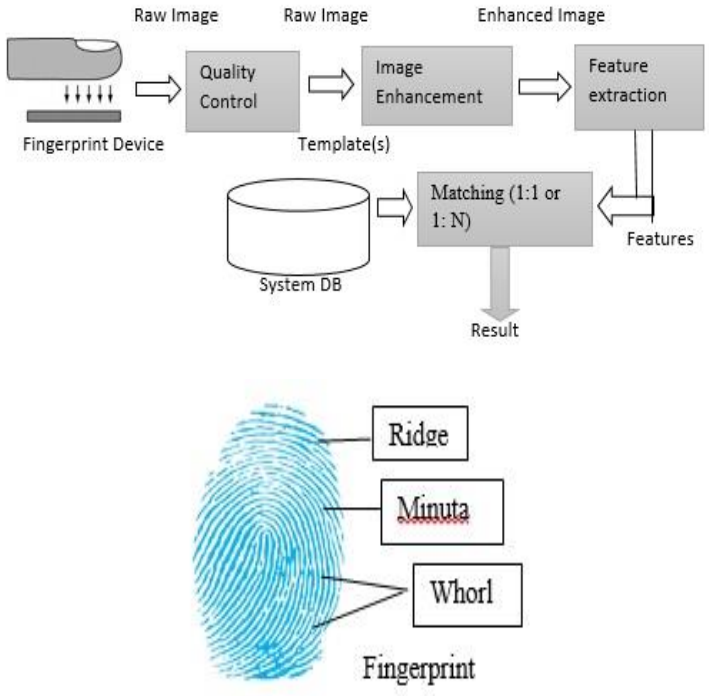

Fig.3. Fingerprint Recognition

Face Recognition System (FRS):

FRS is one of the biometric physiological systems with unique features to identify a person. In fingerprint, only twenty minutiae, where in case of Facial recognition more than sixty minutiae are considered and its working is as shown in Fig.4. Dimensions between minutiae are stored in database [5][6].

Pros- Compared to fingerprint it is hygienic, convenient to use, high usability and accurate.

Cons- Ageing Pose- After some years the same template saved in the database will be expired as the human facial dimension will change.
Illumination emotions- To different scenarios of the person, the facial expressions will get change.

Silicon Mask with the same dimensions with depth and curves.
Application Areas of Face Recognition System:

- Security and counterterrorism. Access control, it helps in comparing surveillance images to get know of terrorists.
- Using Day care we can easily Verify identity of individuals picking up the children
- Residential security: This method helps by Alerting homeowners when someone approaches near entrance of house.
- Voter verification: where eligible politicians are required to verify their identity during a voting process this is intended to stop voting where the vote may not go as expected.
- Banking using ATM: The software is able to quickly verify a customer's face[9][10].

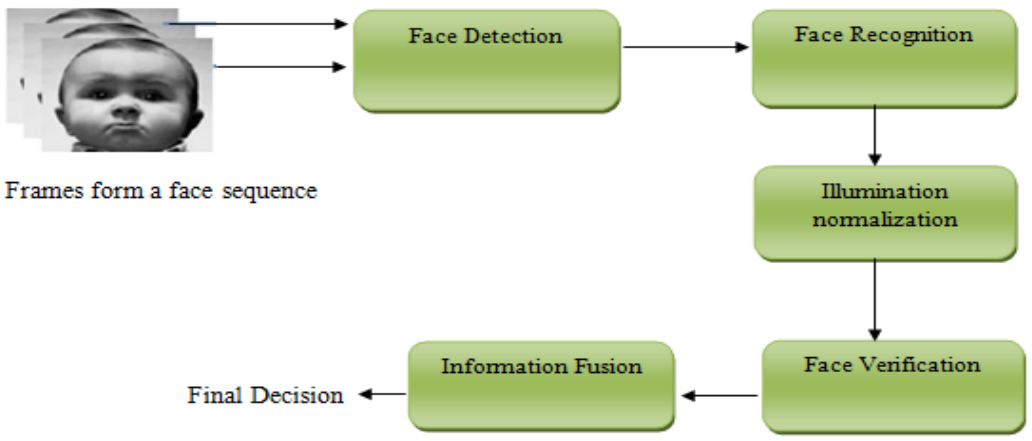

Fig.4. Face Recognition System

Palm Recognition System (PRS):

PRS is one of the biometric physiological system uses a light sensitive microchip or optical sensors which scans the lines on the palm and its operation is as shown in Fig. 5. PRS works similar to FPRS, but it will consider more minutiae than Finger Print. Attackers can use silicon palms, puppets and toys [11][12].

Pros-

- Robust to lighting, occlusions, noise.
- Robust to spoofing attacks.
- Invariant to position and distance.

Cons-

- Complex equipment.
- Can be expensive.

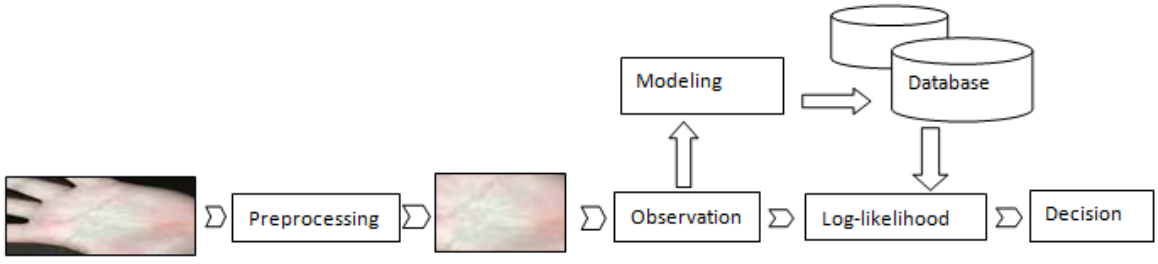

Fig.5. Palm Recognition System

Application Areas of Palm Recognition System:

- It helps in identifying blood relation.
- As a Personal Identification
- Diagnosis of certain diseases.
- In the selection of athletes into groups according to their achievements.

The below Fig.6 shows the differences between finger print and palm vein.

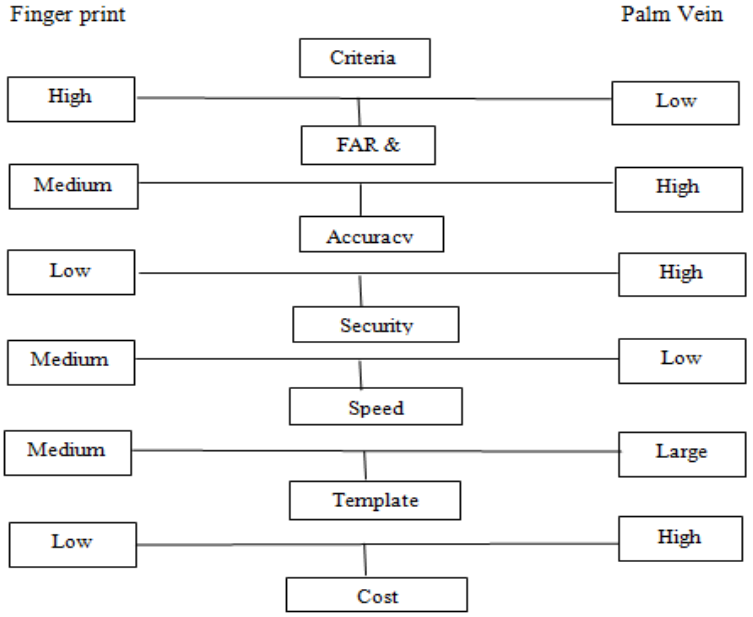

Fig.6. Finger print versus Palm Vein

Iris Recognition System (IRS):

Finally, Iris Recognition stood by counter striking all the drawbacks of the other three biometric physiological systems. Iris does not change during lifetime and it will not change for external force. Hence, iris recognition system is different from other recognition system. The iris patterns are also unique. Identical twins are also having iris patterns and even iris of one's person eye is different from the other eye[12][13][14][15]. Two persons have an identical iris pattern of $1/10^{-78}$. These characteristics made iris as good biometric recognition.IRS works with following steps which is depicted in Fig.7.

1. Iris Scan: Human naked eye is scanned from Infrared ray. The pattern of the iris is taken from the rest of the eye.
2. Analysis: The iris pattern are analyzed and put into pattern as system of coordinates. Extracting these coordinates as digital information called Iris signature, which cannot be restored or reproduced.
3. Matching: The user put in contact with for authentication scanner, which scans and matches with the database.

Iris recognition system is strongly recommended and used in research and development, Migration of countries.

Pros-

- Very high accuracy.
- Verification time is generally less than 5 seconds.
- The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being.

Cons-

- Intrusive.
- A lot of memory for the data to be stored.
- Very expensive.

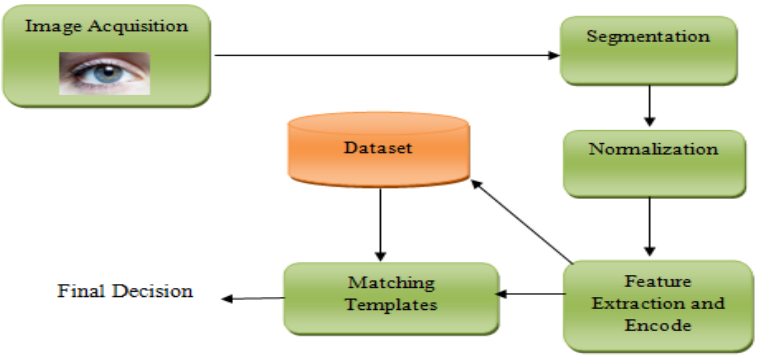

Fig.7. Iris Recognition System

Application Areas of Iris Recognition System:

- Irises are different for even identical twins.
- Iris doesn't degenerate with aging.
- Use of spectacles or contact lenses has no effect whatsoever on the automated reading of iris structures.
- Iris Guard, a company specialized in large scale security solutions based on iris recognition.

Voice Recognition System (VRS):

Voice or speech recognition is a computer software program or hardware device with the ability to decode the human voice as shown in Fig.8. In which the Voice recognition is commonly used to operate a devices, perform commands, or to write without having to use a keyboard, mouse, or to press any buttons[16][17][18][19].

Pros-

- Compatibility
- Convenience
- Speed

- Hands-Free Computing
- Easy learning

Cons-

- Accuracy
- Sound Quality
- VRS learning Curve
- Environment
- Price

Application Areas of Voice Recognition System:

- Letting your voice protect your Bank Account
- Buying Product and services with the Sound of your voice
- A Hands free AI Assistant that knows who you are
- Solving Crimes with Voice Recognition

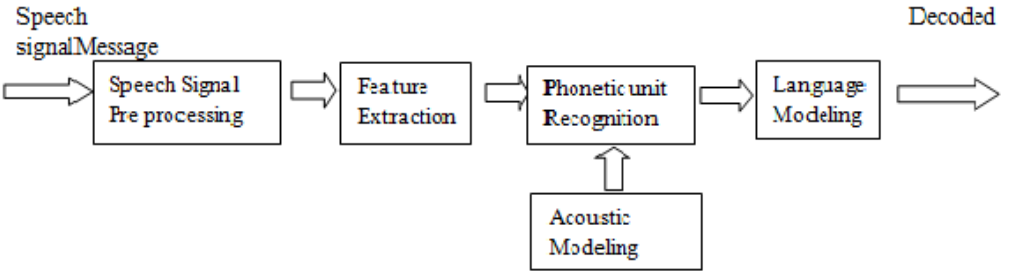

Fig.8. Voice Recognition System

According to the survey, attacks on these biometric recognition systems can be depicted as shown here Fig.9.

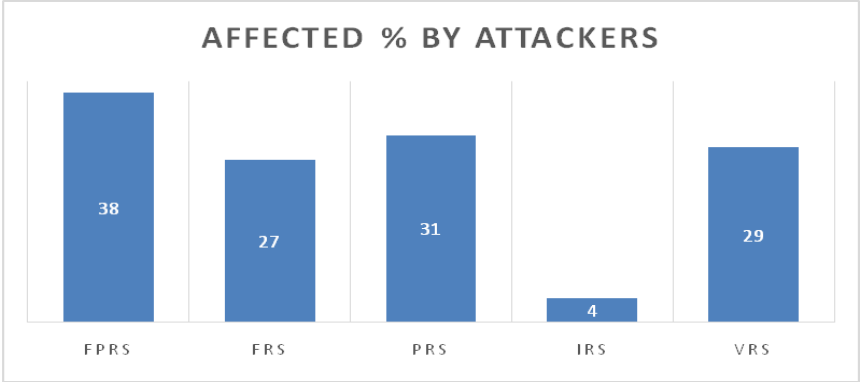

Fig.9. Affected Percentage by Attackers

3. Case Study on Aadhar card

Recently biometrics is merged into digitization technology to improve the credibility of the conventional watermarking techniques. The major access control and authenticity verification have been addressed by digital watermarking biometric authentication systems. By embedding biometrics on the host, we can formulate a reliable individual identification system as the biometrics possesses. Hence, conflicts, problems related to the intellectual property right protection can be potentially prevented. Consequently, it has been decided by governmental institutions in Europe and the U.S. to include digital biometric data in future ID documents. In India, the biometric based UID scheme, Aadhar is started with the goal of issuing a unique identification number to all Indian citizens. This Aadhar number can used in executing all the money transactions related activities including all types of purchases, sales, money transfer, hotel bills, hospital expenses and air tickets etc. Therefore, the main Aadhar based smartcard system will help the major South Asian countries in coming out of corruptions and improving their economies.

The main objective of democracy is “vote” by which the people can elect candidates for forming an efficient government to satisfy their needs and requests such that their standard living can be improved. On developing countries like “INDIA” the election commission follows manual voting mechanism which is done by electronic voting machine. This machine is placed in poll booth Centerand monitored by higher officials. due to some illegal activities the polling center are misused and people's vote to right has been denied. This seldom occurs on rural areas as well as in urban cities because the educated people are not interested in casting their votes to candidates who represent their respective areas. To ensure 100% voting automation came into play. But automated system have been approved only on some developed countries since security have not been ensured to a large extent. Our main aim of the proposed system is to develop a compatible voting machine with high security. The system is mainly designed for our country. It has three phases. First the details of the persons who are above 18years are extracted from Aadhar card database since it had become mandatory in present scenario. Automatically a new voter id with necessary details will be created and intimation will give to the persons through their e-mail. At the time of voting, the user can specify their id and password. To ensure the more security, finger prints of the voter is used as the main authentication resource. Since the finger pattern of each human being is different, the voter can be easily authenticated. The system allow the voter to vote through his fingerprint. Finger print is use to uniquely identify the user. The finger print minutiae feature are different for each human being. Finger print is used as a authentication of the voters. As soon as they cast their vote, their voter id and other details will be erased automatically and the aadhar card details which they used will be tracked and will be locked to access. This is done to preserve security. When people cast their vote the results will be updated automatically and on the same day of election, the results will also be published. Also our proposed system supports the online voting too.

4. Conclusion

In the Digital world security plays a very important role. We examined various biometric attacks, where human intervention is mandatory. Iris recognition overwrites all other recognition system of biometric. Inventively 100% security can’t be given for any system. In future a new security methodology will be design and evaluated.

References

[1] Vladimir I. Ivanov, John S. Baras," Authentication for swipe fingerprint scanners". *IEEE Transactions on Information Forensics and Security* 2017.

[2] Belen Fernandez- Saavedra, Raul Sanchez-Reillo, Rodrigo Ros-Gomez, Judith Liu-Jimenez, "Small fingerprint scanners used in mobile devices: the impact on biometric performance", 2016.

[3] Gustavo Botelho de Souza, Daniel Felipe da Silva Santos, Rafael Gonçalves Pires,Aparecido Nilceu Marana, João Paulo Papa Deep" Texture features for robust face spoofing detection" *IEEE Transactions on Circuits and Systems II: Express Briefs* 2017.

[4] Santosh Kumar, Sanjay Kumar Singh, Amit Kumar Singh," Muzzle point pattern based techniques for individual cattle identification", 2017.

[5] Ceren Guzel Turhan, Hasan Sakir Bilge, "Class-wise two dimensional PCA method for face recognition" 2017.

[6] John Soldera, Guilherme Schu, Lucas RoyesSchardosim, Eric TadielloBeltrao," Facial biometrics and applications", *IEEE Instrumentation & Measurement Magazine*, 2017.

[7] Samik Chakraborty, MadhuchhandaMitra, Saurabh Pal, "Biometric analysis using fused feature set from side face texture and electrocardiogram", 2017.

[8] Jinwoo Kang; David V. Anderson; Monson H. Hayes "Face recognition for vehicle personalization with near infrared frame differencing ", *IEEE Transactions on Consumer Electronics*, Vol. 62,2016.

[9] ArashRikhtegar, Mohammad Pooyan, Mohammad TaghiManzuri-Shalmani"Genetic algorithm-optimised structure of convolutional neural network for face recognition applications" *IET Comput. Vis.*, Vol. 10 Iss. 6, pp. 559-566, 2016.

[10] M.ShamimHossain,GhulamMuhammad, SkMdMizanurRahman, WadoodAbdul, AbdulhameedAlelaiwi; AtifAlamri "Toward end-to-end biometrics based security for Iot infrastructure", *IEEE Wireless Communications* 2016

[11] SandipJoardar, AmitavaChatterjee, AnjanRakshit "Real-time NIR imaging of palm Dorsa subcutaneous vein pattern based biometrics: An SRC based approach", *IEEE Instrumentation & Measurement Magazine*, 2016.

[12] Nassima Kihal, Salim Chitroub,Arnaud Polette, Isabelle Brunette, Jean Meunier"Efficient multimodal ocular biometric system for person authentication based on iris texture and corneal shape", 2017.

[13] Faisal Mansour Algashaam, Kien Nguyen, Vinod Chandran, Jasmine Banks "Elliptical Higher-order-Spectra periocular code", vol.5,2017.

[14] Jianxu Chen, FengShen, Danny Ziyi Chen, Patrick J. Flynn," Iris Recognition based on human Interpretable features "2016.

[15] Clariton Rodrigues Bernadelli, Paulo Ricadro da Silva, Antonio Claudio "Iris Movements: The Best state to dynamic Biometric Recognition process", *IEEE Latin America Transactions*, vol.14, 2016.

[16] Giorgio Biagetti, Paolo Crippa, Laura Falaschetti, Simone Orcioni, Claudio Turchetti, "An Investigation on the Accuracy of Truncated DKLT Representation for speaker identification With Short sequences of speech frames", *IEEE transactions on cybernetics*, vol.47, 2017

[17] Ge Peng, Gang Zhou, David T. Nguyen, Xin Qi, Qing Yang, Shuangquan Wang "Continuous Authentication with touch behavioral biometrics and voice on Wearable Glasses", *IEEE transactions on human -machine systems*, vol.47, 2017

[18] Pavel Korshunov, Sébastien "Marcel Impact of score Fusion on Voice Biometrics and presentation attack Detection in cross Database Evaluations" 2017.

[19] Dipjyoti Paul, Monisankha Pal, Goutam Saha "Spectral Features for synthetic speech detection", *IEEE journal of selected topics in signal processing*, vol. 11, 2017.

Authors' Profiles

Gururaj H L completed his B.E and M.Tech degrees in computer science and engineering from Visvesvaraya Technological University, Belgaum, India in 2009 and 2013 respectively. Currently he is working as an assistant professor in the Department of Computer Science and Engineering at Vidyavardhaka College of Engineering, Mysuru, India. His areas of interest include congestion control algorithms, security issues in cloud computing and routing protocols

for multi-hop wireless networks.

Swathi B H completed her B.E in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, India in 2017. Currently she is perceiving M.Tech degree in Department of Computer Science and Engineering at Vidyavardhaka College of Engineering, Mysuru, India. Her areas of interest include security issues in wireless sensor network, cloud computing and routing protocols for multi-hop wireless networks.

Ramesh B. completed his B.E degree in computer science and engineering from Mysore University,Karnataka, India in 1991 and M.Tech degree in computer science from DAVV, Indore, Madhya Pradesh,India,in 1995 and Ph.D degree from Anna University in 2009.Currently he is working as professor and the head in the Department of Computer Science and Engineering at Malnad College of Engineering,Hassan,India.His current research interests lie in the areas of congestion control QoS-aware routing algorithms in ad hoc networks and multimedia networks.

How to cite this paper: Gururaj H L, Swathi B H, Ramesh B,"Threats, Consequences and Issues of Various Attacks on Online Social Networks", International Journal of Education and Management Engineering(IJEME), Vol.8, No.4, pp.50-60, 2018.DOI: 10.5815/ijeme.2018.04.05