DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5263

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A PROPOSED APPROACH FOR THE PREVENTION OF BLACK HOLE USING FINGER PRINT AUTHENTICATION AND GENETIC ALGORITHM OPTIMIZATION

Pooja Chandel and Rakesh Kumar
Dept. of Computer Science & Engineering, National Institute of Technical
Teachers Training & Research, Chandigarh, India

Abstract: The Internet is a communication network where two or more than two users communicate and exchange the data. When two or more than two different areas combine together to substantially attain a specific goal then it is referred to as Internet of Things. Adhoc network consists of devices that communicate with each other directly. Black hole attack is a security threat in which a malicious node drops some or all of the packets. Biometric features are used for identification of a person. In this paper, author proposed a framework that implements a biometric authentication system to verify the user and to save the user from any internal or external threat in the communication network. The main objective of this research work is to integrate the biometric security with the communication network. The feature extraction algorithm for the finger print is supposed to be minutiae based feature extraction. If the user is authenticated only then prevention mechanism against black hole is applied using the genetic algorithm. Proposed model's performance is evaluated using various metrics like delay, throughput, energy consumption and packet delivery ratio.

Keywords: Internet of Things, Black Hole, Genetic Algorithm, Finger Print Authentication, Ad Hoc Network.

I. INTRODUCTION

Finger print authentication innovation gives an extraordinary level of security, making it the most effective approach to confirm one's personality besides DNA. For example, Eye Lock's application utilizes video innovation to convey a quick and well-disposed client experience to distinguish more than 240 purposes of interesting attributes in every human finger print. It is very embeddable and suitable for use in numerous business sector areas, including social insurance, money related administrations, stadiums, car, government, and many more. As the Internet of Things keeps on growing from home indoor regulators to complex travel systems, propelled processing plants, interconnected financial systems, the security is progressively imperative [1]. The usage of finger print authentication over these business sectors and parts will include an abnormal state of security as well as keeping frameworks easy and simple to utilize. As biometrics provide enhanced security thus for providing access to a particular device it has become the desired authentication mechanism. As a result, it can be integrated into every facet of life. This technology is now being implemented and can be easily integrated into the network to provide high security in the network.

The changing IoT operating environment results in increasing the attack surface area and a threat to the interconnected devices. IoT comprises of different systems having different types of sensors nodes or devices. Technology that is associated with these devices is different at each layer. Devices in IoT are sensed remotely. Devices in the IoT use IPv6 in Internet as address space of IPv4 is limited. IoT devices can be used to monitor health care systems, emergency systems, mechanical & electrical devices, inter and intra vehicular communication, road safety assistance etc [2]. Devices have sensory capabilities and actuation capabilities e.g. locks and lights controlling. As IoT is spreading widely and security industries are well known to various vulnerabilities like as authentication, encryption etc., even then penetration detection and prevention techniques are neglected on these devices. Thus IoT vendors have to perform various security checks before implementing their devices. This helps in mitigating the risk of attacks.

A. Security Threats in Internet of Things

IoT is a network of interrelated physical devices and has the ability to communicate over a network. It greatly affects the way humans live. It can be taken as the step up in Internet technology [3]. The changing IoT operating environment results in increasing the attack surface area and a threat to the interconnected devices.

i. IOT Devices Attacks: For some potential attacker, a device is showing the interesting target for different reasons. A number of devices can have an inherent value with their straightforward nature of their function. For example, a security camera when compromised can give some particular information regarding security posture of a known location.

ii. Communication Attacks: A very usual method of attack considers altering and monitoring of the messages while communicating. These attacks become more dangerous during traversing of sensitive information, because data and messages may get captured, intercepted and manipulated. The concerned threat puts the data and information that is being transmitted at risk.

iii. Master of Devices Attacks: A master must be there for each service or device in IoT. The aim of the master is to manage and issue the devices and facilitate the analysis of data. The attacks against the master, IoT solution providers and cloud service providers can inflict the most amount of harm as they have a large amount of sensitive data.

B. Challenges in Internet of Things

Few doubts to be considered are that the intelligent device is the next technological revolution. With the new conveniences and the miracles, the Internet of things (IoT) also promised to bring new issues and concerns. Some of these issues can be technical, some are social or environmental [4]. Right now, new problems and concerns of the majority received little recognition, although many have begun to emerge:

i. Lack of Security: Every user likes to choose the convenience when they have to choose between convenience and safety manufacturers. Devices like satellite receivers, routers, smart TVs and network storage can be simply attacked. Security is considered as the paramount in applications of industrial internet that are built on at-least thousands of sensor nodes which maximize the threat surface by means of magnitude order. Industry Internet components needs maintenance and upgrading of the construction in mind. Industrial systems need to be maintained and continuously modified to meet changing needs.

ii. Lack of Privacy: IOT is considered as the information wealth for one who has the authentication. Tracking of smart phones is possible but the smart devices points to the future where the supplements of government can census the information with the smart devices output. IOT can produce various examples when there are debates on the privacy of the smart device users [5].

iii. Storage issues: The information generated by smart devices for sharing the data can increase the demands of energy needed by IOT. For example Google may have number of server farms that consists of tens of thousands of square feet, can be dwarfed by smart devices demand. Some data generated by smart devices is needed just for sending the signals to other devices and don't need to be stored and some data like device timers needs to be stored for around a week or two.

iv. Waste disposal: Because of obsolescence, 50 million tons of e-waste like computers, phones, peripherals are generated every year in US only. In the meantime, less than 20% of the e-waste is being recycled. The smart devices are not exactly originating the e-waste, but they are built in the similar method the computer are. Thus they have less lifespan and can double or triple the problem.

v. Energy demands: A few years ago, it was predicted that by 2015, 4.9 billion smart devices will be used and it will increase to 30 percent by 2030. With these boosts, the demand for energy that is comparable to the energy demand produced by Internet would raise. During 2012, data centre has the Internet as estimated for requiring 30 billion watts for power per year. It is sufficient to power small cities, and Things of Internet will require much more. It will be difficult to meet the demand by green energy and enhanced batteries like wind and solar. But adding problems such as wasted energy and pollutants and powering IoT can be an important social issue in the next ten years.

vi. Open Standards requirement: Internet of Things has particular devices for their own condition. As not significant at this phase smart devices must be able to communicate with each other for the further growth. However, worldwide standards with protocols are lacking after the smart technology development, although it is likely that much of IoT will be built with open source software. Some existing efforts tends to be limited to technologies like Eclipse Internet of Things and focussed on applying the existing protocols/ standards for smart devices as a substitute of being created for the novel Internet of Things needs. The growth of IOT will be as slow as possible without a greater degree of cooperation.

vii. Novel use cases: As numbers of organizations are now developing great IoT value, a number of organizations are still hostile for getting started. For helping the organizations, Internet of Things journey is started, the Internet of Things Value Roadmap is developed, and the guide would help the organizations to create business value in connected and smart world. How to use IoT include a timer that typically turns the appliance on and off, but the real purpose may only appear when smart devices be all over the place [6]. It doesn't imply that Internet of Things would never be a successful skill. But it implies that the outcome is difficult to predict. The only reliable advice is advising everyone to expect the unexpected estimates, and that the suggestions for long-term planning are almost inaccurate.

II. BLACK HOLE ATTACK

In black hole attack, router instead of relaying packets to other nodes, drop some or all of the packets. In this routing protocol is used by a malicious node in order to advertise itself. It is hard to detect black hole attack as packets can also be dropped due to a network problem. If the router drops all the packets, then it is easy to discover the attack but if the router drops some of the packets over a particular period of time then it is difficult to discover black hole attack.

The faulty router broadcasts that it has the smallest way to the receiver's node than any other node. The faulty router does not check its routing table. Thus it sends a reply to the requests quickly before any other node. The requesting node gets a reply from the faulty node before receiving a reply from actual node. Thus forged route is created. After establishing the route, the faulty node will either forward packet to unknown address or drop all the packets.

In Fig.1 node "A" sends RREQ packets to node "E" hence route discovery process is initiated. If node "B" is a malicious node then as it receives RREQ packet it sends the reply to node "A" before any other node. Thus node "A" considers it as the active route and initiates transferring the packets to the node "B". Node "A" will refuse all other replies from other actual nodes. Hence entire data packets will be lost [7].

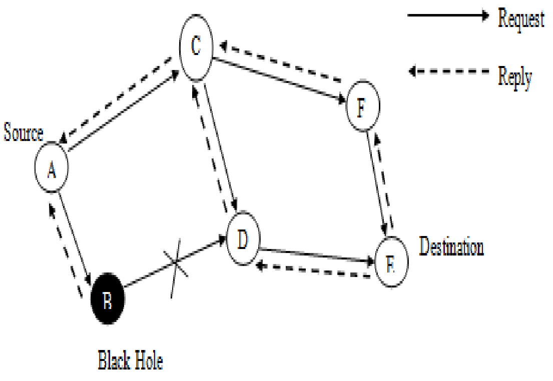

Figure 1. Black Hole Attack

III. FINGERPRINT AUTHENTICATION

The study of the fingerprints came into the moon light in the 18th century. Fingerprint matching is one of the oldest forms of the biometric technologies that are being used so widely. In the field of civilian, criminal investigation, government and commercial device applications like licence card, passport and security device, the fingerprint technology is used. Fingerprints of humans consider being unique and they can never be the identical. Fingerprint identification is the identification practice of personality dependent on the impression pattern of valleys and ridges on fingers [8]. There is an extensive usage of fingerprint technology, but new work is needed to be done for checking fingers distinctiveness. Numbers of factors are there that lead to interruption in fingerprint recognition such as small pressing spot, pressure, device noise, atmospheric factors and skin suppleness. Fingerprints are unchangeable and could decline only after death. Since the Egyptian time, the use of fingerprints was meant for signatures. Major features for biometric gauge are distinctiveness, universality, collectability, durableness, recital and satisfactoriness. Father of fingerprint matching technique is Francis Galton. Combination of patterns called ridges and valley develop the fingerprints. Single arched section is known as ridges whereas part between two adjoining ridges is known as valley and ridge termination is known as minutiae. For fingerprint matching mainly two features of minutiae are used i.e. ridge ending and ridge bifurcation. Fingerprint matching is a very crucial and an essential step in the biometric technology. Fingerprint matching based on minutiae method is a very popular approach. The initial part is known as the 'training part' following the second part which is for testing. The training part involves the following procedures like sensing, feature extraction, saving the extracted features to the database. The following sections, describes the parts of the training segment. Following components that are used for developing the biometric system [9]:

i. Sensor module: The biometric data for particular user is acquired. The fingerprint sensor is needed for capturing finger impression that can be stored in database for the process of verification.

ii. Feature extraction: This component helps in feature extraction for the impressions that are stored in the last process. Such as, for fingerprint image, orientation of minutiae points and the position are needed to be finding out. So to extract feature values in fingerprint image we need feature extraction module.

iii. Matching module: In this module feature values are compared with feature value being stored in previous process. This comparison is performed on the basis of matching score. Like as, in this module, some points are computed among template and query request known as minutiae.

iv. Decision-making module: Once matching is done, the machine gives the response that is either true or false. The decision is given by the biometric system that either that ID has matched or not. If it is matched then access to the system is granted else access is denied.

Fingerprints are known to be the fastest and best method for biometric identification. As everyone has individual fingerprints, therefore, it is used securely and doesn't vary anyone's lifetime. The fingerprint execution is cheap and has the best stability. This can be used in forensics as well as civilian purposes and mostly biometric dependent. It consumes less energy as compare to other systems and is even faster too.

IV. RELATED WORK

Ashish et al. [10], proposed a new protocol named as Secure AODV for preventing the effect of black hole attack on the network. It is based on first route reply caching mechanism. In this protocol, to mitigate the black hole attack, the first RREP that is reaching the source node is ignored. The results are measured using various parameters like packet delivery ratio, delay and throughput that show a considerable improvement over existing protocol.

M. Rajesh Babu et al. [11], proposed an alleviation procedure to detect the nodes that are behaving abnormally. Sensitive guard procedures, hole detection algorithms and timely mandate procedures are used to detect hostile nodes. The proposed procedure is cost-effective and ensures the guaranteed QoS by assuring resource availability proposed algorithm ensures guaranteed quality of service and cost-effectiveness. From the results, authors had concluded that proposed algorithm is better than other solutions for the detection of black hole attack.

Arshdeep et al. [12], implemented genetic algorithm with Black hole attack. In this paper, dynamic source routing protocol is used to prevent system from attack. For simulation, a hypothetical network was constructed and then monitored for a number of parameters.

Ashwini Hosgouda et al. [13], proposed an efficient method to increase the success packet delivery ratio even when black hole is present. The method uses advance BFO algorithm. Java Netbeans IDE is used for black hole attack detection and mitigation and performance are evaluated on the basis of energy consumption and packet delivery ratio.

Rakesh Ranjan et al. [14], reviewed black hole attack. Black Hole attack affects reactive routing protocol that causes a serious loss of data which leads to a security threat. As one of many protocols AODV (Ad hoc On-demand Distance Vector) is usually an easy victim of such attacks. In this type of attack, the node broadcasts that it has the shortest path to the destination and making it easier to access all of the data transmitted. Such nodes are called malicious nodes.

Leila Kabbai et al. [15], presented a new method for extracting Invariant Features from the region of Interest. The new descriptor is derived from the original descriptor, namely, Scale Invariant Feature Transformation (SIFT), that are extensively used for matching of the image by extracting interest points (IPs). However, when the background is complex or destroyed by noise, this descriptor performs poorly. Thus a local binary pattern (LBP) descriptor with a uniform pattern and a centrally symmetric local binary pattern (CSLBP) instead of the gradient feature used in the SIFT algorithm is used. The author has presented new descriptors based on different combinations of SIFT, LBP, and CSLBP descriptors to improve matching results. Then they calculated different evaluation measures for various image transformations (fuzzy attack, rotation, and affine transformations), such as repeatability, recall, and accuracy. Experiments on two different databases have shown that the descriptor results in better results.

Masao Yamazaki et al. [16], concluded Small Area Sensors Fingerprint authentication as the most promising technology for network user authentication on mobile devices such as smart phones. In this case, the size of the touch sensor becomes so small that the traditional detail method should be replaced by a new method. They consider a scale-invariant feature transform (SIFT) method for fingerprint authentication using a touch sensor on a smart phone. In this article, the main focus was on template extension registries to accept any small portion of the query finger for validation.

Tanvi et al. [17] summarize soft computing techniques in biometrics. In the past few years, biometric verification has become one of the most promising technologies, but still, there are issues in FAR and FRR. Great biometric identification system has a high rate of recognition, tolerance for uncertainty and noise in data. Recently, soft computing is widely used in biometrics, which greatly contributes to enhancing its recognition rate. All kinds of soft computing techniques, such as fuzzy logic, NN are used to build a good biometric system. This paper introduces biometric and its related issues. The variety of soft computing techniques for feature extraction, integration, optimization and recognition rate improvement are described.

Chandeep Singh et al. [18], proposed an adaptive approach based on genetic optimization to determine Blackhole attack in AODV (Adhoc on demand distance vector protocol). The Genetic algorithm is used to increase the performance, availability and efficiency of the network. They had analyzed the performance of GA in AODV protocol during black hole attack and concluded that AODV–GA is better than only AODV.

Gaurav Kumar et al. [19], presented detailed information about various types of feature and feature extraction techniques. A comparison is made between different feature extraction techniques and it helps in taking a quick decision about which extraction techniques are better for a particular type of work.

Harpreet Singh Brar et al. [20], presented a unique bacterial foraging optimization method. Minutiae extraction operation and other morphological operations are used to extract features. In this paper, comparisons are made between BFO and SVM (Support vector machines). At last, author concluded that BFO is better than SVM while matching finger prints with angle variations.

Rupak Rathore et al. [21], showed the highlighting of the rapid aging of the population, and obesity-related medical conditions, widely drunk driving incident, advances in medical devices, and 4G mobile networks that makes possible to integrate biometric technology into the car, and related measures in response to save precious lives. In this work, the author proposed an automotive healthcare and safety framework. A control unit called as healthcare control unit controls this framework. This framework is also integrated into an automotive IOT containing telematics and other systems. Performance evaluations shows that this system can help to save lives of pets and infants that are mistakenly left inside parked cars.

Purneet Kaur et al. [22], proposed a technique in which Genetic algorithm and Neural Network are combined together. For extraction of minutiae GA is used and for the recognition of finger print neural network is used. For processing low and high-resolution images histogram equalization process is used. Thinning of lines is done on MATLAB using morphological image processing. The Genetic algorithm is used to find out discontinuous segments. At last, for matching processed image is fed to the trained system. Experimental results show that combination of genetic algorithm and neural network provides better and efficient technique for finger print matching.

V. PROPOSED METHODOLOGY

This work presents an application of precondition that the attacker has access to the local network giving way to the black hole attack. Here we will describe the black hole attack scenario in the network. In proposed work finger print biometric authentication will be done to know that attack has been taken place. To gain access to the system, the user must be identified first and then further checking is done to verify the identity. This work will utilize minutiae feature extraction, feature reduction and failure node detection using a genetic algorithm. In the end proposed model's performance is evaluated using various metrics like throughput, energy consumption, delay and packet delivery ratio. Fig.2 describes the flowchart of the proposed technique.

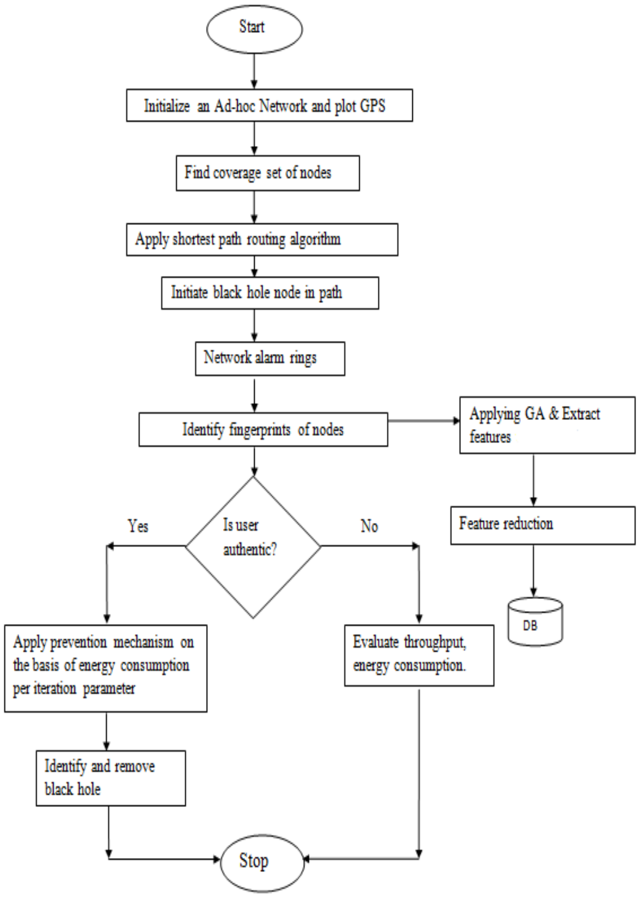
Start
Initialize an Ad-hoc Network and plot GPS
Find coverage set of nodes
Apply shortest path routing algorithm
Initiate black hole node in path
Network alarm rings
Identify fingerprints of nodes
Applying GA & Extract features
Feature reduction
DB
Is user authentic?
Yes
No
Apply prevention mechanism on the basis of energy consumption per iteration parameter
Evaluate throughput, energy consumption.
Identify and remove black hole
Stop

Figure 2. Proposed Flowchart

VI. EXPECTED OUTCOME

A novel method is proposed to designing the Intrusion Detection system to enhance the accuracy in IOT and analyzing the complexity and high security in the development of the proposed model.

VII. CONCLUSION & FUTURE SCOPE

The proposed work has combined wireless sensor network and a biometric authentication system to prevent a native node in sensor network from any suspicious activity if the authentication of the node is true. The authentication of finger print would include a pre-processing feature extraction and a recognition system whereas wireless system would act as some sort of an Adhoc network in which the nodes will change their relative position frequently.

The future aspect of this proposed work is to implement the black hole detection and prevention system along with finger print recognition system to provide secure access to the system. Complexity and high security will be analysed in the development of the proposed model.

VIII. REFERENCES

[1] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi and Talha Kamal, “A Review on Internet of Things (IoT)”, International Journal of Computer Applications, Vol. 113, pp. 1-7, March 2015.

[2] About Internet of Things from website https://en.wikipedia.org/ wiki/Internet_of_things.

[3] Suchitra, Vandana, “Internet of Things and Security Issues”, International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 1, pp. 133-139, Jan. 2016.

[4] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed, “Internet of Things Applications, Challenges and Related Future Technologies”, World Scientific News, pp. 126-148, 2017.

[5] Sanket Thakare, Ashwini Patil and Ashraf Siddiqui, “The Internet of Things – Emerging Technologies, Challenges and Applications”, International Journal of Computer Applications, Vol. 149, pp. 21-25, Sept. 2016.

[6] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul and Imran Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures”, International Journal for Information Security Research (IJISR), Vol. 5, Issue 4, pp. 608-616, Dec. 2015.

[7] Fan-Hsun, Tseng, Li-Der Chou and Han-Chieh Chao, “A Survey of Black Hole Attacks in Wireless Mobile Adhoc Networks”, Human-centric Computing and Information Sciences, Springer, pp. 2-16, 2011.

[8] About Fingerprint authentication from website https://en.wikipedia.org/ wiki/Fingerprint_recognition.

[9] Avinash Kumar Jhal, Supriya Narasimhaml, Sudheer Sreedhara Krishna, V. P. Mahadevan Pillah, “A Neural Network Based approach for Fingerprint recognition system”, International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 808-812, 2010.

[10] Ashish Kumar Jain, Vrinda Tokekar, “Mitigating The Effects of Black Hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks”, IEEE International Conference on Pervasive Computing(ICPC), 2015.

[11] M. Rajesh Babu, S. Moses Dian, Siva Chelladurai and Mathiyalagan Palaniappan, “Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version”, The Scientific World Journal, Vol. 2015, pp. 1-12, 2015.

[12] Arshdeep Kaur, Mandeep Kaur, “Prevention of Black Hole Attack in MANET using Genetic Algorithm”, International Journal of Advance Research in Science and Engineering, Vol. 4, pp. 153-163, May 2015.

[13] Ashwini Hosgouda, M. S. Shobha, Akshay S. Aspalli, “Implementation of Black Hole Attack Detection and Mitigation in MANET using Advance BFO Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5, pp. 465-470, 2015.

[14] Rakesh Ranjan, Nirnemesh Kumar Singh, “Security Issues of Black Hole Attacks in MANET “, IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 452-457, 2015.

[15] Leila Kabbai, Aymen Azaza, Mehrez Abdellaoui, and Ali Douik, “Image Matching Based on LBP and SIFT Descriptor”, 12th IEEE International Multi-Conference on Systems, Signals & Devices, pp. 1-6, 2015.

[16] Masao Yamazaki, Dongju Li, Tsuyoshi Isshiki and Hiroaki Kunieda, “SIFT-based Algorithm for Fingerprint Authentication on Smartphone”, 6th IEEE International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES), pp. 1-5, 2015.

[17] Tanvi, Neelam Goel, Manvjeet Kaur, “A Review of Soft Computing Techniques in Biometric”, Proceedings of 2015 RAECS UIET Panjab University Chandigarh, pp. 1-4, Dec. 2015.

[18] Chandeep Singh, Vishal Walia, Rahul Malhotra, “Genetic Optimization based Adaptive Approach for the Determination of Black Hole Attack in AODV Protocol”,

2nd International Conference on Science, Technology and Management, pp. 2742-2753, 2015.

[19] G. Kumar and P. K. Bhatia, "A Detailed Review of Feature Extraction in Image Processing Systems," Fourth International Conference on Advanced Computing & Communication Technologies, pp. 5-12, 2014.

[20] Harpreet Singh Brar, V. P. Singh, “Finger print Recognition Password Scheme Using BFO”, IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp.1942-1946, 2014.

[21] Rupak Rathore, Carroll Gau, “Integrating Biometric Sensors into Automotive Internet of Things Need and Proposed Implementation”, IEEE International Conference on Cloud Computing and Internet of Things (CCIOT), pp. 178-181, 2014.

[22] Purneet Kaur, Jaspreet Kaur, “Finger print Recognition Using Genetic Algorithm and Neural Network”, International Journal of Computational Engineering Research, Vol. 3, pp. 41-46, 2013.