AN ANALYTICAL REVIEW OF IoT BASED ON BIOMETRICS AND WSN

[1]Manpreet Kaur Maan
Research Scholar, Desh Bhagat Univeristy, MandiGobindgarh
Email: preetbhullar82@gmail.com

[2]Dr. Sawtantar Singh Khurmi
Professor, Computer Science & Engineering
Desh Bhagat University Mandi Gobindgarh

Abstract

This paper contributes a brief description of IoT (Internet of Things) system development with WSN (wireless sensor network) to prevent the network from the intruders. In the past decade, IoT has been a focus of research field for the researchers. Security and privacy are the key issues for IoT applications, and are still facing some enormous challenges in the development of IoT system. In order to facilitate this emerging domain, a brief review of the research progress of IoT with the security area of system to prevent the network from the intruder using the concept of biometric recognition system based on the fusion has been presented. Biometric fusion is the best approach in the IoT system to prevent the network from the different types of attacker and to secure the important data during the transmission. So, in this review we have focused on the system prevention techniques by using the different types of the optimization algorithm along with the classifier like ANN, SVM, K-NN etc. On the basis of this, we have discussed the research status of key technologies including biometric authentication system in the IoT system to achieve the better efficiency of system.

Keywords: ***Internet of Things (IoT), Wireless Sensor Network (WSN), Biometric system, Artificial Bee Colony (ABC), Genetic Algorithm (GA) and Artificial Neural network (ANN)***

INTRODUCTION

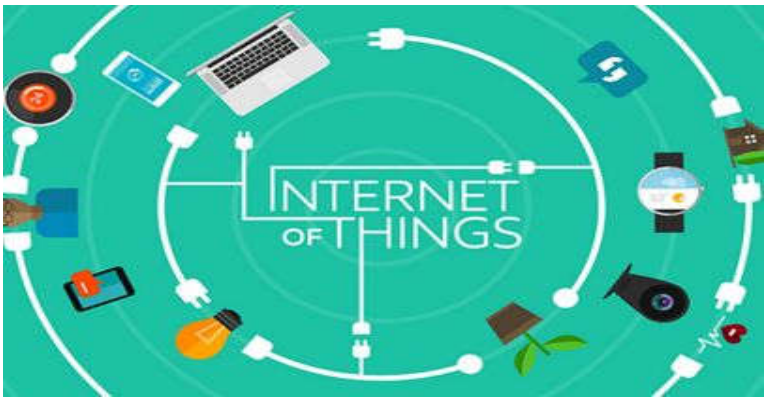
The Internet has grown into millions of phases to reach its current form. The evolution can be broadly divided into five stages. The history of the Internet began with the development of electronic computers in the 1950s. The original concept came from WAN (Wide Area Network) laboratory of computer science in the United States, the United Kingdom, and France. In the early 1960s, the US Department of Defense has signed the contract, including the ARPANET project, operated by Lawrence Roberts, directed by Robert Taylor. The first piece of news came in 1969 from the ARPANET as of the laboratory of computer science professor Leonard Kleinrock at the University of California, Los Angeles (UCLA) in the second network node of the Stanford Institute (SRI). The explanation of these stages is described in table below:

Table 1: The evolution of Internet [1]

Phases	Names	Description
Phase-1	The ARPANET	The ARPANET is abbreviated as "Advanced Research Project Agency Network".
		It was the first network that has used packet switching network.
		The ARPANET was searched by the US military and the DoD (Department of Defence)
		It uses mainly for research area.
Phase-2	The gold Rush for Domain Names	This phase came at the time of HTML and the industries already had registered their domain names quickly.
		This is used for sharing the information about the products and the services.
		It is also known as Brochureware.
Phase-3	The boom and bust of the dot com bubble.	This phase is also known as the transactional exchange phase.
		It is mostly used by the EBay and Amazon companies for purchasing and selling of goods and services over internet.
Phase-4	The social and Experience Web	In this phase, the social interaction came into existence.
		Companies like facebook, twitter came into existence
Phase5	The internet of Things	This is a very important development that affects the ability of the people to work and live.
		The Internet of Things (IoTs) can be described like connecting smart phones, the Internet and other daily needs TVs, sensors and actuators on the Internet carefully linked together to create new forms of communication between things, people, and communication between them and the things itself.

I. IoT (INTERNET OF THINGS)

IoT is a system that uses advanced automation and analytics Networks, sensors, large data and artificial intelligence technologies to provide a complete system for product or service [2]. These systems allow greater transparency, control and performance suitable for any industry or system. IoT system due to its unique flexibility and ability can be applied to all industries that are suitable for any environment. It can improve data collection, automate, operate, and more through smart devices and powerful support technology [3].



The above figure 1 represents the architecture of IoT. As depicted, digital devices such as laptop, cell phone, social media like twitter, facebook, and medical health care unit are interconnected with each other though internet. In this section, a comprehensive introduction to the Internet of Things is provided. It introduces the IoT concept, which is important for the user and deployment of IoT systems. The features, advantages, disadvantages and application of IoT in detail are shown in table 2 [4].

Table 2: Comparative analysis of IoT[5,6]

Features	Advantages	Disadvantages	Applications
Artificial Intelligence (AI): It can be make smart by gathering the data using AI and networks.	**Increased users engagement:** IoT is used to achieve high accuracy and can be engaged effectively with the users	**Security:** As IoT connects numerous of devices connected through internet thus many external attackers can effects the security of the system.	**Smart homes:** In smart homes the users communicate with each other through the internet. IoT helps the owners to provide security.
Connectivity: Practically network exist in a small area that is connected between the devices that are connected in the network	**Technology optimization:** IoT opens the world of serious functional and field data.	**Privacy:** In IoT, the data is usually transfers to the destination node without the active participation of user's.	**Wearables:** IoT can be used by wearable devices such as fitness, health and entertainment fields. An example is attack device that is used to track the heart rate and stored the results in digital device.
Sensors: This is the important device that is used in IoT. These sensors mainly comprises of Energy modules, RF modulation, Wi-Fi, Bluetooth etc. These devices manages the sensed	**Reduced Waste:** IoT makes the use of resource in a managed manner.	**Complexity:** Design, deployment and maintenance is complicated.	**Retailing:** IoT helps to track the goods supply, avoid costly mistakes, gathering the essential customers data etc.

signal gathered from active and passive devices			
	Enhanced data collection: IOT helps to place data to their exact location		**Health care:** IoT is used to sense the physical parameter of patient and sending them to the doctor and record them in the database for future use.

I. WSN (Wireless Sensor Network) in IoT

In IoT, WSN plays a vital role. WSN mainly comprises of small sensor devices that are interconnected through wireless network. Small stable, cheap, low powered Wireless sensors can make the smallest devices installed in any environment, at a reasonable cost. To integrate these devices into IoT can be considered as an important development of wireless sensor networks [7].

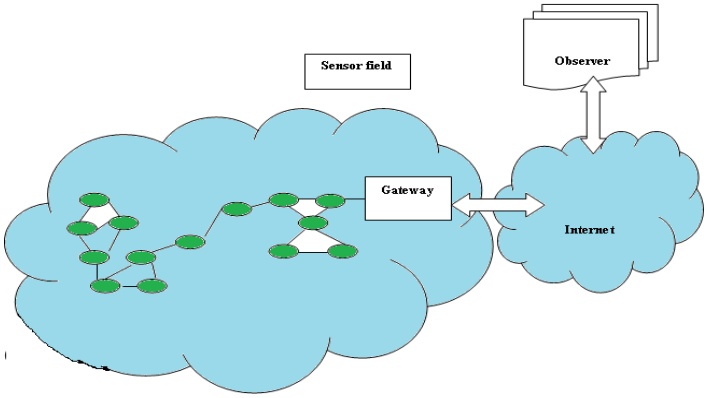


Figure 2: Wireless Sensor network

The green circle in the above figure represents the sensor nodes. These are the main part of WSN. The hardware of sensor nodes are mainly comprises of the power, power management block, a sensor and a microcontroller and a trans-receiver. The power required by the network is provided by the power system. Sensors are used to convert the input signal into the desired signal for example it converts the light, chemical signals into electrical waves. The transferred signals are forwarded to microcontroller Microcontroller is used to process the input data which is transmitted through the transreceiver module [8].

WSN can be connected to the internet through three different methods as discussed below

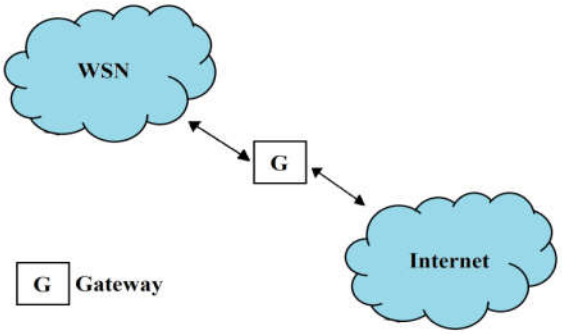


Figure 3: Independent network

The network shown in figure 3 is known as independent network in which internet and WSN are connected throgh a single gatway. This technique is mostly used by WSN's to access the inernet connection

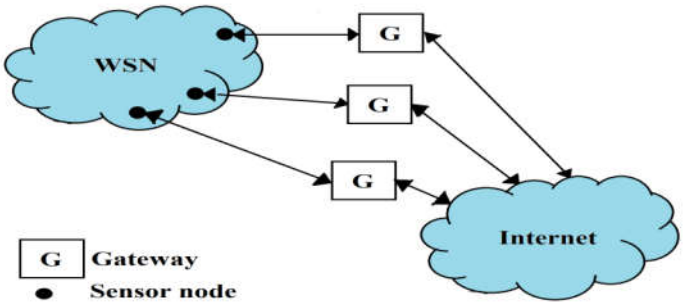


Figure 4: Hybrid network

The second method is known as Hybrid network in which more than one gatway has been used in between the WSN and internet. The nodes are shown in figure below, with the help of these nosdes users can access the internet.In the figure above, each gate comprises of single node that is connected to the internet [9].

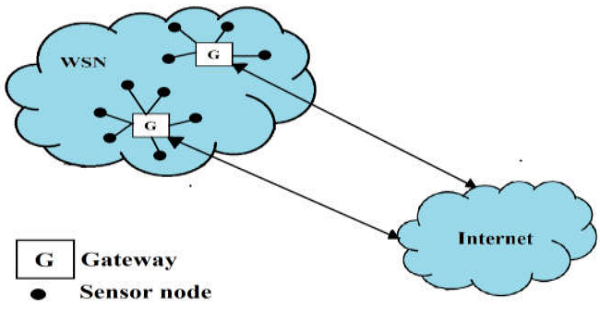


Figure 5: Access point Netwrok

The third method is known as Access point netwrok, in which each gate comprises of more than one node and the gates are positioned within the WSN area [10].
A WSN forms a large netwrok, hence, the security of the network is the main concern, so that the data can be delivered to the destination node accuratly. Therefore, to deliver accurate data, WSN used different authentication system to protect the network. The most commonly used authentication system is the Biometric system.

i. Biometric system

A biometric system is an technique that uses biological information to identify a person. Biometric authentication systems verify a person's via the identity from behavioral traits (signature, voice) or physiological traits (face, iris, and ear). Biometric mainly identifies two characteristic namely Physical and behavioral [11].

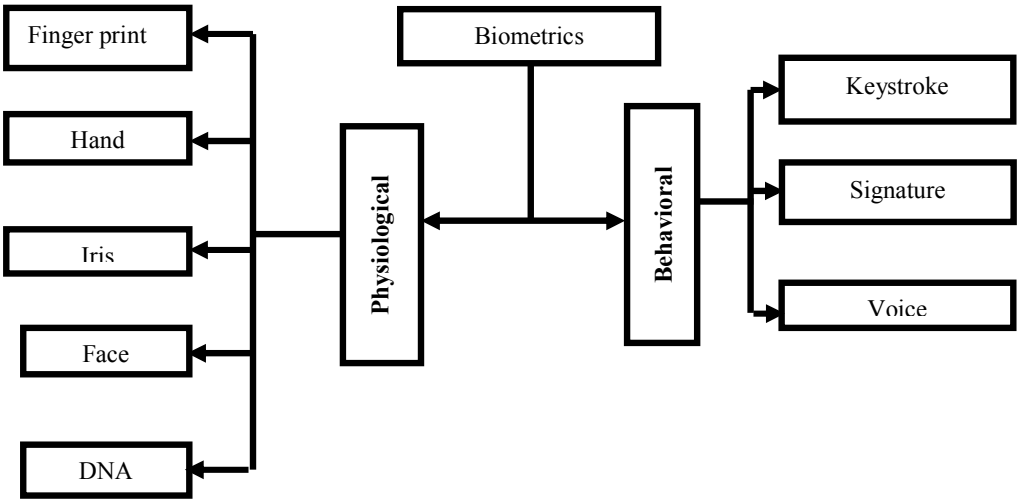


Figure 6: Biometric types

a. Physiological characteristics

In this type of biometric system, a person is recognized on the basis of their physical characteristics. The system come under this technique are discussed below.

i. Fingerprint system

In this system, the fingers of the human beings are used for the identification. The database of finger's features such as arches, threads and rings and a side, and the details of the trench profile are created. A fingerprint mainly comprises of ridge patterns and valley on the surface of fingerprint [12].

ii. Hand

In this system, a huamn being is identified by the geometry of their hands. In this sytem, there is an hand geometry reader that reads the shape of hand and compares it with the database stored into the files.

iii. Iris

Iris's recognition is an automated method of biometric identification that uses mathematical recognition patterns to identify video images of one or both irises of an individual's eye. The complex pattern is unique and stable and can be seen from a distance View.

iv. Face

In facial recognition system, the live images of face are compared with the data recorded into the database.

v. DNA

In this the recognition of person is done by using tisues, blood and other body samples.

b. Behavioral Chracteristics

The person is identified on the basis of human behaviours such as signature, voice and keystrokes are come under this techniques.

i. Voice recognition

In this, the person is identified on the basis of their voice characteristics as we know that every individual person has unique voice.

ii. Signature recogniton

As the style of writing varies from human to human due to their writing style, pressure and velocity of pen, thus, this method can be used to identify an individual.

iii. Keystroke Recognition

In this sytem, the human is identified on the basis of their typing style [13].

3.1 Attacks in Wireless Sensor Network (WSN)

WSN is affected by number of attacks. The attackers could attack their own data bits to the channel through the radio link.A secure network must support all security features. Attacks can be deployed to malicious nodes in the network and has the same capabilities as a normal node or can be utilize memory that covers normal deployment nodes [14]. The attacks in the netwrok are mainly categorized into three forms shown in the figure below

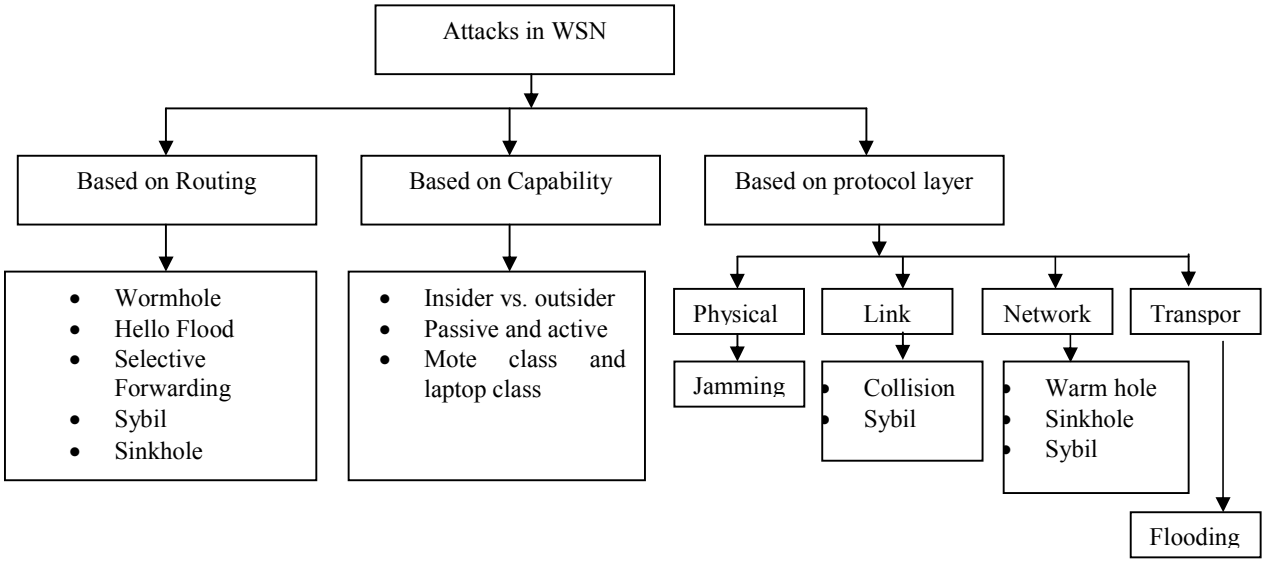


Figure 7: Classification of Attacks in WSN

i. On the basis of routing

Routing protocols are used to transmit the data from source to destination. Therefore, during the transmssion process, hacker can steal the information by using various attackers. The attackers come under routing protocols are shown in figure above.

a. Wormhole attack

In this type of routing attack, more than two malicious nodes are present in the network at dissimilar position. When the actual transmission begins, the sender sends the information which is received by one of the malicious node then this malicious node forwards the information to the another malicious node which sends the information to its nearby node and taking the control of the source data packets by giving the information to the receiving node that is being positioned at a distance of 1 or 2 hop.

b. Hello flood attack

In this type of attack, source node broadcasts the HELLO message. When receiver node receives the HELLO packet, it assumes that the source node is in the range and sends the data packet in response to the broadcaster message. The attacker also sends HELLO message with high transmission power and thus, takes the packet from the source node, modifies that packet or may be drop that packet. In this process, a lot of energy is wasted and also network congestion occurs [15].

c. Selective forward attack

This attack interupts the process of communciation within the network. In this, the nodes select the packets and then forward them into the network. This is also known as Black hole attack as it drops all the packets at the same time.

d. Sybil Attack

A Sybil attack consists of single node that presents a number of identification to another nodes in the network. The nodes affected by the nodes is known as Sybil nodes.These attackers exchange the location information for the routing protocols used in the network.

e. Sink hole attack

In this type of attack, the attackers broadcast the fake routing information to attract the network traffic. This type of attack is mostly affected by WSN system as in WSN, the communication takes place from number of nodes to the single base station.

ii. Based on capability

The data access level and its affect is different and normally depends on the attack type. The attacks come under this are listed in figure 7.

a. Insider and Outsider Attacks

In insider attack, the malicious node is present within the network whereas in outsider attackers, the attackers that can harm the netwrok are not present in the netwrok.

b. Active and Passive Attacks

The passive attackers do not disturb the actual communication of the network. They normally monitors and modifies the data. In active, the attackers interupt the actual communication and the performance of the netwrok is degraded [16].

iii. Based on protocol layer

WSN is consisted of many layers, namely, physical layer, link layer, network and transport layer. The working of each layer is different. The attckers that affects these layers are listed in figure 7.

a. Physical layer

Physical layer is used for transmitting the bits through the radio link. The attackers affect this layer are listed above. These attackers can jamm the radio frequency signal and thus, changes the working of the network.

b. Data Link layer

This layer is responsible for transmitting the data from source node to destination node, to base station and in between the nodes within the network. The attacker affect the data traffic by coming in between the source and destination node.

c. Transport layer

This layer is used to provide communciation between the WSN to theinternet. Flooding and synchronization are the main issues of this protocol [17].

II. ALGORITHMS USED IN IOT SYSTEM

To secure the WSN from all the attacks mentioned above, an optimization algorithms and classification algorithms are used are are defined below:

4.1 Optimization algorithm

In IoT system, to find the attacker, optimization algorithms are used. This identifies the attacker on the basis of the node property.

i. Genetic algorithm

Genetic algorithm is used find the attacker within the network. It is mainly comprises of three functions namely; Crossover, mutation and a fitness function.

Crossover: It is used to validate the fitness funtion.
Mutation: It is used to add variation
Fitness function: It is used to evaluate the data which is usefule for the work [18].

Genetic algorithm

```
function GA ()
{
Initialize population;
Calculate fitness function;
While(fitness value != termination criteria)
{
Selection;
Crossover;
Mutation;
Calculate fitness function;
}
}
end
```

ii. Artificial Bee Colony (ABC)

ABC algorithm is developed by author Dervis Karaboga in 2005, stimulated by the intelligent honey bees' behaviour. It mainly comprises of three components namely, Employed bee, onlooker bee and scout bee. Employment bee is used to find food source. Onlooker bee is responsible for determining the quality of the searched food. Scout bee is used to calculate novel solution [19]. The algorithm is written below.

ABC Algorithm

Initialize the total bee= Total_ data
Initialize the bee categories- **Employed_ bee**
- Onlookers_ bee
- Scouts_ bee
Defined threshold properties=f_t
Set f_s as scout bee
For i=1 → node in route
Call objective function j

$$ABC_{obj} = \begin{cases} E_{Bee} > O_{Bee} \text{ then j True} \\ \text{E}_{\text{Bee}} \leq O_{Bee} \text{ then j false} \end{cases}$$

Return $S_{Bee}j$
Optimize data = $ABC\ (ABC_{obj}, f_s, f_t)$
End
$S_{Bee} = optimize\ data$
Return optimize data and prevent the node using properties of node.

4.2 Classification algorithms

Artificial Neural Netwrok (ANN) is the classification algorithm which is consisted of three layers namely input layer, output layer and hidden layer. The input data is given to the input layer that passes the data to hidden layer on which weights is added so that the difference between input and output is low [20].

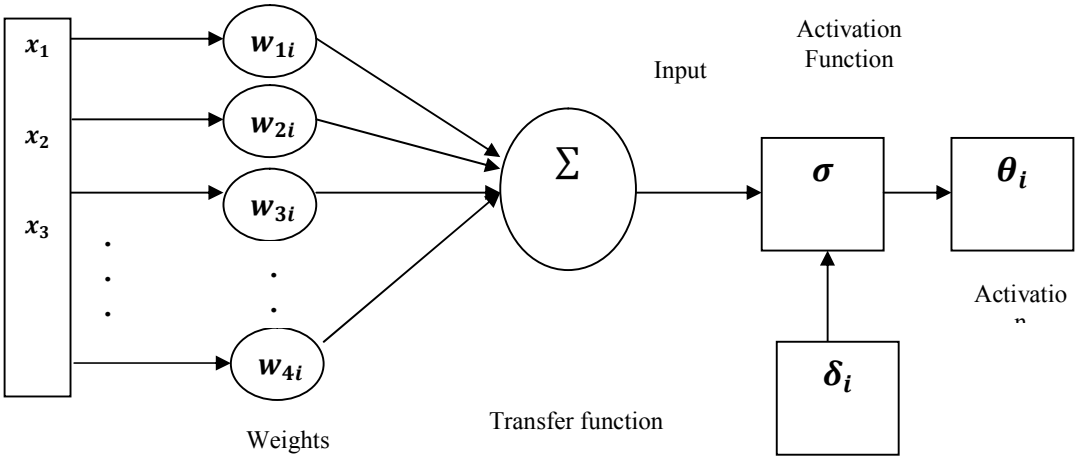


Figure 8: Artificial Neural network

ANN algorithm
Load optimize properties of nodes
Initialize the ANN
Define parameters
Training_ data= optimize data
Group = Real and Attacker node
Epoch=1000
Training _algo=LM
Performing parameters=MSE
Neurons=60
Net= neuro $f_t(Training\_data, group, neuron)$
Net= Train (net, training data, group)
Classification=$\begin{Bmatrix} Attacker; if\ properties\ not\ match \\ Real\ node; if\ match \end{Bmatrix}$
Return $\{Classified\ node\ as\ a\ attacker\}$

I. Related work

In this section, an analysis of previous work done in various fields namely IoT, WSN, and Biometric system is provided along with their advantages, outcomes and methods used in the research work.

Table 4: Comparative analysis of WSN and IoT

References	Methods used	Advantages	Outcome
[21]	SNAIL (Sensor Networks for an All-IP World) protocol, IP adaptation, IPV4 and IPV6	Better network management Good QoS	The average synchronization error calculated for hope1, hope2, and hope 3are 542.875 µs, 593.636 µs, and 788.246 µs respectively.
[22]	Cryptography, KMS	Provide secure channel	Existing key management system

	protocol	The overall scalability is better	has been used for clustering link layer keys among neighboring nodes.
			This research has presented a thorough study for all the possible scenarios that may detect IoT
[23]	RFID (Radio Frequency Identification), Pyroelectrin infrared	The proposed system have low cost, sensing motions.	The parameters like fall and normal event has been measured.
		Easy desgining	
		Energy saving	
			The quantization bit is of 8 bit.
[24]	ABC (Artificial Bee Colony)	The coverage rate of the network is maximized.	ABC has performed better than Particle swarm optimization (PSO)
[25]	A new energy efficient centroid-based routing protocol (EECRP)	Low cost	The energy of source as well as destination node has been determined.
		Good scalability	
			EECRP routing protocol consume less energy to transmit data.
[26]	Track Maison framework. This frame work gathers the data usages, activities, positions from the total of five social networks., Support vector machine (SVM)	High service scalability	The genuine users are identified with 3% of disruption rate whereas the users can kept the devices upto 90% of the time without any disruption.
		High rejection rate	
		Verification of genuine users increases	
[27]	Artiificial Bee Colony (ABC), Continuous authentication (CA), face recognition	Increased security	The recognition accuracy increased from 3.13 % to 83.75%.
[28]	Artiificial Bee Colony (ABC), genetic algorithm (GA)	The average classification error is high for large Kernel size	The parameters such as average classification time, Average classification error, error percentage have been calculated.
		Average computational time is lower	
			It is concluded that ABC algorithm perform better than genetic algorithm.
[29]	Neural network, Back propagation network and Radial basis function	The proposed method can be used for moving images and with different backgrounds	The average recognition accuracy is high when BPN and RBF algorithms used in combination

CONCLUSION

IoT has been gradually bringing a sea of technological changes in our daily lives, which in turn helps to develop our life simpler and more comfortable, through various technologies and applications. There is innumerable usefulness of IoT applications into all the domains including medical, manufacturing, industrial, transportation, education, governance, mining, habitat etc. Though IoT has abundant benefits, there are some flaws in the IoT governance and implementation level. This survey implies a comprehensive analysis of the development of IoT system to prevent the wireless sensor network from the intruders. This literature survey aimed to secure the data in wireless sensor network using the IoT system. The analysis of this study allows to better understand which nodes in the network has provided better security of data during the transmission and how they can be authenticated. Future lies in developing an IoT system in wireless sensor network using the biometric fusion concept based on the optimization algorithm along with the classifier.

References

1. Kulkarni, A., & Sathe, S. (2014). Healthcare applications of the Internet of Things: A Review. *International Journal of Computer Science and Information Technologies*, *5*(5), 6229-32.
2. Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25*(9), 1101.
3. Kopetz, H. (2011). Internet of things. In *Real-time systems* (pp. 307-323). Springer US.
4. Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, *57*(3), 221-224.
5. Yang, S. H. (2014). Internet of things. In *Wireless Sensor Networks* (pp. 247-261). Springer London.
6. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.
7. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.
8. Kouche, A. E. (2012, June). Towards a wireless sensor network platform for the Internet of Things: Sprouts WSN platform. In *Communications (ICC), 2012 IEEE International Conference on* (pp. 632-636). IEEE.
9. Mainetti, L., Patrono, L., & Vilei, A. (2011, September). Evolution of wireless sensor networks towards the internet of things: A survey. In *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on* (pp. 1-6). IEEE.
10. Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, *10*(4), 2233-2243.
11. Monwar, M. M., & Gavrilova, M. L. (2009). Multimodal biometric system using rank-level fusion approach. *IEEE Transactions on Systems Man, and Cybernetics, Part B (Cybernetics)*, *39*(4), 867-878.
12. Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. *IEEE Transactions on pattern analysis and machine intelligence*, *22*(10), 1168-1171.
13. Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), 349-359.
14. Sharma, K., & Ghose, M. K. (2010). Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, 42-45.
15. Pandey, A., & Tripathi, R. C. (2010). A survey on wireless sensor networks security. *International Journal of Computer Applications*, *3*(2), 43-49.
16. Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv:0909.0576*.
17. Mokdad, L., & Ben-Othman, J. (2012, December). Performance evaluation of security routing strategies to avoid DoS attacks in WSN. In *Global Communications Conference (GLOBECOM), 2012 IEEE* (pp. 2859-2863). IEEE.

18. Dewri, R., Poolsappasit, N., Ray, I., & Whitley, D. (2007, October). Optimal security hardening using multi-objective optimization on attack tree models of networks. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 204-213). ACM.
19. Karaboga, D., Okdem, S., & Ozturk, C. (2012). Cluster based wireless sensor network routing using artificial bee colony algorithm. *Wireless Networks*, *18*(7), 847-860.
20. Rahman, M. S., Park, Y., & Kim, K. D. (2009, September). Localization of wireless sensor network using artificial neural network. In *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on* (pp. 639-642). IEEE.
21. Hong, S., Kim, D., Ha, M., Bae, S., Park, S. J., Jung, W., & Kim, J. E. (2010). SNAIL: an IP-based wireless sensor network approach to the internet of things. *IEEE Wireless Communications*, *17*(6).
22. Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. *Computers & Electrical Engineering*, *37*(2), 147-159.
23. Luo, X., Liu, T., Liu, J., Guo, X., & Wang, G. (2012). Design and implementation of a distributed fall detection system based on wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, *2012*(1), 118.
24. Ozturk, C., Karaboga, D., & Gorkemli, B. (2011). Probabilistic dynamic deployment of wireless sensor networks by artificial bee colony algorithm. *Sensors*, *11*(6), 6056-6065.
25. Shen, J., Wang, A., Wang, C., Hung, P. C., & Lai, C. F. (2017). An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT. *IEEE Access*, *5*, 18469-18479.
26. Anjomshoa, F., Aloqaily, M., Kantarci, B., Erol-Kantarci, M., & Schuckers, S. (2017). Social Behaviometrics for Personalized Devices in the Internet of Things Era. *IEEE Access*, *5*, 12199-12213.
27. Tsai, P. W., Khan, M. K., Pan, J. S., & Liao, B. Y. (2014). Interactive artificial bee colony supported passive continuous authentication system. *IEEE Systems Journal*, *8*(2), 395-405.
28. Chakrabarty, A., Jain, H., & Chatterjee, A. (2013). Volterra kernel based face recognition using artificial bee colonyoptimization. *Engineering Applications of Artificial Intelligence*, *26*(3), 1107-1114.
29. Nandini, M., Bhargavi, P., & Sekhar, G. R. (2013). Face recognition using neural networks. *International Journal of Scientific and Research Publications*, *3*(3), 1.

Manpreet Kaur Maan (Research Scholar) Desh Bhagat University,working as assistant professor in Sggs College,Sec-26,chd.She has 10 years teaching experience in computer science field. Her five papers has been published in national and international journals. Her teaching interest in computer networks and artificial intelligence.

Sawtantar Singh Khurmi ,Professor in CSE ,Desh Bhagat university, Mandi Gobindgarh.