Security Techniques in Internet of Things (IoT)

Article *in* SSRN Electronic Journal · January 2018

DOI: 10.2139/ssrn.3170187

Dr Kamna Solanki
Maharshi Dayanand University
58 PUBLICATIONS **38** CITATIONS

Sandeep Dalal
Maharshi Dayanand University
39 PUBLICATIONS **44** CITATIONS

Security Techniques in Internet of Things (IoT)

***Nishika*[a], *Dr. Kamna Solanki*[b] , *Dr. Sandeep Dalal*[c]**

[a]*Research Scholar (CSE), UIET, MDU, Rohtak,India*

[b]*Assistant Professor (CSE), UIET, MDU, Rohtak,India*

[c]*Assistant Professor,DCSA, MDU, Rohtak,India*

Abstract: IOT refers to an area in which two or more than two technologies combine together to enhance the possibilities of the current world. Any technology is not hundred percent threats proof and IOT is not different. This paper is an analytical review of the security threats in the IOT field and the prevention techniques. The paper includes two different technologies namely Biometrics and the Wireless Sensor Network / MANET. The facial recognition system is analysed as the authentication mechanism in any IOT network and WSN is treated as the core data transfer network. Pros and cons of each segment are also discussed in the paper.

Keywords: IOT, Face Recognition, WSN/MANET, Security threats.

1. Introduction

The initiation of Internet, Sensors, wireless communication with another technology has altered the behaviours of the human life. We are now living in a world that is completely surrounded by the Smart things or simply stated as Internet of Things. [1]. The period of the IoT (Internet of Things) have completely reformed an approach of human life, which can be easily evidenced through its several applications in countless fields for instance, construction of smart cities, handling the resources of energy with networks, transportation, logistics, mobility and so on. The Internet of Things is an evolving subject that possesses mechanical, social, and commercial worth.

The term "Internet of Things" refers to such a scenario where the connectivity of network and computing skills extends to, sensors, objects, and conventional items that are not frequently regarded as computers, letting these devices to produce, swap and spend data with least human involvement. [2].

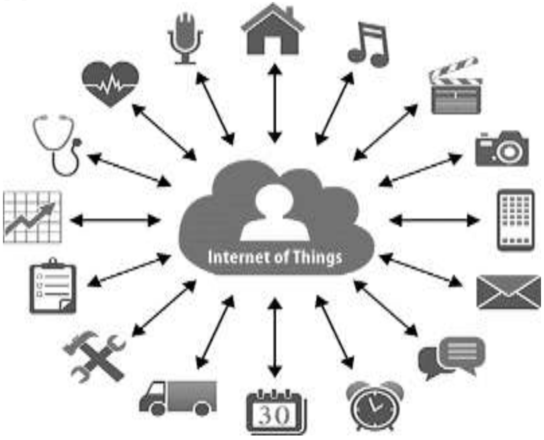

Fig. 1- Internet of Things

It is simply a global network of the things that are uniquely accessible and interlinked on the basis of standard transmission protocols. Commercial products, sensors, robust technological devices, cars and other automobiles, trade and cost components, and additional daily articles are being merged with Internet connectivity including the persuasive data analytic abilities that assure the transformation of our working and living style.

The requirements of large-scale organizations have resulted in IoT development that insists to assist considerably from the provision and visibility, furnished by the ability to pursue all objects within sequences in which they are established. Novel IoT possessions such as applications that are Internet-enabled, home robotics elements, and energy saving tactics are drawing us closer towards the idea of the "smart home'', rendering more security and energy proficiency [3]. Some particular IoT projects like wearable articles, fitness surveying instruments, and network approved health equipments are advancing the mode of the healthcare services that were being provided previously. IoT ensures to be beneficial by empowering the individual persons having inabilities and the aged ones with an enhanced level of freedom and essence of living at a reasonable cost. The IoT systems, for instance, interacted Automobiles, embedded sensors in roads, smart traffic systems, and flyovers draw us closer towards the hypothesis of "intelligent cities'', that minimizes congestion and consumption of energy resources. IoT technology bears the possibility to revolutionize farming, activity, and power generation and supply by proliferating the receptiveness of information accompanying the utility succession of production through the networked sensors.

The unimaginable quantity of information which is apprehended by the plenty of intelligent devices offers remarkable possibilities to make a judgment regarding the world in our surroundings. Social activities in the public spots may be occupied by the monitoring cameras, trails of our location can be enumerated by the cell phone sensors, individual behaviours would be judged with the accomplishment of the jobs having daily objects, civic transit accounts that could be grasped when we utilize credit or debit cards, instant travel information can be obtained from the buses, cars, and cabs rigged with GPS facility [4]. Apparently, such events and activities omit digital trails which can be fused into the widespread description of human day-to-day facades, with the vision to remodel the perception of our persistence, establishments, as well as communities.

IoT technology lures plentiful consideration as the commercial prosperity produced by the technology. On the basis of data being shared with the "Things" on Internet, one of commercial viability is based. The data shared on the Internet is interpreted as information for the other "Things" as an input or as reports to read for people. The data that has been shared over the Internet may be carrying delicate and secret message [5]. Therefore, it is quite necessary to protect the data that is being shared over the internet by the billions of people.

The threats regarding the personal information of the individual user have also become exceedingly critical due to the evolution of the Big Data Technology because such information could be acquired from the raw data that is exposed by the compromised objects and easily abused by the trespasser.

Although IoT technology has presented so many precious benefits to humans, it has also revealed us to various distinctive varieties of security risks concerning our everyday living. Most of the security risks before the invention of IoT technology were merely associated with the information exposure and the failure of service [6]. Now with IoT, security risk came to be closely linked to our explicit endurance and can undeviatingly lead to physical security threat.

2. Related Work

This section defines the work done in the field of IoT. Table has been given below that defines the work by means of the work done (proposed work) with the conclusion and the research gap.

Table 1 – A glance of existing techniques

Author	**Proposed Work**	**Conclusion & Research Gap**
Tome et.al. [2014]	Soft biometrics and application in person recognition at a distance	Performance metrics, like, FAR (False acceptance rate), FRR (False rejection rate), verification rate and error rate has been checked. Because of pre-processing lack, the error rate is more. The improvement in accuracy should be there for less number of errors with the utilization of accurate methods of pre-processing.
Sainiet.al. [2014]	Comprehensive biometric techniques	The research has aimed for recognizing the biometrics but did not work on biometric expressions. Improvement is there in the same case for more efficient work.
Zhou et. al. [2014]	A design framework and taxonomy for survey of single modal and multi-modal face recognition system	The researchers have presented a face recognition review for multi model and single model system. It has been analyzed that the proposed system can be more efficient when the usage of feature extraction algorithms takes place.
Phillipset. al. [2014]	Comparative analysis of human and computer performance across face recognition experiments	The researchers have designed cross model infrastructure with the comparison of machine and human performance with the utilization of varied experiments on varied faces. The under curve area doesn't came out to be acceptable with the statistical models.
Alotaibiet. al. [2015]	Proposed a authentication system for enhancing open authorization (OAuth) services security by an authentication service with face recognition system	The researchers have proposed the face recognition system having OAuth (Open authentication service with the notation of facial landmark. The authors have not focused on face liveliness detection when the authentication process takes place.

3. Security Threats in IoT

In IoT, the security threats have been organized generally into two prime classes. The threats in the first class are adjacent to CIA that is the confidentiality, the integrity, and the availability which is related to the conventional network ecosystem [7]. Though, the convolution and asperity of such threats are considerably more grievous, because of the oversize and diversity of the objects. Since, the IoT objects being deployed all around us i.e. capturing precise evaluations from heartbeats to measuring room temperature at homes, and also being used for several other purposes in diverse areas, therefore, the data dwell in the IoT ecosystem is assumed to be more secluded and vigorous. While several IoT devices accumulate an enormous amount of secret information regarding the IoT users such as their behavior, account passwords, geographical location, daily habits etc., therefore the data possessing such information is considered as private property and any detriment might expose the user's private information which a trespasser may acquire and unveil the secrecy of the IoT user.

One of the most critical problems while securing the information has been acknowledged as Privacy Preservation. For protecting the privacy of user, authentication techniques with the cryptographic tools were employed [8]. An authentication primarily certifies that merely the certified personnel possess the access to the user's personal information, whereas, the cryptographic tools ensure the security of sensitive information during the broadcast, preservation, and alteration of such information. The researches that are proposed recently regarding the privacy preservation mainly in IoT are either at a higher level or the researches that are based on physical layer transmission security. Scalability is the only prime concern that separates IoT from the legendary internet. There are about trillions of objects that are associated with the network in IoT. The devices that are connected to the network in this massive scale is quite difficult for the general naming policy to handle. Therefore, in order to render novel naming convention, the current naming policy is required to be revived or regenerated. In contrast to the naming policy, the methods regarding the identification and authentication are also required to be revived respectively. The other two fundamental challenges i.e. transparency and reliability, further make the design even more difficult concerning the identification and authentication methods [9].

Transparency is known as the main IoT secure augment. To activate the smart devices, most of the users neglect to complete the intricate configuration steps patiently. That is why almost all the settings related to configuration must be transparent to the users. The design of the authentication procedures must be as easy as feasible. Reliability is also a significant concern for the IoT ecosystem. The communication among the IoT objects is error-prone due to the restricted resources and battery potential. IoT ecosystem becomes more complex because of the heterogeneity of the IoT objects and also the employment and assessment of the IoT objects and services thereby become difficult. Furthermore, in the IoT ecosystem, debugging and repairing is also more difficult while errors occur [10]. Therefore, while the development of identification and authentication designs, not only endurance but also the simple debugging and one-step restoration must be brought to attention.

3.1 Major Threats in IoT

It is an integration of massive quantity of the inter-related IoT objects, i.e. from automobiles to wearable wireless things. Although, holding so many things interlinked can be comfortable, yet it also grants boom to lots of distinct threats. There are numerous security threats that emerge on IoT due to the distinct purposes. Some of the common security threats in IoT are as follows [11]:

- Vulnerable Web Interface

The network communication modeled in IoT object authorizes the user to interact with the object, but concurrently engage an attacker to acquire an unapproved access to the object [12]. The susceptibilities which may result to:

i. Account record
ii. Frail Default Authorizations
iii. Identifications Visible during Web Traffic
iv. Cross-site Scripting (XSS)
v. SQL-Injection
vi. Session Managing
vii. Feeble Account Lockout Situations.

- Inadequate Authentication/Permission

A user can acquire advanced levels of access than permitted due to the faulty objects being dwelled to authorize the IoT user interface or imperfect authorization tools, which leads to the initiation of these threats [13]. The weaknesses that may result to the threat are defined below:

i. Absence of code word Complication
ii. Badly Protected IDs
iii. Requirement of Two Factor Verification
iv. Anxious Password Regaining
v. Beneficial Boom
vi. Absence of the control of Role Based Access.

- Vulnerable Network Services

A trespasser acquires informal authorization to the object or associated information by employing the liabilities for the services of network for accessing the object, which leads to this threat [14]. The liabilities that may result to the threat are defined below:

i. Unprotected provisions
ii. Excessive buffers
iii. Unlock Ports with UPnP
iv. Usable services of UDP
v. DoS (Denial-of-Service) via Network Device Fuzzing

- Deficiency of Transport Encryption

This threat primarily associates with the data in an unencrypted composition that is being transacted among the IoT objects. A trespasser could easily sniff the data and then apprehend this data for the future practice or jeopardize the object itself [15]. The following possibilities could result to the threat:

i. Services being unencrypted via Internet
ii. Services being unencrypted via Limited network
iii. Inadequately used SSL/TLS
iv. Miss-configured SSL/TLS

- Privacy Involvement

The acquisition for particular data with the requirement of an appropriate protection to the data leads to the emergence of Privacy concerns. It is quite easy to determine the privacy concerns as the user fixes and originates the object by merely studying the data that is being collected [16]. Actual designs of data that defines the gathering of personal data or more sensible data can also be explored by engaging computerized instruments. Gathering of Redundant individual Information may result into threat occurrence.

- Susceptible Cloud Interface

This threat primarily correlates with the matters that are linked to interface of cloud employed for interacting with IoT objects [17]. It may generally allow an invader to obtain access to the object or the sensitive data which ultimately signify the deprived authentication instruments or data roaming in the format which is unencrypted. Subsequent vulnerabilities may result to the threat:

i. Account details

ii. No Account exclude
iii. Identifications Visible in the traffic of Network

- Vulnerable Mobile Interface

This threat is quite similar to the preceding threat, i.e. the attacker procures an access to the object or crucial data for IoT device which employs the interface of vulnerable mobile for user alliance because of the ineffective authentication or unencrypted data flows [18]. The following vulnerabilities could lead to this threat:

i. Account details
ii. No Account keep out
iii. Identifications Visible in the traffic of network

- Poor Security Configurability

When users of the IoT objects holds poor or not any experience to revise its security restraints then Poor security configurability exists. The configuration of poor security is possible as the object network interface left negative options for producing rough user authorization, like, inflicting utilization of tough passwords [19]. The threat involved here is to IoT object which may sensitive towards attack sanctioning an unapproved execution for the objects/ the crucial data. The weaknesses that may result to the threat are as follows:

i. Absence of the model of Granular Permission
ii. Nonexistence of the options of Password Security
iii. No Security observation
iv. No Security Logging

- Vulnerable Software/Firmware

The lack of expertise for an object to be reorganized exhibits a security weakness on its own. IoT objects must hold the expertise to be rearranged while the weaknesses are revealed with the updates of software/firmware that could be unpredictable while the efficient record itself plus the arrangement of network being executed. Software may be problematic if the holding of hardcoded obscure data, for instance, IDs [20] takes place. The unsuccessful attempt of software/firmware for being updated indicates that the object endures vulnerabilities to the security dilemma that the update is designed to inscribe. The security dangers that could lead to this threat are as follows:

i. Encryption which is not exploited to attain reviews
v. Reviewed File being non-Encrypted
vi. No updation before the updation
vii. Firmware Comprises Complex Information
viii. Functionality of noticeable updates

- Inadequate Physical Security

When an attacker dismantles objects to directly access the storage tool and the data kept on that tool, then Physical security defect persists [21]. Defects also exist when the ports of USB with more external ports could be employed for entering the object utilizing the peculiarities anticipated for development. It may impart an obvious access to the unapproved attacker to the object or the crucial information. The security vulnerabilities that could lead to this threat are defined below:

ii. Acquiring software through USB Ports
iii. Exclusion of Storage Media

There are several activities that have already captured the public attention, such as the hacking of Internet-connected devices, surveillance concerns, and discretion fears. Due to lack of strong security foundations, the attacks and flaws in IoT definitely surpass its advantages. Since IoT is more than merely an insight, it can entirely develop via paradigm that may open several characteristics of everyday life by just merging it with security provisions. In IoT, the security is provisioned for the secure treatment of the user's information. For rendering the protection versus amount of threats, traditional approaches are not enough successful where the access to the object is granted on the basis of alphanumeric passwords, PINs, smart cards, tokens, keys etc. The Passwords, PINs, keys, and tokens might be omitted, lost, stolen or sometimes get compromised. But the Biometric characteristics are the distinct and practically fool proof physical security approach that is utilized for the verification of the human identity.

4. Role of Biometric Security in handling IoT threats

The term “Biometric” is the “Greek word”, “bio” signifies ‘life’ and “metric” signifies ‘to measure’ [22]. It is primarily delineated as the sole characteristics or traits of human body that are employed to identify human’s identity.

Biometric-based approaches has recently emerged as the utmost capable method for distinguishing people, as a replacement for verification of an individual and allowing them the access to dynamic or virtual domains on the basis of the alphanumeric passwords, PINs, smart cards, tokens, keys etc. Biometric technology is primarily employed for the automatic recognition of the human beings on the basis of their physiological attributes or behavioral characteristics [23]. “Passwords, keys, and tokens” may be missed or else may be negotiated whereas the biometric technique is the unique and flawless physical security technique which is utilized for the verification of an individual person.

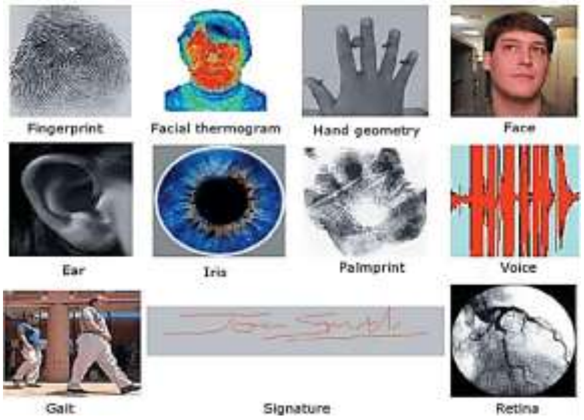

Fig. 2- Types of biometric traits of human body

For the purposes of authentication, verification, and identification, Biometric security turns out to be the most advanced technology that allows the customers to confirm their online activity through fingerprint or voice recognition software as acquainted by the banks to provide online access to the clients regarding their accounts.

The five integrated components that are required to be contained by a characteristic Biometric System are:

Sensor can capture the data and exchange it into a digital format. Signal processing algorithm to execute quality check procedures and generate biometric templates. A data storage element that stores data which will be later compared with fresh biometric templates [24]. A matching algorithm which is required to match the fresh biometric templates with multiple templates stored in the data storage. Finally, a decision procedure that utilizes the results produced by the matching algorithm in order to execute a system-level decision.

Biometric security is primarily employed in the environments with grave physical security provisions or that are exceedingly susceptible to identity theft. Biometric-based security systems or machines stock human body features that do not vary throughout a person's lifetime [25]. An individual's body traits are pre-stored in a biometric security system or scanner, which may be retrieved by approved personnel. As soon as an individual step into a facility or attempts to obtain admittance to a system, the biometric scanner assesses his/her bodily traits, that are coordinated with warehoused records. If a match is achieved, then the access is granted to the individual.

4.1 Usefulness of Biometrics for Security

Biometrics, or using the bodily features in order to access protected systems, is the next-generation resolution to fortifying information and locations. One step ahead from passwords, and two steps ahead from the traditional keyed locks, biometrics offer a real-world, convenient, layered security solution that is no match for even the utmost devoted hacker. There are sure reasons to pick biometrics for the determination of security in various applications [26]. The following are the utmost mutual reasons that states biometrics as a safe method to be employed for verification of the human's identity.

i. Uniqueness: The biometric characteristics i.e. physical or logical are constantly unique for every single human being. The probability of 2 people sharing the similar biometric data is almost nil. The numerous biometrics systems have been established over the unique bodily characteristics of individuals.

ii. Cannot be shared: As biometric asset is an innate property of an individual, it is tremendously hard to replica or share [27]. A person can never provide a replica of his/her face or hand to someone else for the purpose of identity verification. Thus, the biometric traits can never be shared with others.

iii. Cannot be forged: Biometric features of a distinct human being are nearly impossible to forge or deceit, precisely with the dawn of numerous new technologies certifying that the biometric which is being recognized belongs to a live person.

iv. Cannot be lost: As the biometric features are innate and unique assets of an individual and in contrast to passwords, PIN, tokens, etc., they are not mandatory to be recalled. A biometric asset of an individual can only be misplaced in the event of serious accident.

v. More efficient: Biometric verification is an effective method to verify the human identity because the biometrics of an individual human beings cannot be imitated [28]. A Trusted Execution Environment is included in the biometric devices that separate the management of biometric information from the device's operating system. This makes it practically impossible for the hackers to falsify the process of authentication, as there is no way of utilizing malware and other viruses in order to manipulate the concluding results.

There are various modalities of biometrics which can be employed in the process of authenticating the human identity. These modalities mainly comprises of "fingerprints, eye texture, voice, hand patterns and facial recognition" and so on [29]. Though, among all the available modalities of biometrics, fingerprint authentication has been the most widely utilized modality for the identification of human beings and has been well accepted in emerging nations, but still using fingerprints for authentication purpose is not appropriate in the circumstances where people have no finger or else the finger has been mutilated; situations where identification needs to be done quickly because of time limit [30].

Therefore, face recognition system is integrated in this research work for security purpose in the internet of things to confirm the authentication of the user and provide the access to private information. The user's face image is firstly captured and kept in the database, which is then encrypted in order to defend discretion of the user. When user request online-access to the personal information at that point the face captured previously is matched with the image deposited in the database. If both the images matched precisely then the access is permitted to the user, or else the access is denied.

4.2 Face Recognition System

The human face is the easiest feature that can be employed in the security system based on biometrics in order to recognize a person. Face recognition technology, is extremely famous and is adopted more extensively as there is not any requirement of the physical contact between the users and the equipment [31]. Cameras initially browse the user's face and then match it to the stored database for authentication. Furthermore, it is quite simple to establish and does not claim an overpriced hardware. This technology is broadly adopted in a variety of security schemes such as corporal access control or computer user accounts. Face Recognition is basically determined as the task of recognizing a previously detected face as a well-known or a strange face.

The system involving face recognition is designed to offer a precise and constant mode for identifying the face of an individual human being [32]. Face recognition is among the few biometric techniques that hold the qualities of both extraordinary accuracy and low intrusiveness. It deals with automatically recognizing or validating person as of a digital image/video by matching selected facial features. It is a kind of identity access management and access control. Moreover, it is viewed as a passive and non-interfering strategy for authenticating and recognizing people. Though there are additional methods of identification like the PIN (personal identification number), password, signature, fingerprints, iris, palmprint, hand, etc., yet in few situations, it is satisfying to possess an identification technique that resembles the way human beings identify each other.

The biometric face recognition systems will initially gather the data from users' face and store them into a database for imminent use. Afterwards, it will measure the complete outline, arrangement and amount of characteristics on user's face such as gap in-among the eyes, nose, ears, jaw, mouth, eyes size mouth and others characteristics. It is considered as the constituents for fluctuating via the process of the facial recognition. The examples typically involve smiling, weeping, and wrinkles on the face [33].

Two objectives are there for recognition of face, termed as verification and identification. A face image is provided to the system in face identification to state that defines the approx identification while the face verification has provided the identification estimation and face image for assuming the conditions.

Below figure demonstrates the steps that are involved in the process of facial recognition for the identification of face image as recognized or unrecognized face.

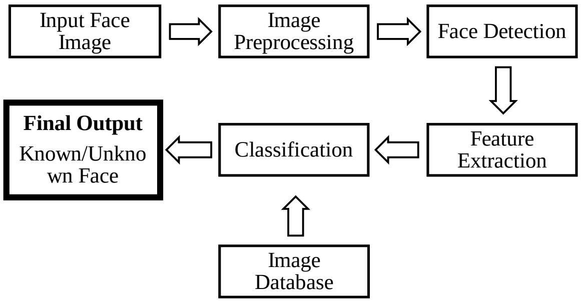

Fig. 3. General Face Recognition System

4.3 Steps of Face Recognition system

The steps of face recognition system are defined below:

- Image Pre-processing

In this step, initially the face images are pre-processed and enhanced in order for enhancing image quality by removing the noises and redundancies from the input image. This step of removing noises from the image is considered as the most significant task in the entire process as the noisy image may possibly affect the accuracy of face recognition and also affects the overall performance of the system [34]. Pre-processing is done for the following two purposes:

i. To reduce noise and probable convolute interfering system consequence,

ii. To change the image in varied space where classification might established easier by some features exploitation.

- Face Detection

The face detection in some image might be simple process for human being but not in case of PCs that chooses the image pixels as face part. In the passport snap, in which the clarity of background is there with the easiness but when the problem of clarity occurs, the issue resulted to be composite. This procedure is the process of face extraction by means of input image. Therefore, the system recognizes some images of face. It is very effective in compression, pose estimation and face tracking as well.

- Feature Extraction

Facial feature extraction is the process of translating the input data into some set of features. The feature points like eyes, nose, mouth is extracted and afterwards employed as input data to application. As soon as, the face is spotted from the input image, the feature extraction from the face will take place. In feature extraction, a mathematical illustration termed as biometric template or biometric reference is created, which is kept in the database and this will form the basis of any recognition task. The features being extracted may be some of the regions of face angles, the measures related to human. The uniqueness of the extracted feature sets is directly proportional to the recognition rate.

Feature extraction can help reduce huge amount of data to a relatively small set which is computationally faster [36]. It is influenced by many complications like difference in different pictures of the same facial expression, the light directions of imaging, and the variety of posture, size and angle. The prime focus of the feature extraction techniques is the extraction of accurate features from face image.

Directly using the human-face patches that are extracted from images, for recognition of face have few disadvantages. Primarily, every patch frequently covers above than 1000 pixels, which is quite huge to construct a tough recognition system. Secondly, the face patches might be occupied by means of diverse camera positions, with diverse face expressions, lights, and might experienced from occlusion as well as clutter. Therefore, feature extraction is performed to avoid these drawbacks and also to execute the arrangement of information, reduction of dimension, extraction of salience, and cleansing of noise. Feature extraction is also named as Dimensionality Reduction and is frequently carried out by employing Principle component analysis (PCA) [37].

- Classification

Classification methods are used in many areas like finance; signal decoding, voice recognition, data mining, natural language processing or else medicine. After the completion of the feature extraction, the subsequent step is the selection of extracted features subset, which is generally done by employing classification method [38]. At this stage, every possible subset of the extracted features is examined and the one that fulfils the criterion function is selected. In this step, the image is classified with the help of an appropriate classifier. Appearance-based face recognition algorithms use a wide variety of classification methods. Sometimes two or more classifiers are combined to achieve better results. On the other hand, most model-based algorithms match the samples with the model or template. Then, a learning method is can be used to improve the algorithm.

Normally, the classification algorithm has few types of learning, namely, unsupervised, and supervised [39]. The unsupervised learning is tough approach, as there are no marked instances. Though, number of applications of face recognition with the subject tagged sets. Consequently, most face recognition systems implement supervised learning methods. There are some stages in which the labelled sets are small. Occasionally, novel tagged sample acquisition may be infeasible. Therefore, semi-supervised learning is required.

The final output after the classification is then matched with the template or the image stored in the database with the help of a matching algorithm [40]. A matching algorithm compares the new biometric template to one or more templates stored in database. Finally, a decision process (either automated or human-assisted) uses the results from the matching module to make a system-level decision [41]. If the match is located, then the individual is granted the access.

5. Conclusion

In this paper, the main focus is placed on security of the Internet of Things for avoiding the intrusion attacks having a trespasser gain access by hacking the accounts due to insecure authorization and significant or confidential information gets compromised. Due to the inefficiency of the traditional approaches like security through PIN, Passwords, Tokens, etc. that are easily faked, forgotten or lost, biometric based security is considered in this paper, as it is the strongest and most fool proof physical security technique used for identity verification. An individual's body characteristics are pre-stored in a biometric security system or scanner, which may be accessed by authorized personnel. Biometric characteristics includes fingerprint, voice, Iris, hand geometry, palmprint, signature, face, gait, etc.

Embedding face recognition approach into the security of Internet of Things allows people to flawlessly communicate and interact with the Internet of Things, creating a link between physical and digital worlds to an extent previously unknown.

REFERENCES

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

Hwang, Y. H. (2015, April). Iot security & privacy: threats and challenges. In Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security (pp. 1-1). ACM.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261-274.

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.

Oweis, N. E., Aracenay, C., George, W., Oweis, M., Soori, H., & Snasel, V. (2016). Internet of Things: overview, sources, applications and challenges. In Proceedings of the Second International Afro-European Conference for Industrial Advancement AECIA 2015 (pp. 57-67). Springer, Cham.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer law & security review, 26(1), 23-30.

Misra, S., Maheswaran, M., & Hashmi, S. (2017). Securing the Internet of Things. In Security Challenges and Approaches in Internet of Things (pp. 39-51). Springer, Cham.

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.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

Zhang, Z. K., Cho, M. C. Y., & Shieh, S. (2015, April). Emerging security threats and countermeasures in IoT. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 1-6). ACM.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

Kozlov, D., Veijalainen, J., & Ali, Y. (2012, February). Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks (pp. 256-262). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Covington, M. J., & Carskadden, R. (2013, June). Threat implications of the internet of things. In Cyber Conflict (CyCon), 2013 5th International Conference on (pp. 1-12). IEEE.

Cvitić, I., Vujić, M., & Husnjak, S. (2016, January). Classification of security risks in the IoT environment. In 26th Daaam International Symposium on Intelligent Manufacturing and Automation (pp. 0731-0740).

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. Computer, 46(4), 46-53.

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT applications and service domains. Wireless Personal Communications, 95(1), 169-185.

Bhattasali, T., Chaki, R., & Chaki, N. (2013). Study of security issues in pervasive environment of next generation internet of things. In Computer Information Systems and Industrial Management (pp. 206-217). Springer, Berlin, Heidelberg.

Ahmed, A. W., Ahmed, M. M., Khan, O. A., & Shah, M. A. (2017). A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 8(7), 489-501.

Misra, S., Maheswaran, M., & Hashmi, S. (2017). Vulnerable Features and Threats. In Security Challenges and Approaches in Internet of Things (pp. 19-38). Springer, Cham.

Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In The Internet of Things (pp. 389-395). Springer, New York, NY.

Ashok, J., Shivashankar, V., & Mudiraj, P. V. G. S. (2010). An overview of biometrics. International Journal on Computer Science and Engineering, 2(7), 2402-2408.

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An introduction to biometric authentication systems. In Biometric Systems (pp. 1-20). Springer London.

Jain, A. K., & Kumar, A. (2012). Biometric recognition: an overview. In Second generation biometrics: The ethical, legal and social context (pp. 49-79). Springer, Dordrecht.

oss, A., & Jain, A. K. (2007, January). Human recognition using biometrics: an overview. In Annales Des Télécommunications (Vol. 62, No. 1-2, pp. 11-35). Springer-Verlag.

Tome, P., Fierrez, J., Vera-Rodriguez, R., & Nixon, M. S. (2014). Soft biometrics and their application in person recognition at a distance. IEEE Transactions on information forensics and security, 9(3), 464-475.

Furnell, S., & Evangelatos, K. (2007). Public awareness and perceptions of biometrics. Computer Fraud & Security, 2007(1), 8-13.

Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. IEEE Access, 2, 1530-1552.

Siddique, K., Akhtar, Z., & Kim, Y. (2017). Biometrics vs passwords: a modern version of the tortoise and the hare. Computer Fraud & Security, 2017(1), 13-17.

Saini, R., & Rana, N. (2014). Comparison of various biometric methods. International Journal of Advances in Science and Technology, 2(1), 24-30.

Zhou, H., Mian, A., Wei, L., Creighton, D., Hossny, M., & Nahavandi, S. (2014). Recent advances on singlemodal and multimodal face recognition: a survey. IEEE Transactions on Human-Machine Systems, 44(6), 701-716.

Ding, C., & Tao, D. (2016). A comprehensive survey on pose-invariant face recognition. ACM Transactions on intelligent systems and technology (TIST), 7(3), 37.

Phillips, P. J., & O'toole, A. J. (2014). Comparison of human and computer performance across face recognition experiments. Image and Vision Computing, 32(1), 74-85.

Park, Y. Y., Choi, Y., & Lee, K. (2014). A study on the design and implementation of facial recognition application system. International Journal of Bio-Science and Bio-Technology, 6(2), 1-10.

Dehghani, A., Moloney, D., & Xu, X. (2017, May). Face detection speed improvement using bitmap-based Histogram of Oriented gradien. In Systems, Signals and Image Processing (IWSSIP), 2017 International Conference on (pp. 1-5). IEEE.

Agrawal, N. J., & Ladhake, S. A. (2016). Anti Theft Mechanism through Face Recognition. International Journal, 4(5).

Lwin, H. H., Khaing, A. S., & Tun, H. M. (2016). Automatic door access system using face recognition. International Journal of Scientific & Technology Research, 4(6), 210-221.

Sathe, I., Patel, C., Mahajan, P., Telang, T., & Shah, S. (2017). Automatic Locking Door Using Face Recognition.

Alotaibi, A., & Mahmmod, A. (2015, May). Enhancing OAuth services security by an authentication service with face recognition. In Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island (pp. 1-6). IEEE.

Xavier, S., & Paul, V. (2016). Face and Facial Expression Recognition for Security and Identification. International Journal of Engineering Science, 6856.

Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (2016). Face recognition for authentication on mobile devices. Image and Vision Computing, 55, 31-33.

Satari, B. S., Rahman, N. A. A., & Abidin, Z. M. Z. (2014, August). Face recognition for security efficiency in managing and monitoring visitors of an organization. In Biometrics and Security Technologies (ISBAST), 2014 International Symposium on (pp. 95-101). IEEE.

Sultana, M., & Gavrilova, M. L. (2014). Face recognition using multiple content-based image features for biometric security applications. International Journal of Biometrics, 6(4), 414-434.

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: a comprehensive survey. ACM Computing Surveys (CSUR), 50(1), 8.

Best-Rowden, L., Han, H., Otto, C., Klare, B. F., & Jain, A. K. (2014). Unconstrained face recognition: Identifying a person of interest from a media collection. IEEE Transactions on Information Forensics and Security, 9(12), 2144-2157.