An Investigation on Biometric Internet Security

Omprakash Kaiwartya[1], Mukesh Prasad[2], Shiv Prakash[3], Durgesh Samadhiya[2], Abdul Hanan Abdullah[1], Syed Othmawi Abd Rahman[1]

(Corresponding author: Omprakash Kaiwartya)

The Faculty of Computing, Universiti Teknologi Malaysia[1]
UTM Johor Bahru, 81310 Johor, Malaysia
National Chiao Tung University, Hsinchu, Taiwan[2]
Hsinchu 30041, Taiwan (R.O.C.)
Indian Institute of Technology, New Delhi 110016, India[3]
(Email: omprakash@utm.my)

(Received Oct. 17, 2015; revised and accepted Jan. 23 & Feb. 28, 2016)

Abstract

Due to the Internet revolution in the last decade, each and every work area of society are directly or indirectly depending on computers, highly integrated computer networks and communication systems, electronic data storage and high transfer based devices, e-commerce, e-security, e-governance, and e-business. The Internet revolution is also emerged as significant challenge due to the threats of hacking systems and individual accounts, malware, fraud and vulnerabilities of system and networks, etc. In this context, this paper explores E-Security in terms of challenges and measurements. Biometric recognition is also investigated as a key e-security solution. E-Security is precisely described to understand the concept and requirements. The major challenges of e-security; namely, threats, attacks, vulnerabilities are presented in detail. Some measurement are identified and discussed for the challenges. Biometric recognition is discussed in detail wit pros and cons of the approach as a key e-security solution. This investigation helps in clear understating of e-security challenges and possible implementation of the identified measurements for the challenges in wide area of network communications.

Keywords: Biometric, denial of service (DoS), e-network, e-security, electronic data storage, highly integrated computer-networks, malicious code threats, passive active attacks, recognition and biometric systems

1 Introduction

Information Technology has become one of the prominent support structure for any organization in this modern era. The primary goal of the technology is to provide efficient and secure flow of information flow in the organization. The present age is running on the wheels of information technology, computational devices and other value added services. Security of data has become increasingly important in any organization, and thus; organizations are working hard in their information security systems for implementing the effective and recent security approach and risk management techniques. Information security system always considers information a critical component of the organization. Protection and security of information has evolved due to unauthorized and non-authenticated changes in information of any organization.

With the rapid evolution of Internet in the last decade, e-security has become the heart of every organization. E-network based organizations can be secured with the use of modern e-security techniques. E-security provides an open and easy communication on a global platform. Network experts, administrators and data center professionals are needed to conceive the basic of security in order to carefully expand and managed today's networks. However, in recent knowledge-based economy, both the private and government organizations are using the advancements of e-revolution.

Organizations regularly observes information as an necessary resource. Data center strategic input and output has been accentuated. With the regular need of the services of e-network based systems, e-security becomes essential for almost every organizations particularly based on e-network systems. With the increasing number of computational devices connected to the network using information technology, the network security problem is becoming increasingly crowded [4].

Network security risk arises both in public as well as corporate sectors. According to the government point of view, anticipation needs to be enforced early on to counter the damage of society in terms of information security [2, 5, 26].

2 E-Security

In this section, e-security is precisely explored. E-security stands for "cyber-security", "Internet-security" as well as "IT-security".

1) E-security or electronic information security means protection of important data and information from undefined and unauthorized disclosure, transfer, modification and deletion of the information.

2) It is concerned with the security of any data that passes over the e-network in electronic form.

3) It mainly deals in securing both information as well as the network(s) through which information flows.

4) E-security is protecting an organization from internal as well as external threats and attacks.

5) It protects information networks and communication networks from the unauthorized use of the information.

6) E-security also secures the intranet, extranet from the outside world.

Due to the wide spread range, vast and continuously changing nature of communication network and environment, solutions derived e-security should be flexible, adaptable and able to detect and provide solutions to different security threats. The solutions should fulfil the requirements of the organization that are based on the e-network and information based systems.

3 Challenges for E-Security

In this section, various challenges in the design of e-security solutions are discussed. There are various challenges for e-security and various measures do exist to overcome these challenges. In spite of these measures, the challenges prevail in the form of newer vulnerabilities, threats and attacks. The security challenges are of many types and manifolds and each with dire consequences if it is not addressed properly. E-security provides open and easy communications as well as secure communication through the internet and electronic media. E-Security is a continuous process by which confidential and proprietary data and information are secured from the unauthorized and non-authenticated access from outside world in the network. Some Challenges for E-Security are listed below.

1) Protect the inadequate knowledge, data, information and tools of companies and also provides the security to internal resources and network.

2) To enable the secured exchange of confidential information, by keeping unscrupulous elements out and by providing the necessary hidden policies and methods.

3) To enable controlled access to IT network and their process, consistent with defined roles and responsibilities.

4) Make-up secure, effective, efficient, robust and trusted network for important and sensitive areas.

5) Avoid attack, fraud within business processes and transaction, and also detect the affected area also release the respond to attempted attack and fraud within the network.

6) Non-availability of e-security information knowledge is great challenges for e-security.

7) Confirm that each component of the e-world or network infrastructure is accessible when needed and also develop the verification of the transaction at the time of resource sharing.

8) To maintain trust and secure platform for transaction and processing in e-network and controlled access to computer systems and their processes, consistent with defined job and responsibilities.

Iterating all possible security factors and challenges are virtually impossible, we therefore categorized these e-security challenges in three main factors: threats, attacks and vulnerabilities. All three main factors threats, attacks and vulnerabilities are discussed in detail in the next sections.

4 Threats

Security threats are an action or process which effect on the confidentiality, integrity or availability of e-network. The threat is the result of some unauthorized disclosure, unauthorized action, and data alteration comes in the network. From an e-business concern Denial of Service (DoS) attacks come out as the most serious threat. Computer security threats are no longer limited to big companies with hundreds of employees (See Figure 1). Security threats in electronic devices such as computer deals in a various ways. There are Internet-based threats, file-based threats and social engineering threats. A security threat can be defined as potential for security violation that exists according to the circumstance, capability, action or process that could crack security and cause harm. Compute security threats could be categorized in two classes; namely, malicious code threats, transmission threats. The two threats are precisely discussed below.

4.1 Malicious Code Threats

On occasion mistakenly associated only with personal computer, malicious code can attack different platforms. Malicious code can be delivered by using various methods. For example, system penetration by the act of hacking and phasing via web sites and emails. Upon successful

delivery of malicious code, the target system can be overtaken and sensitive information can be ex-filtrated. Malicious code refers to Viruses, Worms, Trojan horses, Back door installer and other "uninvited" software. Since different name of malicious code refers to different malicious behavior, malware is common used to refer any software that performs malicious behaviors.

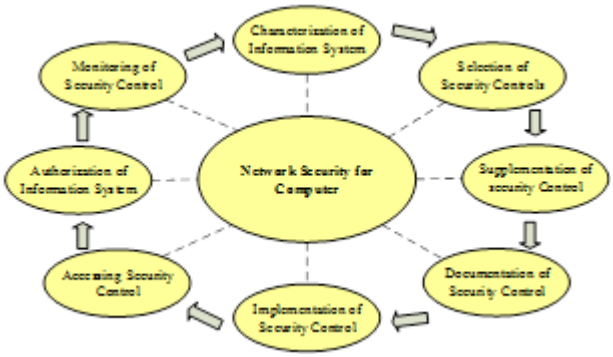

Figure 1: Network security issues

4.2 Transaction Threats

This threat happens during the huge amount of valid/invalid data is issued to a server. Because the server can only handle and process certain data threshold at any processing time or given time, the server can be overflowed with data amount that excess the data threshold vastly. As a result, the availability of the server is compromised. Generally transaction threat refers to Denial of Service (DoS), and DoS can be achieved by SYN flood, ping of death for example. Alternatively, DoS can also be achieved with large amount of legitimate requests in a short period of time

5 Attacks

Any action that makes adjustment with the security mechanism of sensitive information bought by an organization or individual is referred as attacks. The nature of attack that concerns an organization or individual varies greatly from one network to another. In general, attacks are either intentional or unintentional acts that attempt to cause of information or data loss. Ultimately all attacks are developed and originated by people with an aim to steal, cause validation, damage to the system, etc. "security attack is an attempt on system security that break up and violate the securing policy of an e-network". Security attacks are classified into two classes; namely, passive attacks, active attacks. The two attaches are precisely discussed below.

5.1 Passive Attacks

The aim of passive attack is to gain data that is being transmitted over the network. Passive attacks are in the nature of eavesdropping, and monitoring the transaction over the network. These attacks are somewhat challenging to detect because their non-involvement with any modification or alteration of information. Passive attacks can be further divided into two types:

1) Release of Message Contents: for example, eavesdropping on network transmission, detect the e-mail in the network, extracting data from the file.

2) Traffic Analysis: for example, location of data, frequency of the communication and length of the data packet.

5.2 Active Attacks

The active attacks involve with data alternation or develop the false data in the e-network. These attacks needed the attacker to be capable to transmit data to both the direction of network either may be client or server, or can block the information in one or both directions. It is also likely to perform attack like man-in-the-middle. In such scenario, the attacker can be the role of client/server during authentication procedure. The server/client will not identify that the source of the data is not the authenticated party. Active attacks may be sub-divided into four groups: Masquerade, Replay, modification message, and Denial of service.

6 Vulnerabilities

The frequent attacks during the several years, and the speed and spread of these attacks, notices a serious security vulnerability problem in our e-world. Vulnerabilities causes due to weakness of the software program or may be hardware used on a server or a client that can be exploited by a determined raider to get access to or abandon a network. We define System vulnerability as a situation, in which hacker or the attacker can access the resources and data in the absence or weakness of security constrains or technical, physical or other authorities that could be used by a threat. Vulnerabilities are flaws in a computer application that created weakness in the overall security mechanism of computer or network. Vulnerabilities in the hardware and software as well as same in policies and procedure, mainly security methods, applications and process that are using in computer networks. There is not any definite list of each and every possible sources of mentioned system vulnerabilities. The main causes of vulnerabilities are, Password management flaws, Fundamental operating system design flaws, software bugs, and unchecked user data. Some common expels of vulnerabilities are: Buffer overflows, Dangling pointers, Input validation errors, SQL injection, E-mail injection, Race condition, Simulink races, User interface failures etc.

7 E-Security Measurement And Biometric Recognition

In this section, common e-security measures have been identified and bio-metric recognition is discussed as key e-security solution.

7.1 E-Security Measurement

Effective e-security policy must consist of the objectives; namely, confidentiality, integrity, availability, legitimate use (identification, authentication, and authorization), auditing or traceability and non-repudiation. Common e-security measures are listed below.

1) Authentication: A digital certificate that approve authentication during the use of any individual's unique signing key. Basically, authentication mechanisms [6, 22] that existed today use one or more of the authenticators (factors) viz. Knowledge-based, Possession-based and Physiology-based. Knowledge-based is an authenticator only the individual knows, which typically denotes to PIN, pass phrase or a response to a secret security question. In the possession-based is an authenticator only the individual possesses, which usually refers to keys, smart cards and tokens. Physiology-based is an authenticator only the individual is or can do, referring to biometrics. Knowledge and possession-based authentication mechanisms imply that users in order to be granted access to a system, building, service - need to carry or remember the authenticator.

2) Access Controls: This limits unlike classes of users to subsets of information and make sure that they only access authorized data and services. Network constraints to safe access of other computer systems and network.

3) Encryption Policy: By this policy original data should be changed in the cipher data form for security point of view.

4) Intrusion Detection: These product monitor system and network activity to spot any attempt being made to gain access.

A major e-security policy of is ISO/IEC 27001. The main features of ISO/IEC 27001 are; namely, reviewing, the security policy, acceptable use policy. The prevention methods can be also applied for malware, such as antivirus software, firewalls deployment, preventing the download of extruder programs and documents by the Internet and make sure your staff adhere to this policy and also apply the malware alert service in computer network and system. The key components of fine-grained access control implementation in a corporate server environment. The above analysis of e-security and its measures gives some precise practices for e-security which are described in next paragraph.

Either defines, deploys organization level security policies or enabled security threat preventive measures. Check the authorization level of computer network from the outside world. With appropriate modification, these measures can also be applied in wide area of communication networks where security is prime concern during information forwarding in communication [6, 10, 11, 12, 13, 14, 15, 16, 17, 19, 32, 33].

7.2 Biometric Recognition: As a Key E-Security Solution

Biometric Recognition is the statistical analysis and measurement of folks' physical and interactive characteristics [21, 23]. The technique is primarily used for identification, access control and identifying individuals that are under surveillance. The basic evidence of biometric authentication is that each person is unique. She can be identified by her intrinsic physical or behavioral traits. The term "biometric" is consequent from the Greek words "bio" means life and "metric" means to measure. Information security is an unlimited concern to electronic users, which is not only a technical challenge, but also related to human factors. For example one of the key issues in Malaysia related to Internet banking is the pathetic security used for Internet banking application. Hence it is an important study to investigate further the solution and enhance the security issues in Internet banking applications. Modern world is fast world, billions of transactions occur each minute. On behalf of these transactions, data prerequisite to be readily available for the unpretentious. Biometric Recognition is normally considered as physiological or behavioral characteristic based recognition [3]. Physiological characteristic represents to stable characteristics of human beings including fingerprints, structure of face, eyes, ears, hands, legs, and fingers, the pattern of hairs, teeth, and samples of DNA structure. Physiological characteristics of each individual are normally permanent and distinctive. It changes only due to fatal accidents, serious illnesses, genetically induced defects, or in some cases changes due to aging. Behavioral characteristics are represented by the day-to-day way of living life by the particular human being. Interactions with other human beings are also include to measure the behavioral characteristics. Biometric recognition can be utilized as a key e-security solution. Biometric recognition generally works in five steps. The steps and the actions needs to be executed in the corresponding steps are listed below.

1) Sample acquisition: Collection of biometric data using appropriate sensors.

2) Feature extraction: Conversion of biometric data into templates.

3) Storage: Storage of templates in appropriate memory which depends on the application.

4) Matching: authentication of user by comparing bio-

metric template of the user with the existing templates stored in the database.

5) Decision: Based on the result of the matching, the user will be authorized or denied to access the resources.

Biometric system is a pattern recognition system that recognizes the user's identity through their physical or behavioral traits. For using biometric system authentication, the user has to firstly enrollment in biometric systems. Based on application context, biometric system operates in one of two modes; verification and identification for user authentication. During enrollment (cf. Figure 2), features of the individual are extracted from the sensor or user interface and converted into templates. The templates are stored in the system database. Verification (cf. Figure 3) is used for one to one match. It validates a person's identity by comparing his captured biometric traits with the specific biometric template that is stored in system database. Verification method can be used with either centralized storage or distributed storage.

In verification with centralized storage, database exists in a centralized mode in which all biometric templates are stored. From the system database, a specific template is retrieved for comparison with live person's physical or behavioral traits and both data can be either match or not. Two types of error is possible in verification; namely, false match or false positive, false negative or false rejection. In false matches or false positive, a person is not who he claims, but the system accepts it, Acceptance of pretender. In false rejection or false negative, a person is who he claims to be but the system fails to accept, rejection of legitimate person. False rejection will cause unnecessary inconvenience to an innocent individual, whereas the false match is more dangerous as they allow an imposter to pass.

In verification with distributed storage, biometric data stored in a memory device that is carried by individual, for example, smart card in which biometric data of individuals are stored. Verification is done by comparing biometric data which are provided by an individual's memory device like smart card with a specific template stored in the system database. Like, verification with centralized storage, false acceptance and false rejection errors are possible Verification with distributed storage technique. Unlike, verification with centralized storage, memory device like token or smart card can be damaged or can be tampered.

Identification (cf. Figure 4) is used for one to many matches in biometric recognition process. In particular, it is used to discover the identity of a person when the identity is unknown; in this mode biometric data of the individual is captured and compared with all templates which stored in the system database. To determine the identity of the unknown person, database of templates is required that contains biometric templates of all people known to the system. Identification not possible without database of templates. Like verification, identifica-

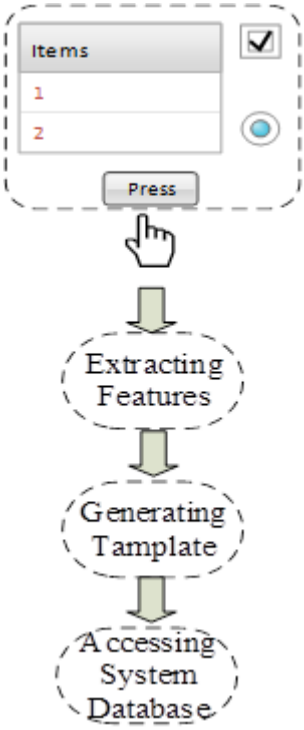

Figure 2: Enrollment in biometric recognition

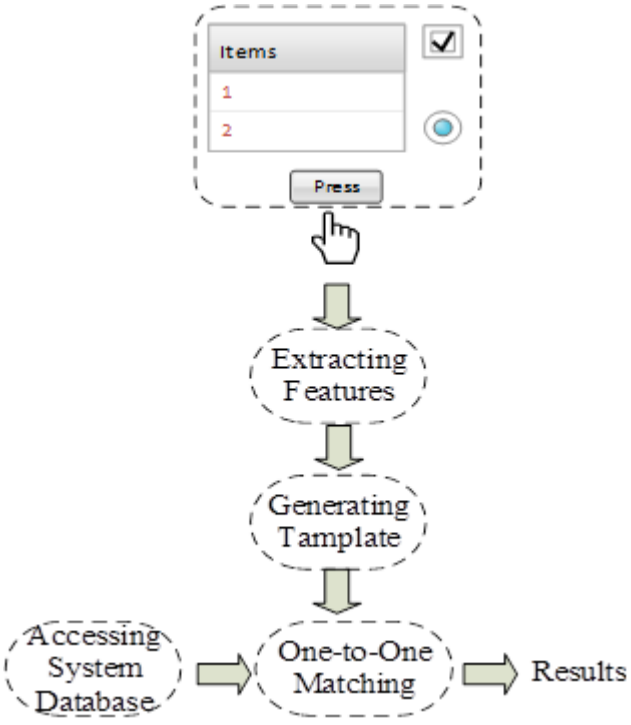

Figure 3: Verification in biometric recognition

tion can also produce two types of error, false match or false reject. There are two types of biometrics; namely, physical traits, behavioral traits (cf. Figure 5). physical biometrics includes five factors of physical attributes that can be used for user authentication. The five factors are discussed below.

1) Fingerprint scan: It is largely watched as an precise biometric recognition method. Nowadays, fingerprint scanners are available at low cost and progressively integrated in electronic devices [1]. Among all the biometric techniques, this is the oldest method which has been successfully used in numerous applications. For example, fingerprint scan use in forensic for criminal identification, use in attendance system. Because the patterns of ridges on the fleshy part of fingertips are unique. No two individuals even twins have same fingerprints. The patterns of ridges leave impression on whatever they touch. Injuries such as minor burns or cuts do not mop out or change the pattern , the new skin grows showing the same pattern.

2) Retina or iris scan: The idea of distinguishing an individual by using iris patterns was suggested by an ophthalmologist in 1936. Later, the idea appeared in some action movies, including 1983's James Bond "Never Say Never Again", nonetheless at that time it remained science fiction. In 1994, the first automated iris pattern recognition algorithm was proposed by physicist and computer-vision expert John Daugman and patented, and continue to be the basis of all current iris recognition systems and products. These have been used to confirm a person's identity by reading the arrangement of blood vessels in the retina or patterns of color in the iris. It is very reliable technique and difficult to map by forgers.

3) Facial recognition: This technique use unique facial attributes to identify an individual. Biometric facial recognition systems generally read the overall structure, shape and proportions of the face taking into account the distance between the eyes, nose, mouth, and jaw edges, upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, etc.

4) Finger vein recognition: The technology of finger vein recognition is quite younger then fingerprint or facial recognition system. Finger vein recognition system uses pattern-recognition techniques based on images of human finger vein patterns under the skin's surface. Key advantage of vein patterns for biometric identification is that the forgers cannot easily create a copy of finger vein due to lack of known method, as it is possible with fingerprints.

5) Palm vein recognition: As the blood vessels zigzag beneath our skin these give a unique pattern that can be used to identify a person. Infrared beam is used to enter in the hand and the veins in the person's palm show up as black lines .Like the finger vein, Palm vein also cannot be easily forged. Due to that they can provide highest level of security.

DNA based recognition: At this time, there exists no technique to allow for immediate and automated recognition of DNA samples. DNA analysis and profiling (genetic fingerprinting) needs a lab environment for a number of hours. Though, significant research and development efforts are ongoing to develop this technique, and also to enable governments to better use the millions of DNA profiles collected and archived in databases of DNA.

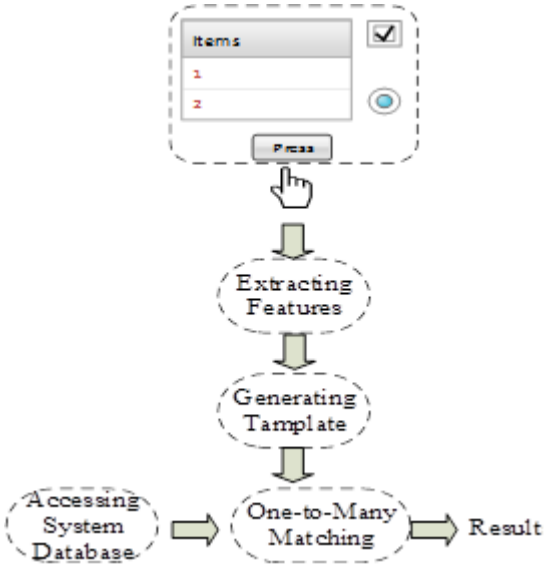

Figure 4: Identification in biometric recognition process

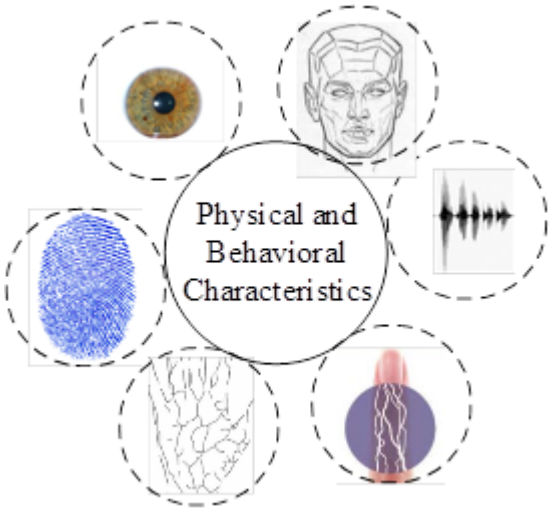

Figure 5: Physical and behavioral characteristics in biometric recognition

Behavioral biometrics includes three factors of physical attributes that can be used for user authentication;

namely, voice, signature and keystroke traits. The three factors are discussed below.

1) Voice scan: It is behavioral biometric which can be learned or acquired, but also include physiological elements. E.g., the human voice is influenced by the physiological characteristics of lungs, tongue, throat, etc. and its behavioral features evolve and change over time. They can be influenced by factors such as age, illnesses, mood, conversational partner or surrounding noise. It uses a voice print that analyses how a person says a particular word or sequence of words unique to that individual.

2) Signature scan: Signature scan is a process of, investigating an individual's signature. The technology investigates speed, direction, and pressure of writing, total time of the signature. Unluckily, signature is one of the least reliable methods of Identification. Forgers have number of ways to reproduce a signature that looks similar to the owner. Signature dynamics is biometric signature recognition systems measure and analyze the physical activity of signing. Important features include stroke order, the pressure applied, the pen-up movements, the angle the pen is held, the time taken to sign, the velocity and acceleration of the signature. Some systems moreover compare the visual image of signatures; however the focus in signature biometrics lies on writer-specific information rather than visual handwritten content.

3) Keystroke scan: It is the recognition of keystroke dynamics is the process of investigating the way an individual types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to recognize the individual based on habitual typing rhythm patterns. Keystroke dynamics are described by speed (the time a key is pressed, the time between keys pressed), rhythm, precision, keys used (e.g., left Shift key or right Shift key, Caps Lock), and other typing features.

The major issue of biometric recognition is that the information used in biometric recognition changes with age and occupation of persons. Also, It may change or damage due to suffering from physical injuries or diseases. Like, password or card biometric data cannot be changed after any misshaping. Advantage of biometric data is that, they cannot get stolen, lost, replicated or forgotten like password or token, cards. They also can not be forgotten, compromised, shared, observed or guessed like password, secret codes or PIN. You don't need to change biometric data from time to time as you do with passwords. No need to write them as most people write password. Due to high security level and accuracy of biometric authentication, government agencies are also attracted towards the biometric authentication method, for example Indian government used this technology to recognize country's people and name of this program is adhaar. In modern world, improved performance and availability of equipment at low cost and automated biometric recognition. Therefore biometric applications are categorized into three key sets which are as follows

1) Forensic applications: These are used in criminal investigations and archeology. For example, corpse identification, parenthood determination, identifying historical fact from fossils, etc.

2) Government applications: This category includes personal documents, for example voter id, passports, ID cards, etc.

3) Commercial applications: This category includes physical access control; network logins; e-Commerce, i-Commerce, m-Commerce, ATMs; credit cards; device access to computers, mobile phones; e-Health etc.

A number of provisions and techniques [36] have been suggested to safeguard security and privacy in biometrics. These are Multimodal biometric, Template-on-token, Match-on-token and Data-hiding methods attack. Data-hiding techniques embed additional information in fingerprint images - an approach similar to hiding digital watermarks in image or audio data to ensure data integrity. If the embedding algorithm remains secret, a service provider can investigate the received fingerprint image for the expected standard watermark to ensure it has been sent from a trusted sensor.

Biometric Systems Development: It is a combination hardware/software system for biometric identification or verification. Key functions of a biometric system are

1) Receive biometric samples from an individual.

2) Extract biometric feature from the sample.

3) Compare the sample of the candidate with stored templates from individuals.

4) Indicate identification or verification upon the result of the previous comparison.

Biometric systems have components which are an automated mechanism and interface with application systems. These pieces may be configured to suit different situations. A common issue is where the stored images reside; on a card presented by the person being verified or at host computer. Recognition occurs when an individual's is matched with one of a group of stored images. Biometric accuracy is the system's ability of separating legitimate matches from imposters. Although biometrics technology provides a strong factors. In [27] security priorities scheduling in Network is discussed with focus on security optimization. The scheduling which considered security, all task want execute in secure mode. The most important Network users' requirements can be representing in form many arrangements therefore it falls under category of NP Class Problem [7, 8, 18, 20, 25, 28, 29, 30, 31, 34, 35]. Then GA and variants applied for single objective optimization. Then NSGA II and variants applied [24] for multi-objective optimization.

8 Conclusions

Because of the changing security maps, clearly some organizations are required to arrange security solutions that preserve adequate counter-measures for every threat and provide the capability to meet industry regulations- Security is very big social issue as a practical and technical one. According to the new economy, information is important both as input and output. Hence information security measurement must be high priority. Security needs must constantly keep pace with ever changing technologies and application. The e-security challenges are many both from the viewpoint of their categories as well as from the view of their way of information implementation in the network.

E-security cannot be achieved through technology alone. There is almost boundless number of ways by which e-network or e-world set up could be assaulted by hackers, crackers and disgruntled insiders. Common threats include active and passive attacks, hacking, malware, Denial of Service (DoS), and vulnerabilities. We control the e-security issue by the three basic attributes known as C.I.A. (Confidentiality, Integrity, and Availability). India has taken a number of strategic initiatives to strengthen information security. This has included the enactment of the Information Technology Act 2000. ISO/IEC 27001 provides a sound basis for the development of a security policy. Biometric recognition is studied and being implemented as a key approach for e-security solution.

Acknowledgments

The research is supported by Ministry of Education Malaysia (MOE) and conducted in collaboration with Research Management Center (RMC) at University Teknologi Malaysia (UTM) under VOT NUMBER: Q.J130000.2628.11J31. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] M. H. Aghdam, P. Kabiri, "Feature selection for intrusion detection system using ant colony optimization," *International Journal of Network Security*, vol. 18, no. 3, pp. 420–432, 2016.

[2] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[3] T. Y. Chang, M. S. Hwang, W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol," *Information Sciences*, vol. 181, pp. 217–226, 2011.

[4] G. G. Deverajan, R. Saravanan, "A novel trust based system to detect the intrusive behavior in MANET," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 31–43, 2015.

[5] W. R. Ghanem, M. Shokir, and M. Dessoky, "Defense against selfish PUEA in cognitive radio networks based on hash message authentication code," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 12–21, 2016.

[6] K. Gupta, K. Gupta, O. Kaiwartya, "Dynamic ad hoc transport protocol (D-ATP) for mobile Ad hoc networks," *IEEE 5th International Conference on Generation Information Technology Summit (Confluence)*, pp. 411–415, 2014.

[7] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," *International Journal of Network Security*, vol. 13, no. 1, pp. 58–60, 2011.

[8] B. Kadri, M. Feham, and A. Mhammed, "Efficient and secured ant routing algorithm for wireless sensor networks," *International Journal of Net-work Security*, vol. 16, no. 2, pp. 149–156, 2014.

[9] B. Kadri, M. Feham, and A. Mhammed, "Efficient and secured ant routing algorithm for wireless sensor networks," *International Journal of Network Security*, vol. 16, no. 2, pp. 149–156, 2014.

[10] O. Kaiwartya, S. Kumar, "Geocast routing: Recent advances and future challenges in vehicular adhoc networks," in *IEEE International Conference on Signal Processing and Integrated Networks (SPIN'14)*, pp. 291–296, 2014.

[11] O. Kaiwartya, S. Kumar, "Cache agent based geocasting (CAG) in VANETs," *International Journal of Information and Communication Technology*, vol. 7, no. 6, pp. 562–584, 2015.

[12] O. Kaiwartya, S. Kumar, "Enhanced caching for geocast routing in vehicular Ad hoc network," in *Intelligent Computing, Networking, and Informatics*, pp. 213–220, Springer, 2014.

[13] O. Kaiwartya, S. Kumar, "Geocasting in vehicular adhoc networks using particle swarm optimization," in *ACM Proceedings of the International Conference on Information Systems and Design of Communication*, pp. 62–66, 2014.

[14] O. Kaiwartya, S. Kumar, "Guaranteed geocast routing protocol for vehicular adhoc networks in highway traffic environment," *Wireless Personal Communications*, vol. 83, no. 4, pp. 2657-2682, 2015.

[15] O. Kaiwartya, S. Kumar, R. Kasana, "Traffic light based time stable geocast (T-TSG) routing for urban VANETs," in *IEEE Sixth International Conference on Contemporary Computing (IC3)*, pp. 113–117, 2013.

[16] O. Kaiwartya, S. Kumar, D. K. Lobiyal, A. H. Abdullah, A. N. Hassan, "Performance improvement in geographic routing for vehicular Ad hoc networks," *Sensors*, vol. 14, no. 12, pp. 22342–22371, 2014.

[17] O. Kaiwartya, S. Kumar, D. K. Lobiyal, P. K. Tiwari, A. H. Abdullah, A. N. Hassan, "Multiobjective dynamic vehicle routing problem and time seed based

solution using particle swarm optimization," *Journal of Sensors*, vol. 2015, Article ID 189832, 14 pages, 2015.
[18] M. Kumar, "An enhanced remote user authentication scheme with smart card," *International Journal of Network Security*, vol. 10, no. 3, pp. 175–184, 2010.
[19] R. Kumar, S. Kumar, D. Shukla, R. S. Raw, O. Kaiwartya, "Geometrical localization algorithm for three dimensional wireless sensor networks," *Wireless Personal Communications*, vol. 79, no. 1, pp. 249–264, 2014.
[20] C. C. Lee, S. T. Chiu, and C. T. Li, "Improving security of a communication-efficient three-party password authentication key exchange protocol," *International Journal of Network Security*, vol. 17, no. 1, pp. 1–6, 2015.
[21] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, Jan. 2013.
[22] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181–2188, May 2010.
[23] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards", *Journal of Network and Computer Applications*, vol. 33, pp. 1–5, 2010.
[24] W. T. Li, T. H. Feng, and M. S. Hwang. "Distributed detecting node replication attacks in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.
[25] C. Lin, Y. Li, K. Lv, and C. C. Chang, "Ciphertext-auditable identity-based encryption," *International Journal of Network Security*, vol. 17, no. 1, pp. 23–28, 2015.
[26] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.
[27] S. Prakash and D. P. Vidyarthi, "Observations on effect of IPC in GA based scheduling on computational grid," *International Journal of Grid and High Performance Computing*, vol. 4 no. 1, pp. 66–79, 2012.
[28] S. Prakash and D. P. Vidyarthi, "Load balancing in computational grid using genetic algorithm," *International Journal of Advances in Computing, Scientific and Academic Publishing*, vol. 1 no. 1, pp. 8–17, 2011.
[29] S. Prakash and D. P. Vidyarthi, "Immune genetic algorithm for scheduling in computational grid," *Journal of Bio-Inspired Computing*, vol. 6, no. 6, pp. 397–408, 2014.
[30] S. Prakash and D. P. Vidyarthi, "A novel scheduling model for computational grid using quantum genetic algorithm," *Journal of Supercomputing*, vol. 65, no. 2, pp. 742–770, 2013.
[31] S. Prakash and D. P. Vidyarthi, "Maximizing availability for task scheduling in computational grid using GA," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 1, pp. 197–210, 2015.
[32] M. Prasad, K. P. Chou, A. Saxena, O. P. Kawrtiya, D. L. Li, C. T. Lin, "Collaborative fuzzy rule learning for Mamdani type fuzzy inference system with mapping of cluster centers," in *IEEE Symposium on Computational Intelligence in Control and Automation (CICA'14)*, pp. 1–6, 2014.
[33] R. S. Rao, S. K. Soni, N. Singh, O. Kaiwartya, "A probabilistic analysis of path duration using routing protocol in VANETs," *International Journal of Vehicular Technology*, vol. 2014, Article ID 495036, 10 pages, 2014.
[34] C. Y. Sun and C. C. Chang, "Cryptanalysis of a secure and efficient authentication scheme for access control in mobile pay-TV systems," *International Journal of Network Security*, vol. 18, no. 3, pp. 594–596, 2016.
[35] J. Wei, W. Liu, X. Hu, "Secure andefficient smart card based remote user password authentication scheme," *International Journal of Network Security*, vol. 18, no. 4, pp. 782–792, 2016.
[36] H. Zhu, Y. Zhang and X. Wang, "A novel one-time identity-password authenticated scheme based on biometrics for e-coupon system," *International Journal of Network Security*, vol. 18, no. 3, pp. 401–409, 2016.

Omprakash Kaiwartya received his Ph.D. and M.Tech degrees in Computer Science from School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India in 2015 and 2012 respectively. He is currently associated with Faculty of Computing, Universiti Teknologi Malaysia (UTM), Skudai Johor, Malaysia as Post-Doctoral Fellow. His research interests include Vehicular Ad-hoc Networks, Mobile Ad-hoc Networks and Wireless Sensor Networks. Dr. Omprakash has published papers in International Journals and Conferences with publishers including ACM, IEEE, Elsevier, Springer, MDPI, KIIS, InderScience and Hindawi.

Mukesh Prasad (M'13) received his Ph.D. degree in computer science from National Chiao Tung University, Hsinchu, Taiwan in 2015 and master degree in computer application from Jawaharlal Nehru University, New Delhi, India, in 2009. He is currently associated with National Chiao Tung University, Hsinchu, Taiwan as Post-Doctoral Researcher. His current research interests include machine learning, pattern recognition, fuzzy systems, neural networks and Wireless Sensor Networks. Dr. Mukesh has published papers in international journal papers and conferences including IEEE Transactions, ACM and Springer.

Abdul Hanan Abdullah received his Ph.D. degree from Aston University in Birmingham, United Kingdom in 1995. He is currently working as a Professor at Universiti Teknologi Malaysia (UTM). He was the dean

at the Faculty of Computing, UTM from 2004 to 2011. Currently he is heading Pervasive Computing Research Group, a research group under K-Economy Research Alliances. His research interests include wireless sensor networks, Internet of Things, network security and next generation networks. Prof. Abdullah has published papers in International Journals and Conferences including IEEE, Elsevier, Wiley & Sons, Springer, MDPI and Hindawi.

Shiv Prakash received his Ph.D. and M.Tech degrees in Computer Science from School of Computer and System Sciences, Jawaharlal Nehru University, New Delhi, India in 2014 and 2010. His research interest includes parallel/distributed system, grid computing, Cloud computing, machine learning. He has published papers in various international journals and peer-reviewed Conferences including IEEE, ACM, Elsevier, Springer, Wiley & Sons and Inderscience.

Durgesh Samadhiya is a scientist at the Emerging Device Division department of National Applied Research Laboratories, Hsinchu Taiwan, working on the IoT tag for all the products around the world that can give you the information about the product and location of the product. Previously he was a Research Fellow at Chung Hua University, Taiwan. He holds a PhD degree in Method Engineering of Software Engineering from Taiwan, Master Degree in computer Science from College of Engineering Roorkee, India. He has published good number of research papers in International Journal and Conference proceeding indexed in Science Citation Index, Ei compendex, Google Scholar, database and logic programming (DBLP), Web of Science.

Syed Othmawi Abd Rahman is currently working working at Faculty of Computing, Universiti Teknologi Malaysia (UTM). He has received post graduate diploma from University of Warwick, UK in 1990 and master degree from UTM in 1996.