Improving Work Ethics and Moral Standards through the Integration of Information Communication Technology (ICT)

Adigwe A. I.
Computer Science Department
Federal Polytechnic, Oko,
Anambra State, Nigeria.
anthonyadigwe@gmail.com
08101647799, 08025078687

Nwokedi C. C.
Computer Science Department
Federal Polytechnic, Oko,
Anambra State, Nigeria.
dioxyonyi2012@yahoo.com
08067576186

Abstract

Improving work ethics and moral standards through the Integration of Information and Communication Technology (ICT) has become a global practice. There has been a paradigm shift from resource to knowledge based and ICT driven economy. Economic prosperity and productivity of an organization are linked with strong work ethics and moral standards, especially through deployment of relevant ICT devices such as Biometric recognition system which deals with ethical issues like lateness and absenteeism at work place. Monitoring employees' behavour will obviously impact work ethics and moral standards positively. Ways in which the behavour of employees can be monitored to ensure that they carry out their responsibilities effectively on their assigned duties no doubt has been a problem in recent times and any management that fails to oversee its workforce to ensure that employees are not spending valuable company time for which they are compensated is failing in its mandate. ICT has become an essential and valuable tool highly used to enhance and monitor the commitments of employees thereby improving work ethics. With wide-spread deployment of ICT in organizations, security and privacy issues have become a major concern among the employers. To address the perceived security threats and vulnerability issues, the researchers focused on theoretical analysis of biometric recognition system (an ICT device), concentrating on how it improves work ethics when properly deployed and implemented. The research equally discussed how the biometric system works, the best biometric method, security threats and vulnerabilities in using this system and equally provides measures to mitigate them. Lastly, the study recommends the need to sensitize employees on the perceived security threats and also encourage various organizations to begin massive deployment of Biometric recognition systems as this will help improve work ethics and enhance productivity.

Keywords: *Work Ethics, ICT, Moral Standards, Biometric Recognition System, Security threats and Vulnerabilities, Biometric Templates.*

Introduction

Technology in workplace has gone from been an innovative luxury to a necessity without boundaries. The deployment and use of Information and Communication Technologies (ICTs) has effectively and efficiently improved work ethics and made the workers more responsive.

Integrating ICT in organizations can influence the moral standard of the employee positively as well as improve their work ethics thereby exposing them to greater opportunities and increase the performance of the organization. It is difficult but important to quantify the degree to which ICT helps in improving the code of conduct of employees during work hours and enable them focus on work tasks. Studies reveal that Institutions that have integrated ICT facilities show higher improvement in their work ethics and moral standards compared to those yet to deploy it. Concurring with the aforementioned, Bargh and McKenna (2004) as cited by Perron et al, (2011) state that the growth of the Internet and use of ICTs has changed how we interact with each other and our positive attitude towards work.

Currently, technology is advancing rapidly, although ICTs are not without problems, the reality remains that they will continue to shape the global community. Assuming employers have a device that solves the issue of attendance taking (to capture and record when the employee shows up and leaves a work place), and also monitor them during work hours, there will be a great improvement in their work ethics and moral standards thereby resulting to greater output. This is in line with Heathfield (2018), who believes that an employee's work ethic is based on their output. Hence, integrating ICT in workplace can be a factor that can be used to inculcate work ethics and moral standards in employees.

In spite of successes recorded through integration of ICT by a number of multinational companies, corporate bodies, and Public Institutions in solving work ethics related issues, there has been an alarming concern regarding security and privacy of employees in such work environment. Deployment of Biometric based attendance management system, Closed Circuit Television (CCTV), security cameras and as well as Mobile phones at work have generated lots of criticisms bothering on privacy, integrity and confidentiality. While we are not disputing the above findings, we believe that deployment of ICT in work place can improve the ethical and moral standard of employees when properly implemented and backed with strong policy. In support of our view, Adigwe and Egere (2014) believe that, though the technology is relatively a new concept, but there is considerable ignorance about their use and implications which are yet to be erased from the minds of employees.

Given the above therefore, this paper explores the conceptual meaning of work ethics in relation to moral standards and as well as ICT. And for clarifications of the perceived ignorance on issues of integrity and confidentiality raised, we equally discussed the role of ICT such as Biometric attendance management system as an emerging technology which can improve work ethics and moral standard of workers without undermining employees' integrity and confidential data when properly deployed and implemented. Conscious effort was also made in discussing the working principles of Biometric recognition systems and counter measures used in addressing the known security threats or vulnerabilities. Deployment of ICT, no doubt, helps an organization maintain efficient and effective work force and also improves security and safety at work.

Conceptual Clarification of Work Ethics and Moral Standards

The term work, work ethics and moral standards have been independently defined by a number of researchers. Work, according to research by Hudson (1973), could be defined as a means of productivity, a means of drudgery, or a necessary evil depending on individual's perception. Hill (1999) believes that work has been with humanity since the fall of Adam and Eve in the biblical context. And with the biblical record of work as a punishment for sin (Bernstein, 1988), emerged the issue of work ethics which defines what is acceptable or unacceptable behavour at work place. Hill (1991) calls this behavour the ethics of work. In alignment with these definitions and believes of work, we begin to look at the conceptual clarifications of work ethics and moral standards

What is work Ethics?

Work ethics originated from Lutheran and Calvinist theology (Buchholz, 1978). Work ethic of the early colonists has different meanings and interpretations when compared to modern day work ethics, which has undergone a lot of transformation through integration of ICT. Work ethics of modern day society has varying definitions as viewed by writers of relevant contemporary literature (Buchholz, 1978; Ford & Herren 1995; Miller & Coady, 1984). Miller and Coady (1984) View work ethics as reliability and trustworthiness, willingness to learn, responsibility for one's actions and inactions, willingness to work, and willingness to work cooperatively. Gilbert (1973), in his definition of work ethics, sees it as the willingness that culminates in application to the job and its evidence through satisfaction with material rewards of work. While Miller and Coady (1989) definition revolve around beliefs, values and principles, Schab (1976) simply defines work ethics as the willingness to stay employed. Ford and Herren (1995) agree with the opinions and positions of Miller, Coady and Schab, pointing out that the highlighted characteristics by the trio provides guideline to the way individuals interpret and act upon their rights and responsibilities within work environment at any given time. Martin and Morris (2015) view work ethics as increased efficiency. While aforementioned researchers seem to be driving at production, performance, maintenance or enhancement, others such as Kelvin and Jarrett, as cited in Wentworth and Chell (1997), purport that there is really no such thing as work ethics. They are of the opinion that work ethics should be regarded as wealth ethics where wealth is conceived as the fundamentals for economic independence. The aforementioned researchers believe that wealth accumulation is and has been for centuries the key factor influencing one's work ethics.

Work ethics, from our point of view, is a written framework or code of conduct which specifically provides guidelines to monitor and regulate the behavour of employees at a work place. The use of ethics, with supportive guidance and mechanisms of reward and sanctions, has been proliferated since the 1980s (Downe et al., 2016), yet this has not positively influenced the ethical conduct of an establishment as anticipated. Work ethics have always been subjected to all forms of abuses and manipulations in spite of the existing rules and regulations.

Moral Standards

Moral standard and work ethics are relatively interwoven and are often used interchangeably. Moral standard is regarded as personal principles created and upheld by the individuals themselves and which can be influenced by culture or society positively. How to make employees exhibit good moral standard has been a problem in many organizations and the way to influence the employee's moral behavour positively has been a course to study in recent times.

Information and Communication Technology (ICT)

At this point, it is important that we clarify one of the key concepts of our discussion, the ICT. Many experts' definitions have been offered by a number of ICT researchers. ICT is an acronym for Information and Communication Technologies. It involves integration of voice and data Networks which previously existed separately as Information Technology (IT) and Communication Technology (CT). Originally, ICT as a compound concept defines any communication device or application that has to do with information storage and dissemination. Such devices include radio, television, cellular phones, computer and network infrastructures. Today, it has assumed new meanings, where devices previously used for communication (Voice network) can as well be used for call reception, short message service (sms), multimedia messaging service (mms) and video streaming. Ugwoke (2011), cited in Onwumere and Adigwe (2017), conceptualizes ICT as a set of technological tools and resources used to communicate, disseminate, store and manage information. It is equally a concept that includes hardware, software, processes and people that are involved with technologically oriented communication. Ekoja (2007) refers to ICT as the equipment used for capturing, processing, storing, transmitting and accessing information which has offered employees and employers from all walks of life tremendous opportunities in information handling and utilization. Information and Communication Technologies are basically driven from two core technologies – information and communication. While the term Information technology means the computer software and hardware that essentially store, retrieve and manipulate information, the communication technology, on the other hand, defines the capacity to draw out voice data or information in the network for utilitarian purposes. ICT, thus, has become an inevitable avenue for assessing globally existing and innovative technologies, be it information or communication, which does not only support but also improves work ethics.

Improving Poor Work Ethic and Moral Standard Using ICT

Deployment of ICT in work environment is done in three broad aspects: here are some of the ways in which work ethics and moral standard of workers can be improved.

1. Use of Biometrics Recognition systems
2. Use of Closed-Circuit Television (CCTV) and digital Cameras
3. Use of Mobile phones

Use of Biometrics in the Workplace

Biometric is an automated measurement of biological or behavioural traits that identifies an individual. Over the last decade, it has proven to be a reliable solution in identifying and authenticating users. Biometrics generally relates to the application of measurable physical characteristics of the human body (Wilkins, 2012).Biometric recognition is an automated measurement of biological and behavioural traits that discloses the identity of an individual (Adigwe & Egere, 2014).The most common methods of Biometric technology include finger print, hand geometry, Voice, Iris, face, hand written signature, Palm print and Gait to mention a few.

Currently, a discussion is ongoing in the academic community on the use of “body odour” as one of human characteristics to uniquely identify an individual. Biometric characteristics being used as an authentication token have a number of features such as reliability, convenience, and so on. The foregoing traits have led to large-scale deployment of biometric authentication systems by multinational companies and public institutions for the purposes of security and recognition of staff at work places.

However, it is pertinent to note that, in spite of the remarkable successes achieved by its deployment, there are still some contentious securities and privacy issues or implications concerning the deployment of biometric-based authentication and identification systems. Expect the issues are meticulously rectified, some members of the public would not accept the deployment of this supposedly emerging technology at work place. Notwithstanding the views of some employees regarding the technology, there has been an increase in number of various types of biometric devices available in the market today and these include:

- Fingerprint, thumbprint and handprint scanners
- Voice recognition recorders
- Software that recognizes keyboard keystroke dynamics, particularly in entering login details and passwords
- Retinal scanners
- Facial recognition systems.

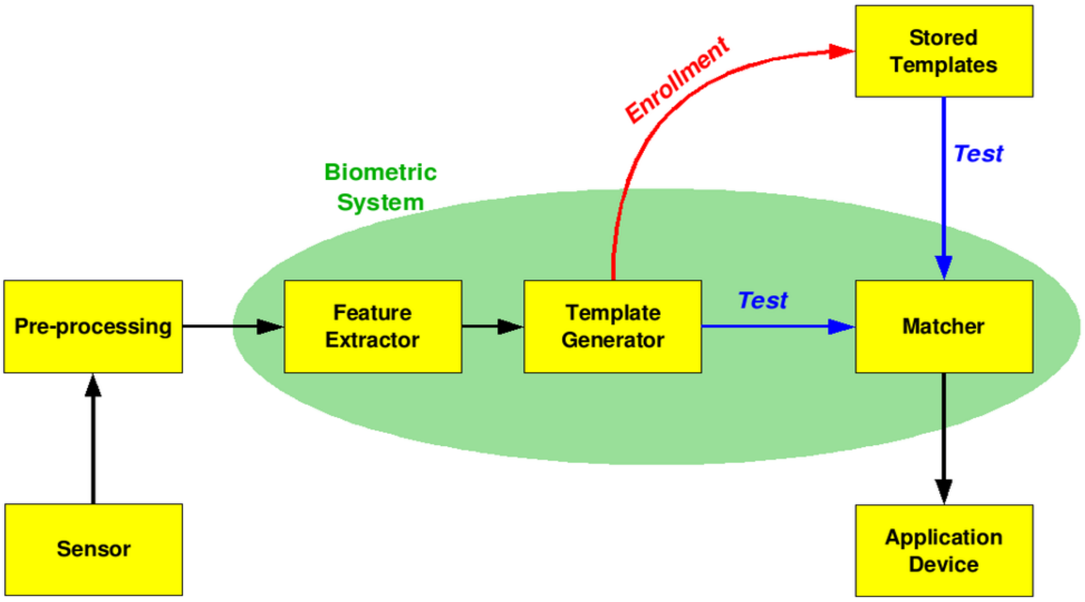
Studies have shown that the use of biometric technology for authentication is always more reliable and faster and thereby regarded as the best and safest way of curtailing employees unethical attitude towards lateness to work and absenteeism. It replaces the conventional attendance taking registers which are mostly used in Government owned establishments. The traditional attendance is full of manipulations because a staff can actually sign in for another staff who has been absent from work and such behaviour is regarded as unethical conduct. Biometrics authentication (or realistic authentication) is field of ICT which has been proven effective for identification and access control mechanisms. We are of the view that biometrics authentication, when properly deployed at workplace, would permanently eradicate the issue of lateness, absenteeism and curb ghost workers thereby improving work ethics and moral standard of employees.

How Does Biometric Recognition System Work?

Before we go on with discussion of how Biometric system works and the issues of privacy and confidentiality raised by critics of this system, it is pertinent we explore the major components of Biometric authentication systems and the interoperability between those components. Except we have correct information on the working principles of these components, we would be unable to establish the confidentiality and privacy implications of deploying such system to improve work ethics.

Study reveals that Biometric recognition system is essentially made up of five major components. Namely: Sensor, Feature Extractor, Template Database, Matcher, and Decision Module. The sensor is the interface between the user and the authentication system and its function is to scan the Biometric traits of the user. The feature extraction Module, on the other, processes the scanned Biometric Data to extract the salient information, the feature set, which is useful in distinguishing between different users. In some cases, the feature extractor is preceded by a quality assessment module that determines whether the scanned biometric trait is of sufficient quality for further processing.

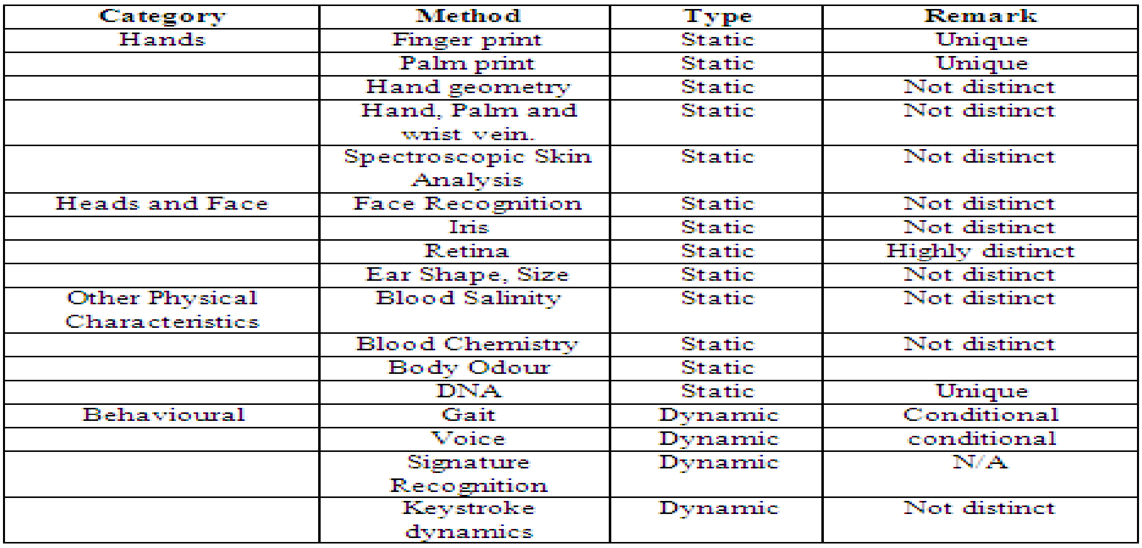
Then, during enrolment, the extracted feature set is stored in a database as a template marked by the user identity information. Since the template database, according to Paul and Patrick (1999), could be geographically distributed which is made possible by the use of Global positioning System (GPS) and contains millions of records, maintaining its data integrity and confidentiality is an important task. Another component is the Matcher Module which is usually an executable Program designed to accept two Biometric feature sets, usually from the template and query respectively as inputs and outputs (Brindha, 2012). Finally, we have the Decision Module which makes the identity decision and initiates a response to the query. From the foregoing, a number of researchers believed that the template can be intercepted and compromised, but this is no longer the case as a lot of counter measures have been put in place to protect the template from being compromised. The diagram of a biometric system is as represented below.



Source: (https://commons.wikimedia.org/w/index.php?curid=2008641)

Which is the Best Biometric Method?

Having meticulously reviewed the major components of Biometric recognition systems, it is important we discuss the popular biometric methodologies on the basis of how they function, type of characteristics of known biometric methods, and what applications they may be best suited for and which of them is the best. The table below represents the methods.



Category	Method	Type	Remark
Hands	Finger print	Static	Unique
	Palm print	Static	Unique
	Hand geometry	Static	Not distinct
	Hand, Palm and wrist vein.	Static	Not distinct
	Spectroscopic Skin Analysis	Static	Not distinct
Heads and Face	Face Recognition	Static	Not distinct
	Iris	Static	Not distinct
	Retina	Static	Highly distinct
	Ear Shape, Size	Static	Not distinct
Other Physical Characteristics	Blood Salinity	Static	Not distinct
	Blood Chemistry	Static	Not distinct
	Body Odour	Static	
	DNA	Static	Unique
Behavioural	Gait	Dynamic	Conditional
	Voice	Dynamic	conditional
	Signature Recognition	Dynamic	N/A
	Keystroke dynamics	Dynamic	Not distinct

Source: Advanced Identity Verification (Ashbourn, 2009)

The table above reveals quite a number of Biometric methods but the most two basic ones in use today is the finger print and face recognition. However, the question, "which biometric is the best", has been one of the most frequently asked when people intend to deploy this technology as a solution to improve work ethics and enhance productivity of employees. Adigwe and Egere (2014) believe that the best answer to such technical question is that there is no biometric method considered "the best". It all boils down to what an employer or stakeholder tries to achieve, with whom, and what prevailing conditions exist. Further study by Nikolaos (2009) equally reveals that methodology which works well within a certain office environment may be less suitable for a busy public airport or a factory shop.

We agree with Adigwe and Egere (2014), Nikolaos (2009) that in considering biometric methodologies for possible deployment, there is need for clear understanding of the application and the situation from the user's perspective and being objective about the benefits of introducing the technology into a given process. For example, face recognition template may cease to be unique where an individual under goes plastic surgery in a case of accident (Adler, 2005).

How Vulnerable are Biometric Recognition System?

With rapid growth in sensing and computing technologies, biometric recognition systems are becoming affordable and are easily embedded in a variety of consumer devices such as mobile phones and key holders. This total integration with ICT devices makes the seemly emerging technology vulnerable to malicious attacks by criminals. In order to subvert any possible security threats, vulnerabilities of the biometric system must be identified and systematically mitigated. Otherwise, the deployment of such highly sensitive technology will, undoubtedly, continue to raise fear of insecurity in the minds of general public as far as privacy, integrity and confidentiality of data are concerned (Adigwe, 2018). A number of researchers have analysed potential security breaches in a biometric recognition system and proposed methods to counter those security challenges. Attack trees, for instance, have been used to study how biometric system security can be compromised. Some of the vulnerabilities associated with biometric recognition systems are *intrinsic failures and failure due to an adversary attack.*

(i) I*ntrinsic Failure*

Intrinsic failures are security lapses which occur due to an incorrect decision made by the biometric recognition system. A biometric verification system is liable to two types of errors when it comes to decision-making; namely*, false accept and false reject.*

A legitimate user may be falsely rejected by the biometric system due to large discrepancies in the user's stored template. These intra user variations may be as a result lack of interoperability between the user and biometric recognition system (changes in pose and expression in face image) or due to noise introduced at the sensor. For example, residual prints left on fingerprint sensor. False accept is usually caused by lack of uniqueness in the biometric traits which can lead to large similarity between feature set of different users. An example is similarities in the face images of twins and siblings. Both intra user variations and inter user similarities may also be caused by the use of non-salient feature and non-robust matchers. Sometimes, a sensor may fail to acquire the biometric trait of a user due to limitations in sensing technology or adverse environmental conditions. For instance, a fingerprint sensor may be unable to capture a good quality fingerprint of dry/wet fingers. This leads to failure-to-enroll (FTE) or failure-to-acquire (FTA) errors **(Catherine, 2013)**.

Intrinsic failure can also occur even when there is no explicit effort by an adversary to circumvent the system. So, this type of failure is known as zero-effort attack. It poses a serious threat if the false accept and false reject probabilities are high. However, ongoing research is directed at reducing the probability of intrinsic failure, mainly through the design of new sensors that can acquire the biometric traits of an individual in more reliable, convenient, and secure manner, or deployment of invariant representation schemes with robust and efficient matching algorithms and use of multi-biometric systems **(Nikolaos, 2009).**

(ii) Adversary attack

In this situation, an adversary purposely initiates an attack on the biometric system whose success relies on the lapses in the system design and the availability of adequate computational resources to the adversary. In this paper, adversary attack is categorized into three: administrative, non-secure network infrastructure, and biometric covertness attacks.

(a) Administrative attack

This kind of attack is often referred to as insider attack which points to all vulnerabilities introduced due to improper administration of biometric system such as integrity of the enrolment process between the adversary and the system administrator.

(b) Non-secure Network Infrastructure: In a networked environment, biometric system is composed of hardware, software, and the communication links between the various modules. An adversary can manipulate the biometric infrastructure, thus leading to security breaches through a thousand ways.

(c) Biometric covertness

Studies reveal that it is possible for an adversary to covertly acquire the biometric characteristics of a legitimate user (e.g. fingerprint impression lifted from a surface) and use them to create physical gummy finger of the biometric trait. Hence, if a biometric system is not capable of distinguishing between live biometric presentation and an artificial spoof, an adversary can circumvent the system by presenting spoofed trait. This, undoubtedly, undermines the integrity and confidentiality of the users of such systems, hence violates their privacy. A compromised biometric system can therefore lead to serious privacy implications; namely, Intrusion and Denial-of-Service attacks (DOS).

Intrusion refers to an impostor gaining illegitimate access to the system which often results to loss of privacy (e.g., unauthorized access to personal information) and various security threats such as interception, modification, and fabrication of employees' data on transit via the network infrastructures or those currently stored in an Organization's database. All the four factors, as mentioned previously, that cause biometric system vulnerabilities (intrinsic failure, administrative abuse, insecure network infrastructure, and biometric covertness) can result in intrusion.

Denial-of- Service Attack

Denial-of-service attack *(DOS)* is a situation where a legitimate user is prevented from obtaining the service that he is entitled to. A system hacker can undermine the infrastructure (e.g., physically damage a fingerprint sensor), hence preventing users of Biometric-enable attendance monitoring system from clocking in and out on arrival and at close of work respectively. Intrinsic failures such as false reject (FR), failure-to-enroll (FTE), and failure-to-acquire (FTA) also lead to denial-of-service attack. In addition, Administrative abuse such as modification of biometric templates or the operating parameters of biometric systems may also be a contributing factor to the denial-of-service attack. Thus, an assumption that the security services can rely on the kernel to supply correct data and lack of trust on the part of other agents undermines confidentiality mechanism **(Matt, 2002).**The good news, however, is that there are solutions to all of the known vulnerabilities and some of them are as highlighted below.

How Effective and Efficient is Biometric Recognition System?

It is paramount to note that in spite of the overwhelming benefits offered by biometric recognition systems, employers have developed cool feet in embracing this technology. Part of this reluctance may be attributed to a high cost of biometric readers in comparison to conventional clock in and out machine or work place register, coupled with the perceived extra complexity of implementation and subsequent running cost. However, we believe that the main reason is unconnected to reluctances on the part of employees who have sometimes perceived the concept as being intrusive or simply unreliable and harmful to their privacy, integrity and confidentiality of data. Early biometric vendors did not always help this situation as some of them made unrealistic claims as to the performance of their devices, which could often not be substantiated under real world Conditions (e.g., distinguishing an artificial biometric template from a real one). It is probably fair to say that vendors and system integrators have largely learned their lessons and that similar installation today is expected to be much more reliable and successful through a combination of intelligent deployment. However, it has taken a while to get to this point and poor early impressions are really hard to erase from the public consciousness **(Nikolaos, 2009).**

Given the above scenario, is a biometric based attendance system viable with contemporary technology? The answer is yes because almost all the known security threats and vulnerabilities, as discussed previously in this paper, can be countered. Solutions to known threats on biometric recognition systems are as discussed below.

Attacks at the user interface

This kind of attack is mostly due to the presentation of a spoof or artificial biometric trait(s). If the sensor is unable to substantiate between fabricated and genuine biometric traits, like finger print patterns which are expected to be unique for all humans including identical twins, the adversary easily intrudes the system under a false identity. This kind of threat can now be countered following a number of efforts made in academic community which has led to development of hardware as well as software solutions that are capable of performing aliveness detection of genuine biometric traits to address such security threat **(Ashbourn, 2000).**The software is capable of detecting flow of blood to distinguish real finger print pattern from artificial one.

Attacks at the Interface between Modules

A researched study shows that an adversary can either sabotage or intrude on the communication interface between different modules. For instance, he can place an interrupting source near the communication channel (e.g., a jammer to interrupt a wireless interface). If the channel is not cryptographically secured, an adversary may also intercept and/or modify the data being transferred. Therefore, the knowledge of cryptography is being used as countermeasure for attacks on interface between modules. For example, **Juels, A. et al (2005)** *outline the security and privacy issues* introduced by insecure communication channels in e-passport application that uses biometric authentication. Insecure communication channels also allow an adversary to launch replay **(Syverson, 1994)**, or hill-climbing attacks **(Adler, 2005).** A common way to secure a channel is by *cryptographically encoding* all the data sent through the interface through the use of private and public keys infrastructure. Even then, an adversary can launch a replay attack by first intercepting the encrypted data passing through the interface when a legitimate user is interacting with the system and then sending this captured data to a desired module whenever he wants to break into the system. A countermeasure for this attack is the use of time-stamps **(Catherine, 2013).**It really takes a lot of time to decipher a captured data. But with time stamp technology, the content of captured data becomes useless by the time the attacker decrypts it because the time must have expired.

Attacks on the Software Modules

The executable program at a module can be modified such that it always outputs the values desired by the adversary. Such attacks are known as *Trojan-horse attacks*. A secured code practice is being used as a countermeasure for such attack **(Seacord, 2005).**

Attacks on Template Database

Studies further prove that one of the most potentially damaging attacks on a biometric system is against the biometric templates stored in the system's database. Attacks on the template can lead to the following three vulnerabilities:

(i) A template can be replaced by an impostor's template to gain unauthorized access to the system.
(ii) Physical spoof can be created from the template to gain unauthorized access to the system (as well as other systems which use the same biometric trait).
(iii) A stolen template can be replayed to the matcher to gain unauthorized access. A potential abuse of biometric identifiers is cross-matching or function creep where the biometric identifier for the purposes other the intended purpose. For instance, a fingerprint template stolen from a bank's database may be used to search a criminal fingerprint database or cross-link to person's health records.

To protect ***Attacks on Template Database***, the most effective way to secure the biometric recognition system and the template is to put all the system modules and the interface between them on a smart card (or more generally a secure processor). This kind of system is known as match-on-card technology. And according to Juels, Molnar and Wagner (2005), the sensor, feature extractor, matcher, and template reside on the card. The good news about this emerging technology is that the biometric information never leaves the card. However, systems on card implementations are not appropriate for most large-scale applications because they are expensive and users must carry the card with them at all time. In addition, the possibility that the template can be gleaned from a stolen card is not ruled out. Therefore, it is vital to protect the template even in match-on-card applications. Passwords and PIN have the property that, if they are compromised, the system administrator can reissue another one to the user. It is desirable to have the same property of revocability with biometric templates. Other properties needed in order to ensure an ideal deployment of Biometric attendance taking system include; diversity, Security and performance.

(i) **Diversity**: the secured template must not allow cross-matching across databases, thereby ensuring the user's privacy.

(ii) **Security**: it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

(iii) **Performance:** the biometric template protection scheme should not degrade the recognition performance of the biometric system **(Brindha, 2012).**

Conclusion

With an increasing violation of work ethics by employees across board, it has become vital to integrate ICT at work place environment by both private and public sectors. Good work ethics have been known to drive productivity and enhance job satisfactions when properly adhered to. Unethical conducts such as lateness to work, absenteeism, proxy signing and unjustly manipulation of sign in and sign out of attendance registers can be taken care of with proper deployment and implementation of Biometric recognition system. Biometric recognition or attendance monitoring systems are being widely deployed to achieve reliable and genuine user authentication, which is a critical component in identity management.

However, the indisputable fact remains that biometric systems themselves are vulnerable to attacks. The analysis of this research paper can easily be understood in the sense that the existing biometric template protection schemes are not yet sufficiently matured for large-scale deployment, simply because they do not meet the requirement of diversity, revocability, security, and high-recognition performance. These four properties should be given a serious consideration when deploying an effective biometric-recognition system. Also noted is a growing fear of privacy, integrity and confidentiality issues. It is true that such security vulnerabilities and threats exist but ICT solutions have emerged to counter all known security issues. In addition, large-scale deployment of such technology is costly but real savings can be realized through the appropriate use of a biometric recognition system to track hours worked in relation to salary and wages. With deployment of Biometric recognition system, therefore, the issues of unethical conducts such as lateness and absenteeism amongst others will be completely eradicated.

Recommendations

This technology, however, is new and there is a considerable ignorance about their use and implications, which are yet to be erased from the minds of the public. The study therefore recommends the need to sensitize employees on the fact that those perceived security threats about the emerging technology now have solutions and therefore encourage both private and public sectors to begin massive deployment of Biometric recognition systems. It is indeed the way to go in improving work ethics and enhancing productivity. Iris and fingerprint-based identifiers have proven to be an effective solution, but demands good administration and management because it remains the most valuable keys for the successful deployment of biometric based systems.

References

Adler, A. (2005). Vulnerabilities in biometric encryption Systems. Proceedings of the 5thInternational Conference on Audio and Video-Based Biometric Person Authentication. 3(9), 1100- 1109.

Ashbourn, J. (2002). Prospective Analysis on Trends in Cybercrime from 2011 to 2020. Retrieved 28 August 2018 from http//www.mcafee.com/us/local content/white papers/wp id theft en.pdf

Ashbourn, J. (2009). Advanced Identity Verification: The Complete Guide. Computers & Security, International Journal of Computer Science, 21(3), 220-228.

Adigwe, A.I. (2018). The Role of Traffic analysis tools in Education and Cybercrime Fight. Journal of Education & Emerging Issues, 1(1), 34-42

Adigwe, A.I. & Egere, A.N. (2014). Security and Privacy Implications in the Deployment of Biometric Based ID Card for University Students and Staff. International Journal of Innovative Research & Development (ijird), 3(9), 181-186

Bernstein, P. (1988). The work ethic: Economics, not religion. International Journal of Business Horizons, 3(12), 34- 45

Brindha, V.E. (2012). Biometric Template Security using Dorsal Hand Vein. Retrieved 30 August 2018 fromhttp://omicsonline.org/biometric-template-security-using-dorsal-hand-vein-fuzzy-vault-2155

Buchholz, R. A. (1978). The work ethic reconsidered: Industrial and Labour Relations Review. Journal of Industrial Teacher Education, 8 (4), 42 - 55.

Catherine, P. (2013). Fundamental concepts in network security. Retrieved 30 May 2014 from http://www.ciscopress.com/articles/article.asp%3Fp%3D1998559

Downe, J., Cowell, R. & Morgan, K. (2016). What Determines Ethical Behavior in Public Organizations: Is It Rules and/or Leadership? Public Administration Review. 76.10.1111/puar.12562.

Ekoja, L. & Montague, R (2002). Library and Information Science Education. Encyclopaedia of Library and Information Science, 3(5), 1645 -1656

Ford, F. A. & Herren, R. V. (1995). The teaching of work ethics: Current practices of work program coordinators in Georgia. Journal of Vocational Education Research, 1 (2), 1 – 20

Gilbert, L. D. (1973). The changing work ethic and rehabilitation. Journal of Rehabilitation, 3(9), 15 – 34

Heathfield, S. M. (2018). Best Ways You Can Demonstrate a Strong Work Ethic: Get ahead by working hard. Retrieved Sept. 20 2018 from https://www.thebalancecareers.com/best-ways-you-can-show- strong-work-ethic-41577

Hill, R. B. (1991). Instill the work ethic in students. Journal of Business Education Forum, 33 (7), 22 - 38

Hill, R. B. (1999). Historical context of the work ethic (Unpublished paper). University of Georgia

Hudson, R. H. (1973). Teacher, your work ethic is showing. American Vocational Journal, 1 (4), 22 - 35

Juels, A., Molnar, C.K. & Wagner, M.L. (2005). Security and Privacy issue in E-passports. Proceedings of the Conference on security and privacy for Emergency Areas in Communications Networks. Athens, Greece: 25(8), 74-88.

Martin, N.P. & Morris, A.O. (2015). Negative Work Ethic Definition. Houston Chronicle. Retrieved from 22 of Sept. from http://smallbusiness.chron.com/negative-work-ethic-definition-10235.html

Matt, B. (2002). Computer Security: Art and Science. New York: Addison Wesley & Sons, Inc.

Miller, C.N. & Coady, A.K. (1989). Work ethics of students who are disadvantaged enrolled in vocational education, analysis of personal perspectives. Journal for Vocational Special Needs Education, 12 (3), 13- 26

Nikolaos, V. (2009). Advanced Signal Processing and Pattern-Danish Biometrics. Retrieved 28 April 2014 from http/www.iti.cs.uni.agdeburg.de/~sschimke/5681_48.pdf

Onwumere, A.A & Adigwe, A.I. (2017). ICT and Youth Empowerment in Nigeria. Journal of Public Administration and Social Welfare Research, 1(2), 39-47

Paul, J. & Patrick, J. (1999). Introduction to biometric identification technology: Capabilities And applications to the food stamp program. Retrieved 2 July 2014 from http://www.fns.usda.gov/sites/default/files/biomeval.pdf

Perron, B.E., Taylor, H.O., Glass, J.E., & Margerum-Leys, J (2011). Information and Communication Technology in Social Work. Journal of Advances in Social Work, 5(6), 67 – 81

Seacord, R. (2005). Secure coding in C and C++. New York: Addison Wesley & sons, Inc.

Syverson, P. (1994). A taxonomy or replay. In proceedings of the Computer Security foundations Workshop Franconia, NH, USA: 3(9), 187-191.

Ugwoke, F.N (2011). Resources for Teaching Information and Communication Technology Courses. Retrieved from https//: www.unn.edu.ng.

Wilkins, P. (2012). Biometrics in the workplace – practical, legal and ethical considerations. Retrieved 28 July 2014 from https://www.securitysolutionsmedia.com