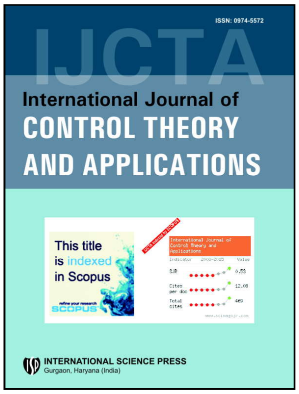

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 14 • 2017

Inhibiting Cognitive Bias in Forensic Investigation Using DNA Smart Card with IOT

S. Mahaboob Hussain[1], Prathyusha Kanakam[2] and A.S.N. Chakravarthy[3]

[1] Department of Computer Science and Engineering Vishnu Institute of Technology, Bhimavaram, AP, India,
Email: mahaboobhussain.smh@gmail.com
[2] Department of Computer Science and Engineering MVGR College of Engineering, Bhimavaram, AP, India,
Email: prathyusha.kanakam@gmail.com
[3] Department of Computer Science and Engineering JNTUK, Kakinada, AP, India, Email: asnchakravarthy@yahoo.com

Abstract: Reducing and tracing various digital crimes is the most significant and prioritized task for the investigators. Many fields of forensic science provide the solution for the crimes to become aware of and to trace. The approach of the forensics investigator team plays a key role in investigating the crime and to reduce cognitive bias. This paper in close proximity of the scenario for analyzing the crime factors by using Internet of Things (IOT) applications from various events that understand the problem with the usage of bio-smart card technology. It simplifies the investigators to analyze and to focus at a source with some practice to diminish crime factors in an efficient and effective approach and can easily eliminate cognitive bias. This paper proposes the system of smart card integration with the biometric of the human being. Thus, by this bio-smart card technology including with the support of the IOT and their applications it is easy to reduce and condemned the digital thefts and crimes.

Keywords: digital forensics, smart card, DNA fingerprint, cyber attacks, biometrics, IOT

1. INTRODUCTION

The universe of cybercriminals is steadily advancing with fresh attack procedures being produced. In this situation, various business or IT sectors need to work in a strong digital insight framework. In the last few years, the majority of the cases across the sectors and regions are registered on cybercrimes [1]. Many of the organizations face challenges to be flexible against the occurrence of cyber attacks. Understanding the cyber threats and cyber attacks is necessary for a variety of e-commerce and business sectors. Study of cybercrime and the surveys facilitates the knowledge of perceptive analysis on these attacks [2].

To keep away from these issues, new mitigation measures need to carry out and implemented to interpret the alertness. To edge the damage from the cybercrimes and cyber-attacks, every organization needs to embark on building their cyber defense. The major issue is the lacking of monitoring and accessible of a critical system for managing the cyber risks. Digital crimes can be separated into two classifications: the main contains violations that objective personal computer straightforwardly, for example, viruses and malware; the second spotlights on online crimes that utilize systems or gadgets as intends to perform extortion and fraud through social business and in addition digital fraud, digital scam, digital stalking and cybernetic combat [3].

This paper enlightens the reduction of these attacks by incorporating the DNA (Deoxyribonucleic Acid) of the individual with a smart card to make use in a variety of IOT applications.

2. PRELIMINARY

2.1. Biometric smart card technology

Smart card innovation makes utilization of an entrenched built-in circuit chip that can be moreover a protected microcontroller otherwise, comparative familiarity by means of internal memory or a memory chip alone. The programmed technique incorporating into a smart card for recognizing and validating the living objects is acknowledged as biometric technologies [4]. Identification and verification are the two significant processes of these biometric smart cards whenever any of the biometrics integrated into smart cards.

Most of the organizations introduce the technology of smart card usage for entry level operations, authentications, and accessibility. Many applications also being used these smart cards technologies for transactions in various sectors. For example, in travelling, purchasing the tickets for train and busses are done by these smart cards. However, in banking sectors, ATM cards are being used for transactions and withdrawals of money using ATM machines. These are all less secure to use and they employed with PIN numbers which are easily transferable from one to another and also credentials are easily stolen [5]. Therefore, integration of any biometric to these smart cards can be highly secured and not easily credentials will be stolen. In this paper, authors introduce a practice of DNA integrated smart card to increase the security of the smart card to access various applications and condense the digital crimes.

2.2. DNA profiling

DNA fingerprinting has transformed into an imperative bit of society in different ways. It has allowed us to help to show chastity or fault in criminal cases, to comprehend development conflicts and clear up the fathers

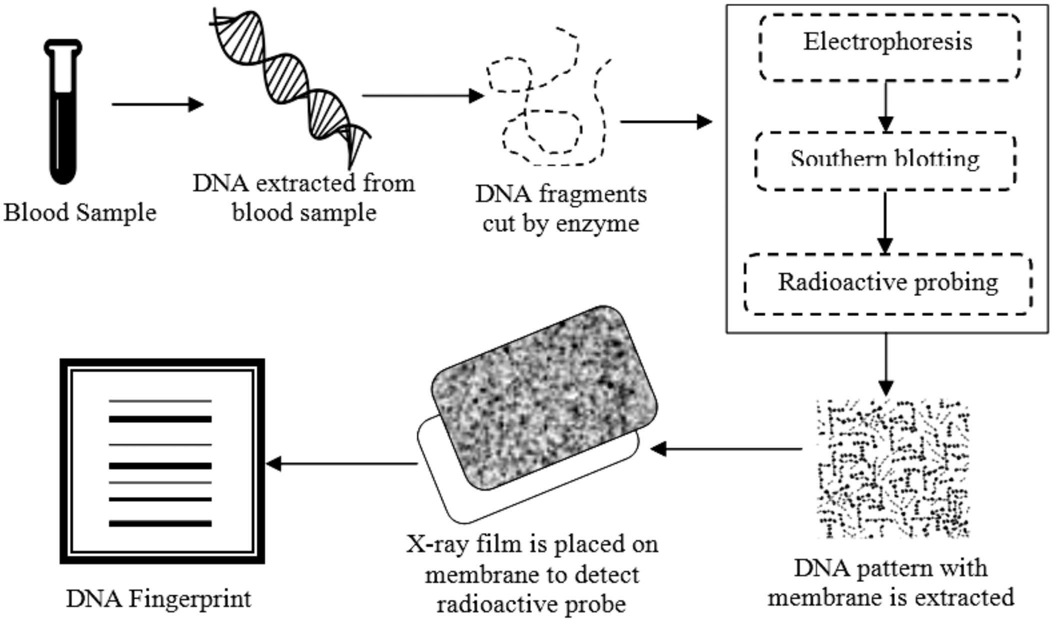
Blood Sample
DNA extracted from blood sample
DNA fragments cut by enzyme
Electrophoresis
Southern blotting
Radioactive probing
DNA pattern with membrane is extracted
X-ray film is placed on membrane to detect radioactive probe
DNA Fingerprint

Figure 1: DNA finger print reading process

of youths [6]. This is all possible in light of the work and research that Professor Sir Alec Jefferys did at the University of Leicester. As the innovation of DNA fingerprinting has propelled, a few social and moral issues have emerged over the privileges of having a subject's DNA. Legitimately in this way, individuals are worried over the outcomes they will confront if their DNA data turns out to be freely available. Hence, one ought to take after the moral principles while working with individual DNA information. The process of an individual's blood sample is metamorphosed into a separate DNA-Fingerprint is shown in Figure 1.

Firstly DNA is extracted from a blood sample, thereby using a restricted enzyme DNA is cut into fragments. These fragments gradually undergo 3 phases- Electrophoresis, Southern blotting, and radioactive probing. During Electrophoresis, an agarose gel separates these fragments into bands and these bands are transferred to the nylon membrane using a special technique called southern blotting.

After that, using Radioactive DNA probe these bands will form sequences on that membrane. X-ray film is placed on this DNA pattern obtained from the membrane for detecting these radioactive patterns. These patterns which are visible on X-ray film is known as DNA fingerprints.

3. INTEGRATED BIO SMARTCARD TECHNOLOGY-WORKING METHODILOGY

The central idea of this paper is the process of inclusion of the DNA onto the smart card to enhance the security from cyber thefts. In this practice, a DNA fingerprint patterns need to be developed from the blood sample of the individual. A smart card is designed by means of an internal region and external surface. The interior part consists of some electronic circuits and a memory buffer area to accumulate the information of the user. A sensor is positioned to interpret the characteristics of the input to validate the users of the particular card. A matching unit will be used to contrast the input pattern with the existed data on the card in the memory area [7]. The DNA of every individual is almost 99.9% identical which consists of 3 billion DNA biopolymer particles of nitrogenous nucleobase or heterocyclic base per each DNA.

Thus, every individual differentiated with no more than 0.1%. For that reason, authors used DNA fingerprint as a biometric on the match on the smart card. DNA is one-dimensional ultimate matchless code for one's individuality. When the user touched the surface of the strip of the smart card, touch DNA will exist; most probably it leaves a fingerprint collected as DNA. This smart card consists substrates of a small minute surface area of glass can be processed for acquiring DNA fingerprint easily. As the area of the smart card surface manufacture as rigid it is easy to access and process the DNA fingerprint. As in Figure 2, DNA fingerprint is processed from the fingerprint from the area it is pressed and lifted on the smart card. When the user uses this smart card in any application, the reader detects the card and confirmed for the authentication.

This process will be done by the card by means of a matching software and compare the pattern which is already existed with the new fingerprint hold by the user. If the authentication success with pattern matches, then it allows the card for the access for various applications. For example, these applications may be bank transactions, entry level authentications in organizations or private areas, to purchase travelling tickets, to show as identity with every detail incorporated in the card. Therefore, a single bio-smart card is enough for every transaction of an individual in his daily life with high security. Crime investigators can easily track the attempts of the stolen cards with the card reader information [8]. Thus, it will reduce the digital thefts and increase security in every transaction and purchases.

4. CONCLUSION

This paper presents an idea to deal with security issues with the smart card transactions. To avoid the credentials thefts of the users' smart cards, a strong bio-smart card is designed. This model can clearly furnish the individual

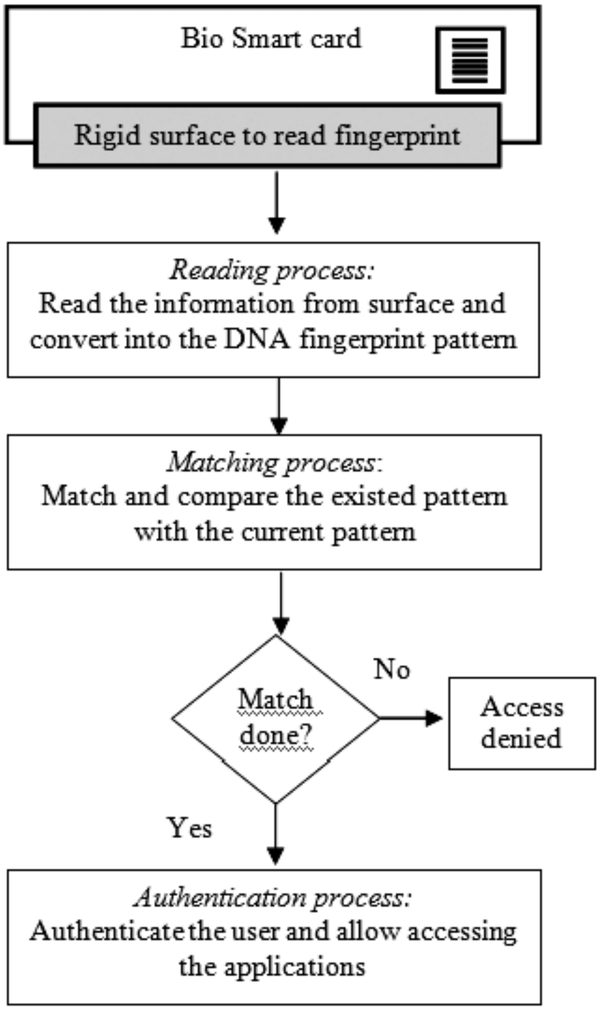
Bio Smart card
Rigid surface to read fingerprint
Reading process:
Read the information from surface and convert into the DNA fingerprint pattern
Matching process:
Match and compare the existed pattern with the current pattern
Match done?
No
Access denied
Yes
Authentication process:
Authenticate the user and allow accessing the applications

Figure 2: Integration and working process of the biometric card

DNA fingerprint pattern on the smart card collected from the blood sample initially. A system which processes the same pattern from the rigid surface of the biometric smart card with sensor technology and matching software inside the card can perform the authentication process and pass the gateway for the transactions.

Any biometric can be used as the security pattern for the smart card, but it may steal easily from the user. For example, fingerprint pattern can be stolen easily from the individual easily with many techniques available in the market. However, the process of collecting the one's DNA and converting into the DNA pattern is not quite an easy task.

Therefore, authors preferred this DNA fingerprint technology to embed on the smart card. So, every bio-smart card can work with the assigned individual only. This type of card can be used for any application where high authentication is required. In future, these smart card can be employed with many applications where secure transactions needed and every of these applications will be centralized. Thus, a single bio-smart card will be unique and worked for all applications to minimize the usage of smart cards for various applications separately.

REFERENCES

[1] Ghosh, S., & Turrini, E. (2010). *Cybercrimes: A Multidisciplinary Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg.

[2] Mazanec, B. M., & Thayer, B. A. (2014). *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*. Palgrave Macmillan

[3] Raghavan, S., & Raghavan, S. V. (2009). Digital Evidence Composition in Fraud Detection. In*Digital Forensics and Cyber Crime* (pp. 1-8). Springer Berlin Heidelberg.

[4] Hussain, S. M., Chakravarthy, A. S. N., & Sarma, G. S. (2013). BSC: A Novel Scheme for Providing Security using Biometric Smart Card.*International Journal of Computer Applications*, *80*(1)

[5] Prasanthi, B. V., Hussain, S. M., Kanakam, P., & Chakravarthy, A. S. N. (2015). Palm Vein Biometric Technology: An Approach to Upgrade Security in ATM Transactions. *International Journal of Computer Applications*, *112*(9).

[6] Smith, G. (2005). *The genomics age: How DNA technology is transforming the way we live and who we are*. AMACOM Div American Mgmt Assn

[7] Noore, A. (2000). HIGHLY ROBUST BIOMETRIC SMART CAFID DESIGN.*IEEE Transactions on Consumer Electronics*, *46*(4).

[8] Fisher, B. A., & Fisher, D. R. (2012). *Techniques of crime scene investigation*. CRC Press.