USING BIOMETRICS TO IMPROVE INTERNET E-BUSINESS SECURITY: A NEW APPROACH

J. Arreymbi[1], V. Odiah[2], A. Ijeh[3], & Ali A. Babatunde[4]
[1&3]*School of Computing, IT & Engineering*
[2]*ShareTray Systems Limited, Knowledge Dock*
University of East London, UK
[4]*e-Promag Consultancy Ltd. UK*
Corresponding Email[1]: j.arreymbi@uel.ac.uk; & Email[2]: vodiahco1@yahoo.com

***Abstract* - Over the past five years, there has been an upsurge in the application and use of biometrics authentication systems on varied IT infrastructure. Today for example, biometric identification and authentication is widely used in airport security, border controls and corporate network security. Most importantly, and in the quest for a more advanced security system to cater for the present day internet e-business environment, the use of biometrics has come to prominent focus. However, using biometrics across insecure communication networks such as the internet has enormous implications and brand new challenges; especially in the wake of increasing and highly sophisticated cyber-crimes such as Identity theft and phishing. The bigger question then arises, what happens when a user's biometrics information is stolen online? This paper proposes a two-layered e-biometric identification and authentication model that aims to prevent the fraudulent used of stolen or spoofed biometrics data.**

***Keyword* -** Biometrics, Two-layered e-biometrics model, BioDater Security Model (BDSM), Internet e-business Security, Biometric security, identification and authentication, Information Systems security, Cybercrime, e-crime, Identity theft and Phishing.

I. BIOMETRICS EVOLUTION AND USES

A. Introduction

Biometrics is the science of the measurement of unique human characteristics, both physical and behavioral. Various biometric technologies are available for identifying or verifying an individual by measuring fingerprint, hand, face, signature, voice, or a combination of these traits [1].

According to [2], many large companies now use fingerprint sensors for logging on to corporate networks. And in Texas State, driver's license authorities employ face recognition for capturing and storing digital photographs and the first iris-scan-protected ATM in the nation was introduced in May 1999.

Biometrics technology has increasingly become important with significant usage and new areas of development or implementation throughout modern societies. Many application methods have been implemented over many centuries [3], and the technologies that come with collection, storage, use and analysis of biometrics data have also evolved and become significantly sophisticated. The evolution is primary from the technological perspectives, though taking into account some organisational complexities. Recently, these technologies have come under a lot of scrutiny due to the security of the stored biometric data and privacy concerns [4].

However, Don Erickson - Director, Government relations, Security Industry Association (SIA) - in a recent interview [4] claims that, the benefits of biometric technology outweigh its privacy concerns.

Biometrics as a unique identification technology may seem new but it has been in application for thousands of years. Its history dates back to the 14th Century when palm prints and foot prints were used by the Chinese to identify babies, and fingerprint stamping on documents was also widely accepted system used to identify authors of written texts [5].

Reference [3] earlier noted that the ancient Egyptians and the Chinese both played a significant role in the history of biometrics. The study also supports the fact that, biometrics technology has actually been in application for thousands of years, although many see it as technology developed in the 20th century. A report by [6] also stated that, since the beginning of civilization, humans have used faces unique and physiological traits-like features to identify known (familiar) and unknown (unfamiliar) individuals. This evidently is still in application today. Humans instinctively recognize each other by their inherent ability to scan, store and compare biometrics traits such as faces, voice, body anatomy measurements.

According to [7], Biometric identification and verification has also played a significant role in law enforcement over the years, especially in identifying criminals. In the 19th century Alphonse Bertillon, a French Police clerk developed a system, which was later known as the Bertillonage system. The system of biometric identification made use of measurements of some specific parts of the human anatomy, as well as marks on the body. The Bertillonage system is a form of anthropometry - a system by which measurements of the body are taken for classification and comparison purposes. This system of biometrics recording required numerous and precise measurements of the bony parts of a human's anatomy for identification. It also involved recording shapes of the body in relation to the differential markings on the surface of the body such as scars, birth marks, and tattoos. These marking added additional accuracy based on the assumption that no two individuals will have exactly the same marking on exactly the same parts and position of their bodies. However, the Bertillonage system was eventually dismissed due to significant inaccuracies introduced through human errors in recording the actual measurements used for identification and also the lack of standards.

The significant evolution of biometrics systems has led to further advancements and refactoring of existing systems. Modern advancement of technology has led to many improvements in the area of biometrics. One such major development is the signature authentication system, developed in the 1960s which led eventually to the signature verification system in use today [8]. It has long been known that each person has a unique handwritten signature. The way a person signs their name or writes a letter can be used to prove a person's identity. As a replacement for a password or a PIN number; dynamic signature verification is a biometric technology that can be used to positively identify a person from their handwritten signature [8].

And reference [3] had also confirmed the idea that, signature biometric authentication procedures were in existence since the 1960s and 70s. However, the biometric field remained fixed until the military and security agencies researched and developed biometric technology beyond fingerprinting. Today, there are a wide range of biometric authentication technologies and these are spreading with the speed of the present day information technologies.

Meanwhile, [9], in an article "Biometric pace of change gives Canberra the jitters" noted that, Biometric technology has changed and is continuously changing at such a rapid pace that government departments have no other choice but to work continuously on backend systems in preparation for biometrics deployments; while waiting for the emerging technologies to mature.

B. Types of Biometrics

Biometrics has been deployed in several areas of our everyday life including airport security to immigration and border controls [10].

Some of the present day biometrics authentication systems identified in this paper includes the following:

1. Fingerprint identification
2. Face recognition
3. Iris scan and retina identification
4. Hand geometry
5. Handwriting and signature
6. Voice identification and verification
7. Facial thermograph
8. DNA matching

9. Gait recognition
10. Ear Shape identification
11. Keystroke Recognition

The development, application and use of biometrics in today's dynamic information systems environment, spans across government and private networks from airport security and border control, to military and corporate access control, as well as in banking, medical (records) establishments and schools; and all these poses new challenges which can be affected by various factors such as political, legal and ethical issues. Reporting on the use of biometrics in Schools, [10] found that thirty per cent (30%) of High Schools the UK are taking fingerprints simply to speed up basic administration activities such as borrowing library books, registering in the mornings and buying canteen lunches. In fact the reasons for this, have very little to do with the issues discussed and sometimes they ignore the implications of collecting and storing such data. Biometrics today, with retinal scans, voice recognition, hand geometry, movement and signature recognition, have far surpassed anything our ancestors would have predicted [11].

II. DRIVING FACTORS

The fast and increasing range or use of biometrics application today can arguably be attributed to the following main factors [12]:

1. The need for a more advance user identification, verification and authentication system in terms of access control.
2. The need to demarcate and preserve information systems, and the increasing volumes of sensitive information that these systems continue to process, transport, and store.
3. The uniqueness of the physiological traits used for most biometric authentication - fingerprints.
4. Government and business drive for improved security – identity, fraud and terrorism (both inland and cyberspace).

According to [13], the National Fraud Authority reported that ID fraud is one of the fastest-growing crimes of the 21st century. It now affects more than 1.8 million people every year in the UK, with fraudsters netting at least £1.9 billion from the crime. Also, [14] and [15] had both stated the fact that, internet security has grown to become a major IT challenge in recent years. They believe that there are many inadequacies in the current information security counter-measures. Internet users are vulnerable online where their data or private information can be stolen in a number of ways, for example, through use of spywares and/or phishing. A website holding users information can easily be compromised using spoofing techniques, which entails the use of a look-alike website to fraudulently collect users' information unsuspectingly.

Presently, usernames, passwords and pins are the most widely used internet security mechanisms. However, in recent times there have been increasing accounts of more sophisticated e-crimes, exploiting the known flaws of the password and pin security systems. In their research [14], [16] clearly identified that the system of username and password is too easy to compromise using monitoring software and spyware, phishing and other readily available tools and techniques. Meanwhile [17] reported that the number of PCs compromised with software that lets cybercriminals to control the machines remotely, had more than quadrupled in recent times. The issue raises many questions; and, from a security point of view, it is very alarming. It demonstrates serious need for more advanced security system to preserve the future of the new "internet culture" which has so much benefited the human race within this short period in history. The undeniable truth is that, the highly complex and increasing volumes of crimes against information systems, especially e-commerce systems and internet users show that; current protective measures in information systems are inadequate and have outstretched the traditional pin and password defensive measures.

The present day technological environment has outgrown the traditional password and pin security infrastructure that we seriously rely on every day, seemingly to protect our virtual domains. Again, [14] noted that the reasons for the current increase in attacks have been due to the following factors:

1. The fact that, so many people are increasingly connected to the internet.
2. And most users are not taking adequate precautions in protecting their personal details.

Reference [14] suggested that, adequate measures in this context could imply using modern security implementation tools and techniques to protect the ever increasing digital assets. That is, 'looking beyond the traditional password and pin', into for example; digital signatures, certificates and biometrics. It is very evident that securing users' information as well as organizations digital assets is highly imperative, especially with e-commerce distributed systems. In fact, very few will argue that, when pitted together - the present day sophisticated cybercriminals against the ordinary online users' – the two do not compare. The traditional user-password and pin security measures are so inadequate to the advanced skills/abilities of the techno-savvy criminals. Therefore, this singular notion undoubtedly justifies the need for a more advanced security system that can withstand the rigours of high-tech cybercrime attacks associated with the current internet environments. The reference [18] reported another incident where a hacker used virus-laden spam emails and online webcam to remotely spy on women, harvesting users personal emails and peeking on confidential hospital patients and government records.

Therefore, the serious IT threat, that of using technology to fraudulently capture and use unsuspecting users' information by criminals must be curbed. These online activities have increasingly driven many IT security stakeholders to consider the use of biometrics and in this case, electronic biometric (e-biometrics) systems as a security measure; an alternative to, and/or timely replacement or enhancement of the password and pin security measures.

However, for this to happen there is need for a better way of biometric integration between and within systems. For example, in a vertical integration, the National crime, Health care, Police and the Judiciary systems should share their databases, to make the processes more effective. But, such a process could be faced with issues of privacy, and therefore requires a mandatory legal framework before integration.

According to [19], the fact that identity theft and other security breaches continue to be on the increase; many businesses and governments are finding it very hard to retain clients and achieve or maintain 'consumer-trust.' And it is a goal ever more highly sought after by organisations and governments across the globe. Therefore e-biometrics might just be the key to maintaining trust and building consumer confidence in online systems use.

A. The Fear Factor(s)

One major factor that has hindered the widespread use of biometrics security across the internet is the threat of theft of biometrics data. A preliminary unpublished research survey by Arreymbi & Odiah in March 2009 showed that, all of the respondents (100%) feared their biometric information could be stolen and/or compromised if captured, stored or used on any online system. Also, a majority (85%) of the respondents expressed concerns with ethical issues of biometrics.

Therefore, in this paper we will attempt to provide some answers to the following questions:

1. How do we prevent the exposure, and theft of users' biometrics details online? Noting how easily users' login information can be stolen through the use of software or other methods such as phishing.
2. How do we prevent online users' biometric data misuse or fraudulent use, if captured or compromised?

B. The Solutions

The fact that biometrics are tied to users' physiological traits that may not change over a period of time; there is great need to prevent the theft and use of stolen biometric data. Therefore there have been several attempts or approaches to creating a flexible/ cancellable biometric, such that, stolen biometrics can be cancelled and reset as easily as resetting a users' password.

Reference [20] identified 4 ways of creating cancellable biometric, namely:

1. Biometric salting- this approach wraps the original biometric around a pseudorandom string.
2. Bio-Key Generation: this approach stores a parameterised biometric data instead of the original data.

3. Fuzzy schemes approach: this method combines the actual biometric with a public auxiliary information.
4. Non Invertible transforms- this approach transforms the biometric using a one-way function.

The above approaches are based on the combination of the biometric data with a token, with a view to creating a new biometric signature that encapsulates the original biometric data and improve security and user privacy.

For simplicity this can the illustrated as follows:

$_pS(B_o)$ where;

$_pS$= the pseudorandom string,
B_o= the original biometric data

It is clear these approaches address the issue of making biometrics cancellable or reset-able. However, they do not address the issue of reuse of a compromised biometric data, where the stored biometric data has not been reset, as any comparison will be based on value against value, such as:

$_pS(B_o) = {}_pS(B_o)$.

The system will only be effective in a case where, the stored biometric data has been reset to create a new signature, such as $_pS_2(B_2)$, thus the comparison will be:

$_pS(B_o)$ against $_pS_2(B_2)$.

Therefore, with regard to the above, we present a proposed BioDater security model to further address this grey area.

III. THE PROPOSED BIODATER SECURITY MODEL (BDSM)

A. Introduction to BDSM

The BioDater [Biometric + Date stamp] security model (BDSM) is a two-layered e-biometric model based on an algorithm that combines the original biometrics data (B_o) with a pseudo-random string ($_pS$) and the current timestamp (T_c) to create a more flexible and query-able signature. The biometric data in use can be any form of biometric data captured such as, finger print data entered through a scanner for the purpose of identification. The resultant biometrics object (B_rO) created by the BioDater security model (BDSM) is a product of the original biometric, the random string and the timestamp and therefore creates an extra layer of comparison based on its date and time attributes.

i.e. BDSM ==> $B_rO = B_o + {}_pS + DT$

This date-time attribute of the BioDater object (BDO) enables the querying of specific attribute like date and time of creation (DTC) and the object's Time-To-Live (TTL).

B. The BDSM registration and authentication process

At the point of enrolment of biometric data, the entered biometric data is parameterised with a pseudorandom string and the current timestamp. The algorithm is illustrated as follows:

$_pS\ (B_o) + T_c$. Where;

$_pS$ = the pseudorandom string,
B_o = the original biometric data
T_c = the current timestamp

The BDSM authentication algorithm comprise of comparisons at two separate layers as follows.

1. Layer 1: at this point T_c is compared against T_n
2. Layer 2: $_pS(B_o)$ is compared against $_pS_n(B_n)$.

The layer 1 comparison as above queries the Timestamp attribute (T) of the BioDater object in line with the following:

1. Test for Time-To-Live
2. Test for exact duplicated samples
3. Test for Out of range samples.

B.1. Test for Time-To-Live

This test ensures that the entered BioDater sample, which will be used for authentication has not outlived a specified TTL. By attaching a specific TTL to a BioDater sample, we aim to prevent the reuse of a Biometric sample that may have been stolen in transit; for example, through a man in the middle attack, or phishing techniques. The

sample will expire as soon as it outlives its TTL.

B.2 Test for Duplicated samples

Testing the time-stamp attributes for exact duplicates at this layer aims to prevent the use of a BioDater sample that may have been compromised directly from the storage source, for example, a case where the sample has been stolen directly from the database. The time-stamp attribute will match value for value and will not be authenticated as the time-stamp on the sample required for authentication must be different from the time-stamp attribute of the stored copy.

B.3 Test for Out of range samples

If the date-stamp attribute of the entered sample is less than the date-stamp attribute of the stored copy, this will imply that the entered sample has been created earlier than the stored copy. At this stage the authentication will fail as the sample required for authentication must bear a time-stamp attribute greater than that of the stored copy.

Based on the BDSM, re-enrolment creates a new biometric template (BT) with a new time-stamp attribute. Therefore, any previously stolen BioDater sample will bear a date and time stamp less than the new template. And, any BioDater sample stolen before the BioDater template update cannot be used.

C. Layer-2 Security

The second layer security is an authentication process which deals with comparison of the actual parameterised biometric data (i.e. ${}_pS(B_o)$ as above). In essence, it is comparing the extracted biometric data sample entered, with that of the stored template. And the process will only be executed if the layer 1 security tests have been successfully.

IV. VALUE OF BIODATER SECURITY MODEL (BDSM) IN E-BUSINESS.

Researchers such as [14], [21] and [22] have all highlighted the fact that internet and e-business users (over 40%) still fall prey to cyber scammers and easily give away their private login and banking details. Hence, it can be deduced that users' e-biometric information could be vulnerable to phishing and other threats. And it becomes even more critical if users' e-biometric data is captured or stolen online. Therefore it is imperative that a solution is provided to prevent the fraudulent capture and use of e-biometric data.

For e-business applications, it is believed, the BioDater security model (BDSM) will prevent the fraudulent use of stolen or spoofed biometric data over the internet. It will also prevent the exposure of users' plain biometrics data, which most users fear could be used for other fraudulent purposes, by creating a BioDater sample which is made up of the user's biometric data, a pseudorandom string and the current date and time stamp at the point of entry.

V. CONCLUSION

In this paper, we have examined methods of creating cancellable biometrics and used the techniques to propose a model for online biometric data security called BioDater security model (BDSM). The model provides a two-layered biometrics authentication algorithm with a view to overcome the threats of re-use of stolen biometric samples. The BDSM approach is continuously being developed and tested, and requires further studies to provide improve e-biometric security.

REFERENCES

[1] Xiao, Q. (2007), *Technology review - Biometrics-Technology, Application, Challenge, and Computational Intelligence Solutions,* (Computational Intelligence Magazine, IEEE), Available online at; http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4168416 (Accessed 04/11/2010)

[2] Stikeman, A. (2003), Biometrics (MIT Technology Review). Available online at: http://www.technologyreview.com/printer_friendly_article.aspx?id=12255 (Accessed 04/11/2010)

[3] Osborn, A. (2005), *Biometrics History - Looking at Biometric Technologies from Past to Present,* (Evaluseek Publishing) Available online at; http://ezinearticles.com/?Biometrics-History-Looking-at-Biometric-Technologies-from-Past-to-Present&id=91803 (Accessed 29/11/09)

[4] Erickson, D. (2010), *The security benefits of biometrics technology outweigh the privacy concerns,* (Haymarket Media). Available online at: http://www.scmagazineus.com/the-security-benefits-of-biometrics-technology-outweigh-the-privacy-concerns/article/167966/ (Accessed 04/11/2010)

[5] Ríha, Zden and Matyáš, Václav (2000), *Biometric Authentication Systems.* Available online at; http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf (Accessed 25/11/09)

[6] NSTC Subcommittee on Biometrics (2006) Available online at; http://www.biometrics.gov/Documents/BioHistory.pdf (Accessed 25/10/09)

[7] GlobalSecurity.org (2008) Biometrics Available online at: http://www.globalsecurity.org/security/systems/biometrics.htm (Accessed 20/04/09)

[8] BioVeriCom (2004), *Handwriting Biometric.* Available online at: http://www.biovericom.com/biotech/signature.html (Accessed 05/11/2010)

[9] Tung, L. (2008), *Biometric pace of change gives Canberra the jitters* (CBS Interactive/ ZDNet), Available online at:http://www.zdnet.com.au/biometric-pace-of-change-gives-canberra-the-jitters-339286421.htm (Accessed 04/11/2010)

[10] Clark, L. (2010), *One in three secondary schools fingerprinting pupils as Big Brother regime sweeps education system,* (Associated Newspapers). Available online at: http://www.dailymail.co.uk/news/article-1285305/One-schools-fingerprinting-pupils-Big-Brother-regime-sweeps-education-system.html (Accessed 04/11/2010)

[11] Associated contents AB (Aug 09, 2006), *A Short History of Biometrics*. Available online at; http://www.associatedcontent.com/article/48809/a_short_history_of_biometrics.html?cat=15 (Accessed 20/9/2009)

[12] *Biometric Market & Industry Report 2009-2014.* International Biometric Group (2008). Available online at: http://www.biometricgroup.com/reports/public/BMIR_2009-2014_TOC.pdf (Accessed March 2010)

[13] Davies, L. (2010) *Will you fall for ID fraud*. Experian, (November 2010). Available online at: http://74.6.239.67/search/cache?ei=UTF-8&p=will+you+fall+for+ID+fraud%3F&fr=yfp-t-702&u=uk.m2.yahoo.com/w/ygo-frontpage/lp/story/uk/20629/coke.bp%3Fref_w%3Dfrontdoors%26.ysid%3D.oQymImzc4ohT8uWhCJk1Jmt%26.intl%3Dgb%26.lang%3Den-gb&w=will+fall+falling+fell+id+fraud&d=NEQlHVtsV02O&icp=1&.intl=uk&sig=8qVzzneGoMFgACkP3qon8g-- (Accessed 10/11/10)

[14] Arreymbi, J. (2005), *Online Banking: Spoofing Scams exposes Security Loopholes.* In Securing Electronic Business Processes. Paulus, S., Pohlmann, N., and Reimer, H.; (Eds). ISSE 2005, Vieweg Publishers. Germany pp 289-300

[15] Tyler, Thompson (2005) Internet Security Article PC Mech. Available online at; http://www.pcmech.com/article/internet-security-article/ (Accessed 19/9/2009)

[16] Saita, A. (2005) *Taking a swipe at two-factor authentication.* SearchSecurity.com. Available online at:http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1077406,00.html (Accessed 20/9/2009)

[17] Krebs, B. (2008) '*Number of Bot-Infected PCs Skyrockets*'. Washington Post, September 4, 2008. Available online: http://voices.washingtonpost.com/securityfix/2008/09/number_of_bot-infected_pcs_sky.html (Accessed 10/12/09)

[18] Attewill, F (2010) *Hacker who spied on women jailed.* London Metro Newspaper, p23. Wednesday Nov. 24, 2010

[19] Cohn, M, (2007), *Biometrics: Key to securing consumer trust* (Biometric Technology Today / Elsevier B.V.) Available online at: http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6W70-4NBYDTT-M&_user=10&_coverDate=03%2F31%2F2007&_rdoc=1&_fmt=high&_orig=search&_origin=search&_sort=d&_docanchor=&view=c&_searchStrId=1533687914&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=9356ad121527ae79352e128905e09c6e&searchtype=a (Accessed 04/11/2010)

[20] Ratha, N., Chikkerur, S., Connell, J., and Bolle, R., (2007), *Generating Cancelable Fingerprint Templates* (IEEE Computer Society) Available online at: http://www.comp.hkbu.edu.hk/~ycfeng/project/Generating%20Cancelable%20fingerprint%20templates.pdf (Accessed 04/11/2010)

[21] Bright, M. (2003), *Online Identity Theft: Spoof Email Phishing Scams and Fake Web Pages or Sites*. Available online at: http://www.millersmiles.co.uk/identitytheft/gonephishing.htm (Accessed 23/2/10).

[22] Knowthenet.org.uk (2010) Available online at: http://www.knowthenet.org.uk/articles/knowthenet-study-reveals-face-brit-most-likely-be-scammed-online-0 (Accessed 15/11/2010)