ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 2 (Issue 1) (2018) Pages 35-43

Gaps in the Management and Use of Biometric Data: A Case of Zambian Public and Private Institutions

Melissa K. Chinyemba
School of Engineering
Dept. of Electrical & Electronics Engineering
The University of Zambia
Lusaka, Zambia
email: kaemelissa@gmail.com

Jackson Phiri
School of Natural Sciences
Dept. of Computer Science
The University of Zambia
Lusaka, Zambia
email: jackson.phiri@cs.unza.zm.

***Abstract* —The current physical and cybersecurity systems rely on traditional three factor authentication to mitigate the threats posed by insider attacks. Key is the use of biometric information. Biometrics are a unique measurement and analysis of the unique physiological special traits such as voice, eye structure and others that can be used in the discipline of varying person identification. Biometry, which is the analysis of these biometrics is a complex process but guarantees identification and non-repudiation. If used to identify humans then several issues such as where is the biometric data stored? Who has access to it? And how does one ensure that such data satisfies the principle of availability. To achieve AVAILABILITY, secure transportation arises. To achieve transportation, non-repudiation, confidentiality and authentication, integrity arise. A storage and transport system is recommended to these challenges. In this paper, we explore the gaps into how public and private institution store and manage biometrics information. We benchmarked each organization again the ISO 30107 and ISO 24745. Our results show that while most companies are adopting and using biometrics systems, few have adopted the ISO biometrics standards that govern the storage and management of biometric information and hence creating security risk.**

Keywords — *Storage, Confidentiality, authentication, integrity, transport.*

I. Introduction

Secure, correct and efficient user authentication is an integral component of any meaningful security system. Protection of data from unauthorised access, including resilience of the underlying ICT infrastructure to various sorts of attacks, has become one of the main technological challenges faced by business houses today. This is because ICT has become more prevalent and complex, meanwhile the increase in the sophistication and volume of cyber-attacks by both insiders and outsiders are at an alarming rate. Digital storage is the ability of a computer device to accept, hold or retain data until such a time that is requested for by a computer user or resource. Storage can be classified into two namely, primary and secondary. Primary storage holds all data that is currently in use. Secondary storage holds data that is not currently in use[1] [2].

Primary storage cannot hold biometric data because this type of storage retains operational data transiently. Secondary storage forms the base for storage of biometric data as this type of storage retains data that can be transported to main storage should it be needed. Primary storage has volatile features that inhibit its use. Volatility of a storage medium is its capacity to lose contents when power is disabled from it [1]. Examples of primary storage includes read-only memory (ROM) chips and Cache housed on a printed circuit memory module. Secondary storage does not have volatile features. Examples of secondary storage includes removable flash drives, portable hard drives, internal hard drives and optical mediums such as compact disks and others which permit logical access to data as cloud storage systems that are Internet access based. Flash drives prove to be the most popular medium of choice for most people due to the portability factor and convenience of carrying. The discussion on problems of secondary storage is skewed towards them [1].

An insider is a past of present employee or business stakeholder who has or had legitimate access rights to the organisational resources, but decides to compromises the security of the resource [3]. This is a complex threat for most organisations to avert today because it borders on disclosure of classified information by actors who have full access by virtual of being an employee of stakeholder [1]. Cyber security the two types of threats which organisations have to deal with includes insiders and outsiders. However, Insider threats more are challenging because of their nature and complexity to detect and deter. Insider threats are grouped into two categories including; malicious (intentional) and non-malicious (accidental) [4].

A malicious insider is any business associate who has or had access rights to the network system and intentionally abuse the same privileges in a manner that adversely affects the organisation's information systems confidentiality, integrity or availability [4]. Malicious insider threats includes; IT sabotage, Fraud and IP theft [5][6]. Basically, one does not become a malicious insider until they abuse their access rights and or committed a crime [7]. They are simply an insider, however, it is worthy probing the track taken from being an insider to malicious insider [8].

II. BACKGROUND

A research of insider attacks in the banking and finance sector summarized the observed characteristics of the attacks are as follows [9]: Utmost incidents required little technical sophistication, Activities were planned, Inspiration was financial gain, Deeds were committed on the duty and Incidents were commonly detected by non-security personnel and by manual techniques.

Bearing in mind that the sample size was small and biased, this brief list still proposes both that there is a great deal of room for improvement in defying insider threats, as well as finding solutions that need to engage both human and technical systems[10]. The interplay between security policies and organizational dynamics is critically important to successfully reducing insider threats, since insiders have exceptional knowledge of the organization than outsiders. Organizations do work around security policies deemed unacceptable, while the real flow of work may be very different than the official representation. Understanding and managing organizational realities is a nuanced and difficult problem in developing effective policies. This pressure between technical methods and the need to integrate sociological and organizational perceptions is an essential aspect of the insider threat arena. We acknowledge this pressure by in turn examining each of the major solution spaces: technical methods, methods that seek to apply socio-technical methods finally sociological methods. We generally consider three core types of insider attacks namely; misuse of access, bypassing defenses, and access control failure [9][10]. For each the relative effectiveness of technical versus non-technical approaches varies:

- Access-control failure- insiders should not have access to specified resources. This is a technical problem and, while prevention is straightforward, detection of access-control failures is difficult same as with access-control misuse [10].
- Access misuse - the insider has rights and within those rights can misuse system resources, probably the hardest form of attack to detect or prevent technically, since the insider already has legitimate access [10]
- Defense by-pass - insiders already inside the perimeter, and therefore have more opportunity for mischief. Purely technical defenses are insufficient, because if they worked, the problem would not exist. Dependence on technical or non-technical detection of anomalous behavior or actual attacks is vital [10].

The insider threat is a single name jacketing a variety of different threats. In practice to date no single method has proved prevailing as a solution, hence the importance to consider any solution space as likely combining elements of prevention, detection and response against the three acknowledged attack types using both technical and sociological mechanisms.

Privacy threats in biometric systems

Below we showcase the potential privacy pitfalls arising when using a biometric identifier. Biometric can expose sensitive data such as information about one's health and racial origin and this information can then provide a basis for unjustified discrimination of the individual data subjects [11].

Researchers also revealed that biometric data are unique identifiers but are not secret: fingerprint is leaved on everything we touch, faces can be easily acquired and voice can be simply recorded. Hence, the potential collection and use of biometric data without knowledge of its owner, without his/her consent or personal control make this information very sensitive [11].

Many advocates of biometric systems claim that it is adequate to store a compact representation of the biometric rather than the raw data to ensure privacy of individuals. They contemplate that template is not delicate information because it doesn't allow for reconstruction of the initial signal. However, very recent, several research works showed that this reconstruction is possible [12][13].

The connection problem which means the possibility to cross harmonized data across different services or applications by likening biometric references is another privacy distress. Biometric characteristics exclusivity allows an intruder to relate users between diverse databases, enabling defilements as tracking and profiling individuals [10][11].

A function creep is another secrecy risk where, the acquired biometric identifiers can later be used for purposes not meant for. The inherent inevitability of biometric features in case of data misuse like database concession or identity theft makes biometrics very profound. With the present risks on privacy violation, carefully handling biometric data becomes more imperative. Bearing in mind the implication of personal identified information' (PII) sensitive data, biometrics use falls within the purview of laws and regulations. In the consequence, we are interested in the main attack vectors regarding biometric systems [11].

III. LITERATURE REVIEW

A. *Review of Current Biometric Storage systems*

*Data-at-Rest Risk Factor*s: The identified risk factors targeted at secondary storage medium includes; Media Theft-where the device containing the biometric data gets or the device is stolen [5][6]. Data Corruption where the data held on the device or flash-drive gets corrupted due to incorrect usage [7]. Storage Wear (flash-drive) refers to the wear and tear of the storage device due to time or age. A flash drive memory cell's lifetime is finite and each flash drive memory cell has limited endurance. The data written and deleted onto or from the device cannot be done time beyond a certain number (reprogrammed continuously). Each flash drive memory cell is called a single level flash cell (SLC) and each SLC has an industrial tolerance of approximately 10k program/erase (P/E) cycles while a 2-bit multi-level cell (MLC) has an industrial tolerance of about 3k P/E cycles [8]. Data Diddling - A possibility exists where an attacker can fiddle with the data held on the storage device (flash drive) before handing it over to systems users for either storage or processing.

Data that is resident in Cloud Systems suffers the risk of Confidentiality, Integrity & Availability. The issues of keeping information secure and confidential in a cloud storage system are paramount. The owners of the cloud service system have literal control over the data they hold on behalf of their customers and this may imply that they can modify data to their liking without the data owner's consent. This act amounts to insider threats. Cloud systems are internet based making them accessible to both insiders and external hackers [14]. The difficulty therefore is managing access control.

The ideal access-control policy simultaneously grants the user sufficient privileges to perform necessary tasks, while constraining access according a set of rules. The rules are based on principles of least privilege, escalation and separation of duties [11]. Access control is the mechanism of providing and limiting access to electronic resources based on a set of credentials. The two components of this mechanism namely, authentication: showing who or what you are (e.g., biometrics), by demonstrating possession of certain credentials and authorization: determining if your credentials are sufficient to provide you with a requested type of access. The extent to which explicit, fine-grained access controls can be defined and enforced shapes very directly the type of insider misuse that might occur [13].

B. Access control

In its basic form access control maps users with access to resources. Role-Based Access Control (RBAC) is a finer-grained method that maps defined roles with access to resources. Temporal RBAC extends this method by specifying time constraints on when a role can be enabled or disabled. Different methods of implementing access control have also been proposed, more iimportantly that access control policies also need to be able to specify monitoring and auditing requirements[15]. However, access control has a number of limitations, because even perfect access control will not prevent insider attacks who are only using privileges that are deemed necessary for their daily task. Various studies shows a disconnect between what real world practitioners desire and what the research communities offer. Meanwhile, llimiting access legitimately can have a negative impact on the productivity for non – malicious employee [15].

C. Biometric attack vectors

The possible attack vectors in biometric systems have been discussed from different viewpoints. The first being the scheme of figure 1, by the international standard ISO /IEC JTC1 SC37 SD11. This identifies where possible attacks can be conducted[16].

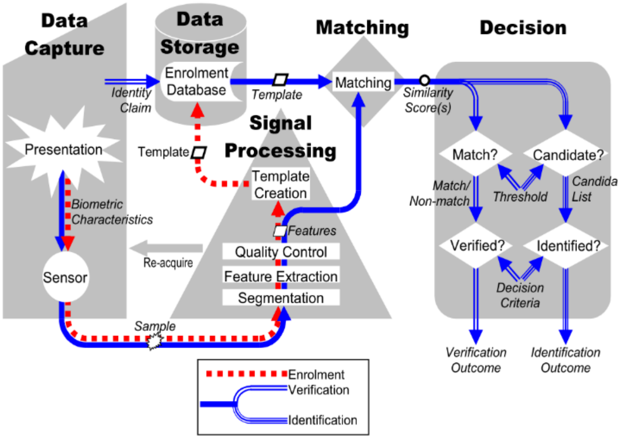


Fig 1. ISO Illustrations of error rates for different biometric modalities [16]

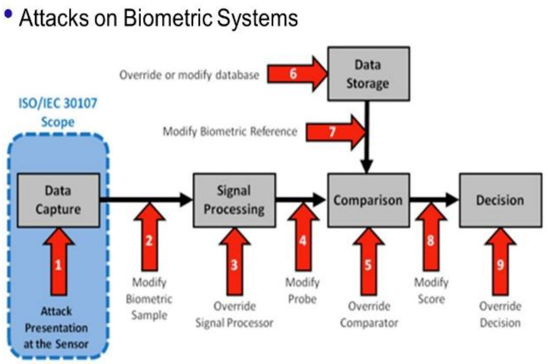


Fig 2: ISO's model attack framework [16]

All biometric systems involve two steps namely Enrollment step and verification step. ISO 30107 illustrates a presentation of a biometric attack detection [16].

IBM researchers identified and categorized a number of the biometrics related. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system:

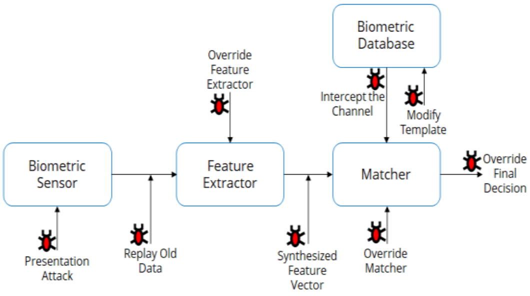


Fig 2: IBM's biometric threat model [17]

Presentation Attack – Spoofing the biometric trait, such as with a finger mold, presented at the sensor, Replay Old Data – Resubmitting illegally intercepted data to the system. Override Feature Extractor – Overriding the feature extractor to produce predetermined feature sets. Synthesized Feature Vector – Replacing legitimate feature sets with synthetic feature sets. Override Matcher – Overriding the matcher to output high scores, thereby defying the system security. Modify Template – Compromising the templates stored in the database. Alternately, introducing new templates to the database. Intercept the Channel – Altering the data in the communication channel between various modules of the system. Override Final Decision – Overriding the final decision output by the biometric system. Several security techniques exist to thwart attacks at various points, including encrypting communication channels, using mutual authentication, placing the feature extractor and the matcher in secure locations, and limiting unsuccessful attempts.

Figure 8. Cloud Storage [18]

D. Data-in-Motion Factors

Cloud related systems have problems in data transportation systems that includes;

Insecure Protocols and insecure implementation of secure protocols: Wireless authentication protocols like Open System Authentication protocol (OSA) do not offer any form of secrecy or privacy and send everything in the clear state. In addition OSA allows any device to connect to its wireless network as along as it has capability to connect. This may breed access to sensitive data held on cloud storage systems. Other protocols transmitting data in the clear state includes Telnet, FTP and HTTP among others. A network level TCP session hijack may take place on HTTPS and indeed if it proves to be successful, this may result into the impression that a secure channel is in use by a user and a file server holding biometric data when in actual sense an unsecure channel is in use [19][20]. The *Simple Network Management Protocol* (SNMP) presents authentication problems as credential data is sent over network connections in the clear state [21]. The effect of this insecurity results into; Data Interception, Eavesdropping, Replay attacks and Modification of the data [22].

Unknown longevity of cloud storage: whereas the convenience of access of online storage materials is ideal, caution must be taken when using such systems as some close down for some reason [23].

Data transportation via Email: Email, does not provide secure transportation of data due to the following factors [24][25]

The Advent of BotNets: Malware (Malicious **S**oftware) is an enabler for cybercrime. Numerous arrangements of malware in form of bots or botnets may infect and injure a network’s operations. Backdoor and Crimeware are typical examples of botnets that may compromise a computer network and either steal biometric data or corrupt such data. A Backdoor may occur in a computer system, cryptosystem or algorithm and this may be a means of circumventing authentication that safeguards a computing resource. Backdoors have abilities of obtaining remote computer access stealthily making it very difficult to detect them. Backdoors can be installed on software or hardware systems. Crimeware are types of bots engineered to automate identity theft crimes. This allows a botmaster (creators of the botnets) to access online accounts of users at financial institutions and in some cases online retailers for the purposes of stealing money or to perform unauthorized transactions to the benefit of the botmaster. Crimeware may export private information such as biometric data that may include, personally identifiable information (PII) like facial data from a network so as to allow for financial exploitation [26][27].

Whereas the convenience of access of online storage materials is ideal, caution must be taken when using such systems as some of these systems have been known to close down for some reason. This closure has ability to create disorientation in the user [27].

Ttransportation of data in the clear state and insecure storage of emails and its systems.

Email servers may be in a non-authentication mode which allows no authentication between a host and the email server which may result in data theft of the biometric data [2].

IV. SUMMARY OF GAPS IN REVIEWED BIOMETRIC DATA TRANSPORTATION AND STORAGE

A. Storage Problems (data-at-rest or data-in-motion)

Whether cloud storage systems are employed or secondary storage systems are in use, it is important to bear in mind that Silent Data Corruption (SDC) may occur. Among the more common SDC include; Errors unreported and undetected in storage systems, corrupt data will be returned to applications without any warning and a single bit error can affect a significant volume of data[28][29]

Several factors may harm biometric data and make it unreliable due to data corruption. This may be caused by; On-the-wire corruption which is the data path corruption, as the data propagates on a network from one end to the other electronic magnetic interference, network jitter or data burst may all lead to changes in the data-in-motion and result into an erroneous package content [29][30].

B. Incorrect writes

Incorrect writes may be caused by incorrect parameter definitions that may prevent data being written to or being accessed from a device. This problem is common on external optical drives, flash drives and other related externally connected mediums such as Secure Digital (SD) cards. Such parameter problems are normally caused by issues that include, file systems corruption, bad sector presence, and incompatible sectoring systems in use and general disk errors or power issues, unstable revolutions for optical drive mechanisms. The results of such would normally be, Unfinished writing and Misdirected writes (displacement) [29][30].

Cloud storage of biometric data may present problems such as; Trust between the owner of the biometric data and the provider of this cloud storage system. There is no way that a customer can know that the provider of the cloud service can be trusted. Insider attacks from the owners of the cloud system having the ability to steal and sell the information belonging to their clients. Legal boundary of service considering that a provider of the cloud storage service may exist in a foreign country to the customer and as such the laws covering the two may differ. Provision of confidentiality may be a problem for the customer as the biometric data may be stored in a far off country where the customer has no control over. Provision of integrity in the biometric data is equally a problem for the customer due to the uncertainty that the biometric data received may have been tempered with or poisoned in transit [31].

C. Transportation of Biometric Data

1. Cloud Systems Transportation

Data that is being transported from point A to point B is referred to as data in-motion. Biometric data can be transported in many forms using; removable flash drives, portable hard drives, internal hard drives and optical mediums such as compact disks and others which permit logical access to data as cloud storage systems that are Internet access based. Data-in-motion may occur on Internet Based Systems e.g. downloading data from a cloud to computer or other storage systems [1].

2. Secondary Storage System Transportation

Data that is being transported from point A to point B is referred to as data at rest. Biometric data can be stored in many forms and on different storage media such as: removable flash drives, portable hard drives, internal hard drives and optical mediums such as compact disks and others which permit logical access to data as cloud storage systems that are Internet access based. Data at rest sometime may and may not require Internet Based Systems e.g. downloading data from a cloud to computer or other storage systems requires internet while downloading from a flash drive does not require internet [1].

D. Consequences of Loss

The various consequences of loss that may come to an organisation or individual that may use storage systems and transportation systems described to retain and maintain biometric data area include; Integrity losses, Exposure of private and personal data as well as Loss of confidentiality integrity and availability [2]

V. METHODOLOGY

This research employed both a survey questionnaire and a face to interview for data collection. The design of the research questions consisted of five sections including; section A. knowledge of biometrics, section B Organisational adoption of biometrics, Section C adoption of ISO 24745, Section D adoption of cloud computing and security, and Section E, Company's preferred storage and transportation medium. A total of 8 Public organizations each receiving 5 questionnaires and 5 street interviewees were targeted in the primary research.

The results were analyzed using Microsoft's Excel Program for statistical values [32]. Recommendation of biometric data Transportation and Storage based on ISO 24745 has been proposed [33].

VI. FINDINGS

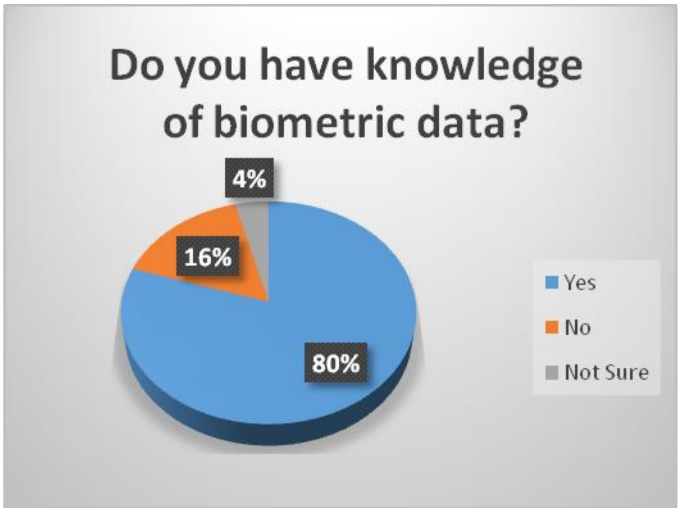


Fig. 1. Employees with knowledge of biometric

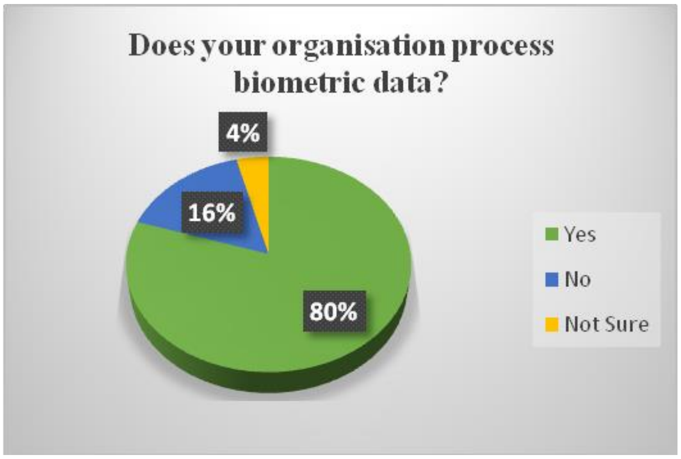


Fig. 2. Organisations that process biometric data

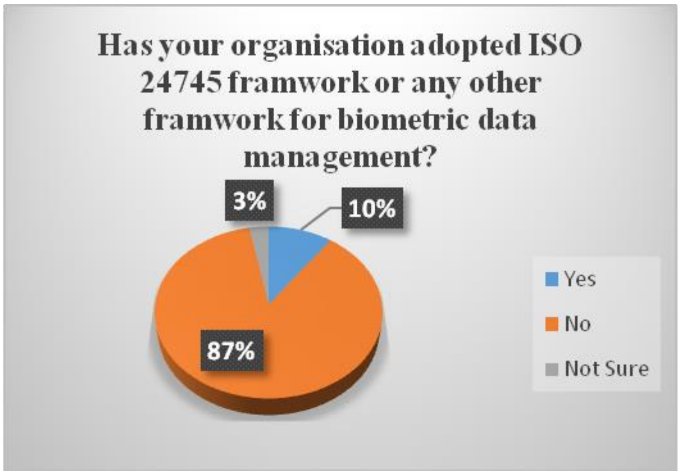


Fig. 3. Organisations that that claim to have adopted ISO 24745

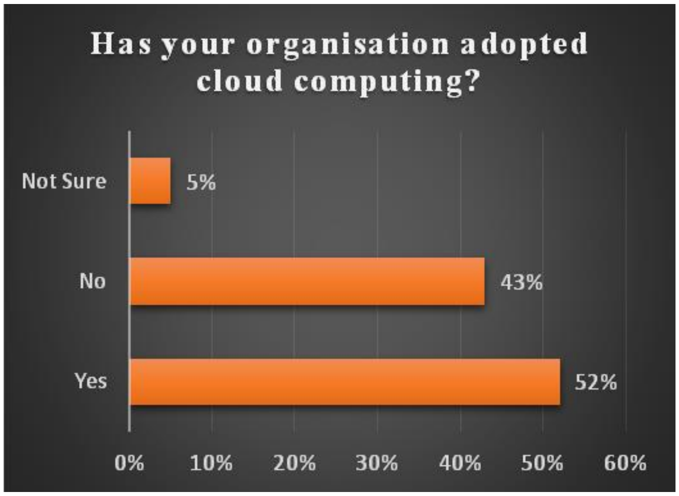


Fig. 4. Organisations which have adopted cloud computing

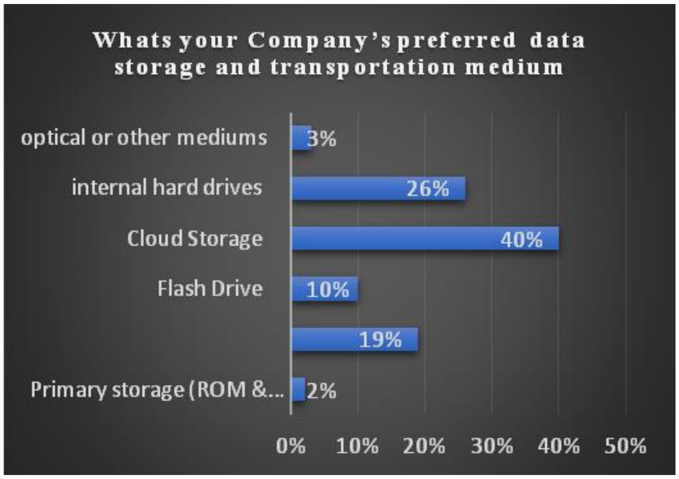


Fig. 5. Organisations prefered data storage and transportation medium

VII. DISCUSIONS

A. Solutions to Storage & Transportation Problems

Despite the very particular character of such information, there are virtually no legal provisions in the world that are specific to biometric data protection. Legal texts instead rely on provisions relating to personal data protection and privacy in the broad sense. But such legislation sometimes proves to be poorly adapted to biometric data. To effectively secure biometric data or any other organizational or digital data, it is primarily important to have a security mechanism that is guided by an information security policy. This policy should indicate the various regulations or in certain instances even measures and practices that must be adhered to by an organization in order to enforce security a mechanisms that provides information assurance to information [26].

B. Secondary Storage Systems

Secondary storage systems can be used to store and retain biometric data if the following steps are followed;

1. *Encryption:* A cipher text is a scrambled or hidden message to a third party. It is meant to be incomprehensible to all except those who legitimately possess the means to reproduce the original plaintext by way of a decryption key and an encryption/decryption algorithm. To generate a cipher text, an encryption algorithm with an encryption key are applied to what is known as plain text. Plain text is any information, data or message that is intelligible to a third party. The process of converting plain text to cipher text is called Encryption.
2. *Physical lock-down:* This is the physical restriction to storage media access from anyone and everyone except for authorised personnel. Locking the storage devices in physically secured libraries is an example. To access the media, strict authentication must be made available either electronically or by some of physical authentication such as presenting security access pass.
3. Logged access to the biometric data by use of RFID technology

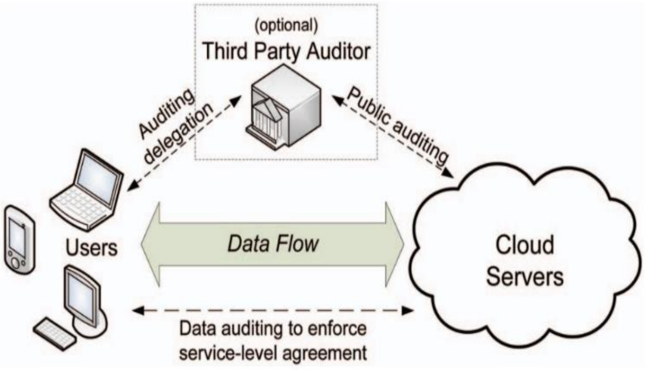
C. Cloud Storage Systems

Cloud storage systems can be used to store and retain biometric data if the following steps are followed:

a) Encryption - It is recommended that pre-encrypted biometric data is stored or kept in a cloud storage system. This has the potential to hide biometric data in plain sight. Should an attacker or hacker succeed to intrude into the cloud storage system and access the biometric data, the retrieved data would be unintelligible as the data would be scrambled. A suitable current public key cryptographic system is advised such as Rivest Shamir Adleman (RSA) or SHA.

b) End-to-end Encryption Approach

An end-to-end argument may be understood as "*The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)*" [34][35]. Because an endpoint cannot trust the service of a network, then a need to supplement the network's service exist [1].



c) Employing Time-to-Destruct

Cloud systems may use the time to destruct technology to transport biometric data from one end of the system to another. This data must however be tied to a time frame. This time frame entails that, should the time expire while the data has not been delivered, then this data would be destructed (Deleted). Care must be taken to understand the parameters of operation of cloud transportation and know the tolerance time limits available. These tolerance time limits must be incorporated into the cloud biometric data transportation. This advantage of the time to destruct is to ensure that biometric data in motion does not remain resident on a network or receiver's device longer than it is needed [35].

d) Employing Tunneling Systems

In networking communications, tunneling is a network communications process that shelters the contents of a particular protocol packets. This is achieved by a process called encapsulation. The protocol packets are encapsulated in packets of another or different protocol. The process of encapsulation is given an illusion that a communications tunnel is created over another, this is usually called to as an untrusted network. This tunnel is referred to as a virtual Private Network (VPN). At either end of the communication route, a de-encapsulation entity exists that exhumes the encapsulated traffic or data from the tunnel and makes it available to the rest of the communication process [41]. Four common protocols are used to implement VPNs; these being: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding, Cisco developed (L2F), Layer 2 Tunneling Protocol (L2TP) and internet Protocol Security (IPSec). VPNs can be created to operate on any type of network and they can be used to bypass firewalls, gateways, proxies, or other traffic control devices. This tunneling has an ability to stop traffic control devices from blocking the on-going communication process because the devices cannot determine what the data packets contain. Biometric data from cloud systems can therefore be transported from one end to the other after a tunneling mechanism has been employed on that network [35].

e) Employing an audit service architecture.

Figure 9. Cloud Storage Audit Architecture [42]

A cloud service architecture will have three points of connection i.e. users, third-party auditor (TPA) and Cloud Servers. The TPA is brought in the cloud systems is to ensure that transactions of data to and fro the cloud servers pass through an auditing mechanism so as to ensure the challenges discussed in cloud storage systems are addressed.

f) Email Systems

The +security concerns that can be studied in email systems include; the content of email is in plain and clear text format. This therefore implies that during transmission, data from email is not encrypted. This further implies that data can be easily revealed if an attacker gets access to the mailbox. Gaining access implies that the attacker is well vest in network attack methods. This issue generates the first problem in email systems called the problem of email secrecy.

Email is stored and transmitted in plain text. This implies that a person who can access email has the potential to change or modify the contents without the receiver or sender ever knowing that the content has been modified or changed. This creates a second issue in email security called the problem of integrity.

Because basic Email is NOT secure, employing a security mechanism in email is cardinal. Email security must therefore attempt to provide the following; Provide for nonrepudiation, restrict access to messages to only their intended recipients, maintain the integrity of messages, authenticate and verify the source of messages, verify the delivery of messages and classify sensitive content within or attached to messages.

Technology exists that can be incorporated within email to make emails secure. Imposition of security on email is possible, but the efforts should be in tune with the value and confidentiality of the messages being exchanged. Several protocols, services, and solutions can be used to add security to email without requiring a complete overhaul of the entire Internet based Simple Mail Transfer Protocol (SMTP) infrastructure. These include Secure Multipurpose Internet Mail Extensions (S/MIME), MIME Object Security Services (MOSS), Privacy Enhanced Mail (PEM) and Pretty Good Privacy (PGP) [2].

S/MIME offers authentication and privacy to email through public key encryption and digital signatures. Authentication is provided through X.509 digital certificates. Privacy is provided through the use of Public Key Cryptography Standard (PKCS) encryption. Two types of messages can be formed using S/MIME: signed messages and secured enveloped messages. A signed message provides integrity and sender authentication. An enveloped message provides integrity, sender authentication, and confidentiality [1][31].

MOSS can provide authenticity, confidentiality, integrity, and non -repudiation for email messages. It employs Message Digest 2 (MD2) and Message Digest 2 (MD5) algorithms; Rivest, Shamir, and Adelman (RSA) public key; and Data Encryption Standard (DES) to provide authentication and encryption services.

PEM is an email encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation. It uses RSA, DES, and X.509 [33][34].

PGP is a public-private key system that uses the international data encryption algorithm (IDEA) algorithm to encrypt files and email messages. PGP is not a standard but rather an independently developed product that has wide Internet support.

By using these and other security mechanisms for email and communication transmissions, one can reduce or eliminate many of the security vulnerabilities of email [2][36].

Digital signatures can help eliminate impersonation. The encryption of messages reduces eavesdropping. And the use of email filters keep spamming and mail-bombing to a minimum. Blocking attachments at the email gateway system on a network can ease the threats from malicious attachments [22].

VIII. CONCLUSION

Based on the above discussion, we believe that the "design space" for continuous authentication (or, equivalently, de-authentication) techniques needs to be explored further. From the outset, we acknowledge that a perfect continuous authentication method is unlikely to materialize; in fact, one might not even exist. In other words, since each previous method has a distinct set of advantages and limitations/flaws, the same will certainly hold for our current efforts.

Zambian as a nation lack a biometric storage framework that would guide public organisations collectively on how to store and transport biometric data. All the public Organisations that collect, transport and store biometric data execute such task based on their "know how" knowledge. Since biometric data cannot be transferred because it stays consistent through-out its life time, and the fact that this data can be used to identify an individual. The absence of a framework makes the data subjects vulnerable to data theft, Identity theft, or data misuse. Therefore, biometric storage framework must considered by the ICT authority be in place. This paper limits its discussion to the proposed recommendations on how to secure biometric data whilst at rest and or in motion so as to deter attackers in public organisations.

IX. REFERENCES

[1] Jackson Phiri, Tie-Jun Zhao, Johnson I. Agbinya, "Biometrics device metrics and pseudo metrics in a multifactor authentication with artificial intelligence", Broadband and Biomedical Communications (IB2Com) 2011 6th International Conference on, pp. 157-162, 2011.

[2] C. Kabuya, J. Phiri, T. Zhao, Y. Zhang, "Metric Based Technique in Multi-factor Authentication System with Artificial Intelligence Technologies" in Future Wireless Networks and Information Systems, Springer Berlin Heidelberg, vol. 143, pp. 89-97, 2012.

[3] N. Udoh, "Zambia: Dec Nabs 2 MTN Employees for K1.3 Million Theft," All Africa, 17 September 2014. [Online]. Available: http://allafrica.com/stories/201409170984.html. [Accessed 13 April 2018].

[4] Microsoft, 2011. Threats and Countermeasures. [Online] Available at: www.https//technet.microsoft.com/en-us/library/hh125922(v=ws.10).aspx [Accessed 30th March 2018].

[5] Walters, P., 2012. The Risks of Using Portable Devices. s.l., Carnegie Mellon University.

[6] LLC, A. D. G., 2017. ACE Data Group LLC. [Online] Available at: www.datarecovery.net/newsletters/what-kills-flash-drive.aspx [Accessed 2 December 2017].

[7] Yu Cai, E. F. H. O. M. K. M., 2012. Error Patterns in MLC NAND Flash Memory: Measurement, Characterization, and Analysis. LSI Corporation, 1110 American Parkway NE, Allentown, PA, 8(6), pp. 1-6.

[8] M. B. Salem, S. Hershkop, and S. J. Stolfo, A Survey of Insider Attack Detection Research. Springer, 2008,

[9] S. M. Bellovin, The Insider Attack Problem: Nature and Scope. Springer, 2008, ch. In

[10] http://www.societalsecurity.net/sites/default/files/d6.2_societal_ethics_and_biometric_technologies_0.pdf

[11] A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, The 'Big' Picture' of IT Sabotage Across U.S. Critical Infrastructures. Springer, 2008,

[12] Feng. J., and A.K. Jain. 2009. FM model based fi ngerprint reconstruction from minutiae template. Proceedings of ICB 2009 , Alghero , 544–553.

[13] [9] Patnaik, S., 2016. 2nd International Conference on Intelligent Computing, Communication & Convergence. Odisha, India, Elsevier.

[14] Anil K. Jain and Ajay Kumar Biometric Recognition: An Overview - Michigan State University, East Lansing , MI 48824-1226 , USA

[15] https://www.iso.org/standard/53227.html

[16] https://www.veridiumid.com/blog/solving-biometric-vulnerability-liveness-measures

[17] Nec, 2017. Nec Cloud Storage. [Online] Available at: www.nec.com [Accessed 08 January 2018].

[18] Oriyano, S.-P., 2016. CEH™ Certified Ethical Hacker. Indianapolis,USA: John Wiley & Sons.

[19] Jithin, 2017. What is Session Hijacking and how to prevent it?. [Online] Available at: https://www.interserver.net/tips/kb/session-hijacking-prevent/

[20] Bellovin, S. M., n.d. A Look Back at "Security Problems in the TCP/IP Protocol Suite". s.l.:AT&T Labs—Research.

[21] Kaufman, L., 2009. Data security in the world of cloud computing. IEEE Security & Privacy, 7(1540-7993), pp. 61-64.

[22] Vacca, J. R., 2009. Computer and information Security Handbook. Amsterdam: MK.

[23] Ms.Priyanka S. Kamthe, M. P. N., 2015. Email Security: The Challenges of Network Security. International Journal on Recent and Innovation Trends in Computing and Communication, pp. 1-5.

[24] MUSAMBO, Lubasi Kakwete; CHINYEMBA, Melissa K.; PHIRI, Jackson. Identifying Botnets Intrusion & Prevention – A Review. Zambia ICT Journal, [S.l.], v. 1, n. 1, p. 63-68, dec. 2017. Available at: http://ictjournal.icict.org.zm/index.php/zictjournal/article/view/28

[25] Lyoko Gift, Phiri Jackson, "Secure automation of the Zambia Police Service business processes", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 12, pp. 12404 - 12411, December 2015. DOI:10.15680/IJIRSET.2015.0412141, (Accessed on 20 June 2018) https://www.ijirset.com/upload/2015/december/141_Secure_F.pdf

[26] Pang, T., 2017. End-to-End Data Protection. Infortrend.

[27] Haines, A., 2017. Fix the Parameter is Incorrect on External Hard Drive in Windows 10/8/7.

[28] Martin, K., 2012. Everyday Cryptography: Fundamental Principles & Applications. New York: Oxford University Press.

[29] Sehgal, S., 2016. Road Towards Cloud Computing - What are the Issues? Part 1. [Online] Available at: www.simplilearn.com/cloud-computing-issues-part-i-article [Accessed 30 January 2018].

[30] Microsoft, "Get a better picture of your data," Microsoft, 13 April 2018. [Online]. Available: https://products.office.com/en-us/excel. [Accessed 13 April 18].

[31] ISO, "Information technology -- Security techniques -- Biometric information protection," ISO/IEC, June 2011 . [Online]. Available: https://www.iso.org/standard/52946.html. [Accessed 18 April 2018].

[32] Clark, D. D. & Blumenthal, M. S., 2000. Rethinking the design of the Internet: The end to end arguments vs. the brave new world. TPRC, December.pp. 1-30.

[33] NAMIT, 2018. Activate the self-destruct in the secret message chats of telegram. [Online] Available at: www.technocrates.org/activate-the-self-destruct-in-the-secret-message-chats-of-telegram/10

[34] Stewart, J. M., Tittel, E. & Chapple, M., 2008. Certified Information System Security Professional. Canada: Wiley.

[35] Cong Wang, Q. W. K. R. C. W. L., 2012. Toward Secure and Dependable Storage Services in Cloud Computing. IEEE TRANSACTIONS ON SERVICES COMPUTING, 5(2), pp. 1-13.

[36] Raja, S. H., 2012. Securing Risks of Electronic Mail Based on the Type of Organization. International Journal ofInnovation, Management and Technology, 3(3), pp. 1- 4.