Doctoral Research Paper

Cybersecurity Risk Management in Identity Systems Using Biometric-Based Multimodal Authentication

¹Talabi, Adedoyin Abiodun

²Longe Olumide Babatope

³Muhammad Aminu Ahmad

⁴Olusanya Kunle

¹PhD Candidate

African Centre of Excellence

on Technology Enhanced

Learning (ACETEL)

Nat. Open University of Nigeria

Abuja, Nigeria

²Faculty of Computational

Sciences & Informatics

Academic City University

College, Accra, Ghana

³Dept of Computer Science

Kaduna State University,

Kaduna, Nigeria

⁴Industry Expert

ISACA, Ibadan, Nigeria

Corresponding E-mail

doyin.talabi@gmail.com

ABSTRACT

This increasing inter-connectivity of systems and dependence on computer and internet-based networks has made Cybersecurity related risks management issues major considerations in designing, developing and managing identity systems. Thus, this paper investigates Cybersecurity and related risk management challenges in Identity Management Systems by undertaking a comparative analysis of different biometric traits. The analysis proved that biometric-based multimodal systems are more secure than uni-modal systems with high accuracy rates. Also, it produced minimal false acceptance and false rejection rates. The biometric-based multi-modal authentication systems will assist organizations to restrict access to authorized users and protect digital assets by ensuring confidentiality, integrity and availability.

Keywords: Cybersecurity, Risk, Identity, Biometrics, Multimodal, Behavioural, Fusion

Proceedings Reference Format

Talabi, A.A., Longe, O.B., Muhammad, A.A. Olusanya, K. (2021): Cybersecurity Risk Management in Identity Systems using Biometric-based Multimodal Authentication. Proceedings of the 28th iSTEAMS Intertertiary Multidisciplinary Conference. American Int University West Africa, The Gambia. October, 2021. Pp 61-88 www.isteams.net/gambia2021.

DOI - [https://doi.org/ 10.22624/AIMS/iSTEAMS-2021/V28N2P5](https://doi.org/10.22624/AIMS/iSTEAMS-2021/V28N2P5)

1. INTRODUCTION

The Internet has grown from its initial use for communication and browsing to diverse uses and the dependence on it is growing. Our society has become interconnected through the Internet and it has become an integral part of our daily lives. Many organizations, businesses and government agencies alike utilize internet-based technologies to create and manage access to corporate databases and networks. This creates exposure to cyber-attacks from internal and external vulnerabilities and threats. This result in Cybersecurity risks that must be managed appropriately. This exponential growth in the use of the Internet as a superhighway for data collection and storage for major applications globally has made cyber-attacks common resulting in unauthorized access, hacking of systems, data corruption, and identity-theft with dire consequences including disruption of operations, loss of data, and loss of reputation, loss of revenue and court cases. All the above can happen once an unauthorized person gets access to the database.

2. RELATED WORKS/LITERATURE REVIEW

"Cybersecurity is the state or process of protecting and recovering networks, devices, and programs from any type of cyber-attack". (Ibikunle, 2013)¹

Multimodal authentication involves the use of multiple biometric traits for identifying individuals in identity systems. This may include the use of fingerprint, face, palm or the iris. Multimodal systems provide a higher level of authentication than unimodal systems. The minutiae matching and edge extraction technique is used and the resulting performance is the minimization of False Acceptance Rate (FAR) and False Rejection Rate (FRR). (**Parkavi et al, 2017**)²

Multi-instance fingerprint authentication systems do not have problems encountered in unimodal systems. All features in the fingerprints are extracted and stored in a database using the crossing number technique. This technique uses the ending of the ridges and its bifurcation form a single image of a pixel using a 3 by 3 window. Two randomly requested fingerprints from the user are extracted and compared to the database to determine a matching score. Each matching score is fused using a weighted score rule. The research concluded with an accuracy level of 98.67% and an average run time of 3.82 seconds for each verification (**Ilugbusi et al, 2017**)³

¹ Ibikunle, Francis. (2013). Approach to cybersecurity issues in Nigeria: Challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education

² R. Parkavi, K. R. Chandeesh Babu and J. A. Kumar, "Multimodal Biometrics for user authentication," (2017) 11th International Conference on Intelligent Systems and Control (ISCO), 2017, pp. 501-505, doi: 10.1109/ISCO.2017.7856044

³ Ilugbusi, Abiodun & Adetunmbi, Adebayo. (2017). Development of a multi-intance fingerprint based authentication system. International Conference on Computing Networking and Informatics (ICCNI) 1-9. 10.1109/ICCNI.2017.8123780

Biometrics-based systems are used in different security systems. There are four modules in a typical biometric system; feature **extraction, sensor, decision making and matching modules**. Multimodal biometric systems result in secure and highly accurate biometric identification systems as compared to unimodal biometric-based system because of non-universality. (Suneet et al, 2017)⁴. Biometric fusion involves the use of multiple types of biometric data or different ways of processing data to improve performance. Biometric evidence in a multimodal system can be fused at several different levels. The fusion process is divided into two stages; **pre-matching fusion**, where fusion occurs before matching of biometrics and **post-matching fusion**, where fusion is done after the fusion of biometrics. This post matching fusion stage includes the **match score level fusion, rank level fusion and decision level fusion**. The pre-matching fusion comprises **sensor level fusion and feature level fusion**.

The paper proposed the development of a fusion of the face and fingerprint at the match score level fusion using Scale Invariant Feature Transform (SIFT) algorithm and the hamming distance measurement technique. The **match score level** fusion has been studied extensively in research literature and has been found to produce acceptable performance rates, though normalization is sometimes required for the scores data from different unimodal systems. The paper established that multimodal systems have 92.5% accuracy and a False Rejection Rate (FRR) of 7.5% and False Acceptance Rate (FAR) of 3.75%, whereas when only face is used, the experiment gives 90% accuracy and when only fingerprints are used, it gives 82.5% accuracy (Mwaura, G. 2017)⁵

Various security technologies including barcode, RFID, Magnetic Card have been used and biometric-based cards are common because of uniqueness, but fingerprint-based biometric systems are widely recommended and used in ATMs, attendance and point-of-sale (POS) applications. Fingerprint-based security systems are sometimes augmented with the use of SMS based one-time password (OTP) messages, mobile-based scanning systems using Wireless Wifi to connect to the Internet. (Zeehan,J et al, 2017)⁶. Fingerprint patterns are the most commonly used physiological information to confirm the identities of persons in fingerprint recognition systems. Challenges of such systems include mismatching due to physical distortion caused by injuries and cuts in fingers, displacement and rotation during scanning in the sensor, unauthorized access due to finger plasticity or clay printing and variances between different impressions of the same finger due to other skin conditions or noise in the sensor.

⁴ Garg, Suneet & gupta, Renu (2017). Multimodal Authentication System: An Overview. International Journal of Control Theory and Applications

⁵ Mwaura, Grace. (2017). Multimodal Biometric System:-Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level. International Journal of Scientific & Technology Research. 6. 41

⁶ Shameem, Z.A., Mohite, J.N., & Sharmin, S (2017). **A Review on Advance Biometric Fingerprint Based Security Systems**. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887. Volume 5 Issue X1, November 2017-

These issues provide a wide scope for research to improve the performance of fingerprint-based systems, doing any of the following suggested procedures.

- (i) *Enhancing the process of capturing input images accurately without losing pertinent information with better image processing techniques.*
- (ii) Using a better algorithm to reduce mismatching as a result of physical distortion or displacement.
- (iii) *Using a combination of fingerprint algorithms to get higher accuracy levels in recognition rates and matching techniques. (Kumar, M, 2018)⁷*

Various factors including scars, skin ailments can affect the quality of fingerprints captured for identification and verification in fingerprint recognition systems. Fingerprint Recognition systems involve five different activities – (i) Image Acquisition, (ii) Image Pre-Processing, (iii) Feature Extraction (iv) Matching and (v) Image Identification. Modern techniques like the use of fuzzy and neural networks give more accurate results in each of the fingerprint processing stages (Parvarthy, J et al, 2018)⁸

Digital rights management (DRM) systems have use biometric technology to provide access only to authorized users as content owners are losing billions of dollars annually through illegal copying and sharing of digital content. This is because the most important part of a DRM system is perhaps the authentication of individuals to determine whether authorized to access available content Cryptographic systems use possession of decryption key to establish user authenticity, on the assumption that cryptographic keys are usually about 128 bits and not easily remembered. However, users tend to store their passwords in open folders and many users use same passwords multiple times.

These problems led to the use of physical and behavioural biometrics like fingerprint, face and signatures because they are unique to individuals and not easily forged, stolen or forgotten. Biometric systems provide a good alternative to traditional methods of authentication and have been found to be more reliable. Biometric systems usually consist of the following components; a scanning device for reading the feature, a software to convert the data collected into digital format and an electronic database to store the data securely. For security purposes, the software identifies particular areas of the data and records them as unique or match points which are then processed using an agreed algorithm into a hash value that can be used for comparing biometric data already in the database to ensure that there are no duplicate entries.

⁷ Kumar, Munish. (2018). Fingerprint Recognition System: Issues and Challenges. International Journal for Research in Applied Science and Engineering Technology. 6. 556-561. 10.22214/ijraset.2018.2080

⁸ Parvathy. J, Dr. Poornima G. Patil. (2018). A Survey on Fingerprint Identification Techniques. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887. Volume 6 Issue I, January 2018-

Fig. 1 – Generic Biometric system:

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012a)

A biometric system usually works in three modes.

- (i) **Enrollment Mode** - In this mode, a sample of a biometric trait is captured, processed and stored in the database. The sample collected is used to create a template. Usually, this would be a string of alphanumeric characters

Fig. 2 – Biometric system Enrollment Mode:

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012b)

- (ii) **Identification Mode** – In this mode, the system identified a person by searching through the entire database using the biometric trait. Some refer to this as “one-many” matching

Fig. 3 – Biometric system Identification Mode

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012c)

- (iii) **Verification Mode** – In this mode, the system authenticates a person based on previously stored pattern. This is faster and referred to sometimes as “one-to-one” matching

Fig. 4 – Biometric system Verification Mode

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012d)

Biometric systems use False Acceptance Rate (FAR), False Rejection Rate (FRR), and Failure to Enroll (FTE) and Equal Error Rate (EER) to measure performance statistically. The probability of classifying a wrong person as the owner of a biometric trait is referred to as false acceptance and its probability called, False Acceptance Rate (FAR). The probability of rejecting the true owner of a biometric trait is called False Rejection Rate (FRR). The probability that a user will not be able to enroll successfully is referred to Failure to enroll (FTE).

When the results of false acceptance rates (FAR) and false rejection rates (FFR) are plotted on a graph, the point at which FAR and FRR are equal is called the Equal Error Rate (EER) and the lower it is, the higher the accuracy of the biometric system. The paper used the fingerprint, iris, voice and face and concluded that while iris is the most secure, but expensive to deploy, voice and face were more popular amongst user, the fingerprint offered the optimal solution when considering all issues including cost, easy implementation, noninvasiveness and acceptable FAR and FRR. (Manivannan, S, et al, 2015)⁹. User authentication techniques are usually categorized into token based and knowledge-based. Tokens include smart cards and knowledge-based include passwords. Biometrics has an advantage over traditional methods as natural traits cannot be misplaced or forgotten and difficult to spoof. Biometric solutions have become popular due to higher accuracy and used for human security applications that require identification and authentication.

Biometric applications include forensic investigation, surveillance systems, border control, access control, paternity determination and electronic medical records management. Its use in other fields is also becoming widespread. *“Biometric technologies can be defined as automated methods of verifying and/or recognizing the identity of a living individual based on physiological traits or behavioural traits”*. Physiological traits include fingerprint, hand, finger geometry, face, iris, pam print, odour, voice and DNA. Behavioural traits include gait and signature. Some researchers are considering using human electrocardiogram (ECG) signals. Fig 1 below shows different biometric traits by category and origin.

⁹ Manivannan, S. & Padma, E. (2011). Comparative and Analysis of Biometric Systems. International Journal on Computer Science and Engineering. 3. 2156-2162.

Fig 5 – Biometric Traits. (Source:
<https://www.intechopen.com/media/chapter/60675/media/F2.png>)

Multimodal systems provide a lot of benefits. These include addressing the issue of noisy data and non-universality and it is very difficult for an impostor to spoof all the multiple biometric traits of an enrolled person. Multimodal systems also help when a single trait does not provide sufficient evidence.

Biometric systems must meet certain criteria to be considered reliable.

- i. **Universality** – All individuals should have the biometric trait, measured by the failure to enroll rate.
- ii. **Distinctiveness** – Two individuals should have uniquely different characteristic, measured by the False Match Rate(FMR)
- iii. **Permanence** – The biometric characteristic should be stale over a period of time, measured by False Non Match Rate(FNMR)
- iv. **Collectability** – Biometric characteristic can be measured quantitatively and amenable to capture by electronic sensors. Measured by the system's throughput rate
- v. **Performance** – This refers to the biometric trait's recognition accuracy and resources required to implement.
- vi. **Acceptability** – Acceptability by the user public and level of objection to collection. Measured by doing a poll survey of users
- vii. **Resistance to Circumvention** – Level of resistance to fraudulent attempts

No single biometric trait can be declared as the best in all cases of application, technology and administration. There are limitations in using single modal biometric. Using iris has some limitations of camera distance, lenses and reflections. Face changes over time and twins have similar faces. Fingerprints may be defaced by cuts and injuries or other permanent injuries. DNA takes several hours to obtain and hand geometry may not be distinctive enough. Signature also changes with time. The conclusion is that using multiple biometrics will reduce the effects of all these conditions on accuracy as single modal system may not achieve desired error rates or performance levels. Problems of single modal systems include noise due to accumulation of dirt on the sensor for example, non-universality, spoof attacks, can be easily circumvented and does not cover large populations

Multimodal systems have advantages over unimodal systems as it combines biometric traits for high performance. Some of its benefits include higher recognition accuracy and data privacy.

- i. **Recognition Accuracy** – Multimodal systems have higher reliability due to the fact that biometric traits are independent and is quite difficult to forge all of them. Accuracy levels
- ii. **Privacy** – Multimodal systems provide privacy as it is difficult to spoof multiple biometric traits or the biometric system
- iii. **Data Enrollment** – Multimodal systems address the problem of non -universality; when a particular biometric data is unavailable or poor in quality, another biometric data can be used instead.

Multimodal systems can be synchronous, where two or more biometric traits are combined and used in a single authorization process or asynchronous when two biometric traits are used one after the other. Multimodal system can also operate in three modes. In serial or cascade mode where each modality is examined individually to reduce duration for recognition and the number of possible identities. In parallel mode where data from multiple modalities are captured and used concurrently to perform recognition and the results combined. In hierarchical mode where biometric traits are combined in a tree structure, used particularly when a large number of data is expected

Different integration combinations are possible in multi-biometric systems

- i. **Multi-sensor systems** – Here, multiple sensors(e.g. capacitive and optical sensors) are used to collect the same biometric data and combined using sensor level fusion technique
- ii. **Multi-modal systems** – Here, more than one biometric like face and voice are used. This may be more expensive as a different sensor is used for each biometric trait. However, the improvement in accuracy is material.
- iii. **Multi-instance systems** – Here, the same biometric trait is captured multiple times e.g. one or more fingers of the same individual can be combined. This may be cost efficient as it requires only one sensor
- iv. **Multi-sample systems** – Multiple views of the same biometric trait can be used e.g. multiple sample of fingers or voice. This may improve accuracy but will require multiple sensors , may be expensive and takes longer time

- v. **Multi-Algorithm system** – Here, a combination of different extraction techniques and algorithms are used. This may be cheaper as only one sensor is involved but may be complex depending on the algorithm selected.
- vi. **Hybrid Systems** – Involve the combination of any of the above methods. For example, combining multi-modal with multi-algorithm or multi-instance with multi-sensor

Fig 6 – Multi-Biometric Systems.

Source: https://www.researchgate.net/profile/Ramadan-Gad/publication/279490555/figure/fig1/AS:294413646483487@1447205091884/figure-fig1_Q320.jpg

Multimodal systems have limitations which include high cost of implementation due to additional hardware requirements and fingerprint scratches that create noise in the biometrics data and is susceptible to Trojan horse attacks, substitution attacks and transmission attack in a network implementation. Multimodal fusion combine unique and different biometric traits for higher accuracy levels. The most important part is to determine what information should be fused and the method of fusion. There are five fusion schemes; sensor level, feature level, match score, rank and decision level. These can be classified into three; prior-to-matching, after-matching and hybrid, which is a combination of any of prior and after-matching fusion level schemes.

Fig 7 – Fusion levels.

Source: [https://encrypted-](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSgGn4uLZQbyttPmQfbGbjXE19JgdiuFmfyUg&usqp=C)

[tbn0.gstatic.com/images?q=tbn:ANd9GcSgGn4uLZQbyttPmQfbGbjXE19JgdiuFmfyUg&usqp=C](https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSgGn4uLZQbyttPmQfbGbjXE19JgdiuFmfyUg&usqp=C)
AU

Fig 8 – Multi-Biometric Fusion Techniques.

Source - <https://www.bayometric.com/wp-content/uploads/2017/10/different-fusion-levels.jpg>

Fig 9 – Different Integration Combinations in Biometrics.

Source (<https://encrypted-tbn0.gstatic.com/images>)

Prior-to matching fusion is in two categories;

- i. **Sensor level fusion** – Merging of raw biometric data obtained from multiple sources but from a single sensor

Fig. 10 – Sensor level Fusion

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012e)

- ii. **Feature level fusion** - Biometric features extracted from different modalities fused using particular algorithm to get a composite set and used as input into the match module after normalization, transformation and reduction techniques have been applied e.g. sequential forward or backward selection)

Fig. 11 – Sensor level Fusion

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012f)

After-matching fusion is also classified into three:

- i. **Matching score level fusion** - Feature of vectors extracted individually for each modality are compared with data already in the databases to get matching scores that are used create composite matching score. This is also called a confidence or measurement level fusion. The matching scores have to be normalized before use because they are based on different scaling methods from different modalities.

Fig. 12 – Score level Fusion

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012g)

- ii. **Rank level fusion** – Here, each enrolled trait is associated with a rank and the higher the rank, the better the match. The matching unimodal outputs are consolidated and a new rank to help in making final decision is estimated.

Fig. 13 – Rank level Fusion:

Source: https://media.springernature.com/original/springer-static/image/prt%3A978-0-387-73003-5%2F6/MediaObjects/978-0-387-73003-5_6_Part_Fig1-159_HTML.jpg

- iii. **Decision level fusion** – This level, also called the abstract level fusion is used when there is only access to individual decisions and this is obtained from the different biometric modalities using different techniques like behaviour, and majority voting.

Fig. 14 – Decision level Fusion

Source: Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012h)

- iv. **Hybrid level fusion** – This involves using different fusion at different levels of the system to check whether the system can become faster and with reduced error rates and some researchers got improved performance

There are many design issues in multimodal systems and they include choosing the correct biometric modalities and number of traits, ensuring the best samples are used, applying appropriate fusion level, methodology, and scenario. Also there is need to consider cost against performance, accuracy against reliability and the identification and verification modes of the application and difficulties in expert features selection. It is important to sort out design issues first in order to get the benefits of multimodal recognition systems. Therefore, a decision as to whether to combine multiple biometric data or multiple samples of the same trait, considering data privacy issues and balancing accuracy with extent of coverage must be taken so that an effective design methodology and system architecture can be in place.

The authors suggest different research directions from this paper that can improve the security and performance of multi-biometric systems. These suggestions include using

- i. **Multi-data Database/Real data set** – The use of homologous database, which contains different traits of the same person or use of heterogeneous database, which involves use of the same trait from two different databases. However, very few multimodal databases are available publicly. Examples of heterogeneous databases include BANCA and XM2VTS which have face and voice biometrics; BIOMET which includes signature, face, voice and fingerprint. SDUMLAHMT homologous database includes iris images, finger print images and face images from 7 angles
- ii. **Soft Multi-biometrics** - Soft biometrics traits include height, weight, eye, skin or hair colour. This method has challenges of easy extraction with inconveniencing the users and combining this with the natural biometric traits like fingerprints. It is claimed that soft biometrics can be implemented using SQL server programming language tool that has capability to integrate pattern recognition and image processing with database management
- iii. **Multi-algorithm fusion methods** – The suggestion here is to use linear programming method or adopt the K-means cluster approach. It might be of interest to experiment the performance of these new techniques with the serial fusion of multiple classifiers like *F-SIFT*, *iGRNM*, *PSO*, and *HMM* algorithms
- iv. **Identification of Identical Twins** – Multimodal systems can increase the distinguishability between identical twins as they cannot have the same face, fingerprint and iris together. As such, face, iris and fingerprint can be fused to identify them.
- v. **Indexing Search** – The search space and time of multimodal systems can be improved significantly by adopting indexing combined with cloud computing. Different approaches using multidimensional trees are being proposed.
- vi. **Embedded hybrid recognition system** – There is a suggestion to combine physiological and behavioural traits, offline and online signatures and at the same time applying multi-fusion with multi classifiers at different fusion levels. The complexity that may arise may be resolved using parallelism in feature extraction and identification phases or hardware like ARDUINO, FPGA or similar parallel processing elements, since the systems will be used in public, real time internet-based authentication environment.

The research paper provided a panorama of integration strategies and discussed different fusion levels, their advantages and disadvantages and highlighted design issues and considerations. In conclusion, it suggested several areas of improvement in future research and multi-biometric applications. (Ramadan Gad, et al, 2015)¹⁰. The need for reliable identification and authentication systems have become critical issues in our daily lives and new approaches are required that would ensure that authorized users are allowed access with higher accuracy and intruders denied access to secure facilities, networks and e-commerce sites. Biometrics provide automatic recognition based on behavioural and physiological characteristics. Biometrics provide a reliable way to authenticate the presence of a user. Single-biometric systems sometimes fail due to insufficient information and that's where using multiple modalities and algorithms can achieve higher performance.

Multi-biometric systems can be classified in five different ways; *multi-sensor systems, which uses multiple sensors, multi-algorithmic systems which uses different extraction techniques and algorithms, multi-instance systems, where multiple samples of the same biometric trait is used, multi-sample systems where multiple samples are collected to account for variations and multi-modal systems, where multiple biometric data is collected.* Research has shown that multi-modal systems are better, difficult to spoof and achieved a higher level of accuracy. Multi-modal systems use four different fusion methods; sensor level fusion, where raw biometric data is combined, feature level fusion, where different feature vectors are combined, matching score level, where matching scores for different biometric data are combined and decision level fusion, where decisions from individual systems are combined. This paper considered the use of the palm and face as the biometrics, the matching score level fusion as the technique and PCA, FLD and ICA algorithms in different combinations.

The results from the research indicated that multimodal systems yielded far improved results over the multi-algorithmic approach, which just gave incremental improvement results. Other research proved the same that multi-algorithmic systems builds on supplementary information and perms lower than multimodal systems. Multimodal systems use multiple biometric data from multiple sources while multi-algorithmic systems rely on supplementary information. The research conformed that complimentary information provides better results that supplementary information, using the best combination of algorithms rather than the number of algorithms is better, the modality used will determine the performance level of the algorithm and lastly, multimodal systems always yield better results than different versions of multi-algorithmic systems that utilize the same modality or algorithm. (Imran, M et al, 2010)¹¹

¹⁰ Ramadan Gad, Nawal El-Fishawy, AYMAN EL-SAYED and M. Zorkany, "Multi-Biometric Systems: A State of the Art Survey and Research Directions" International Journal of Advanced Computer Science and Applications (IJACSA), 6(6), (2015). <http://dx.doi.org/10.14569/IJACSA.2015.060618>

¹¹ Mohammad Imrana, Ashok Raob , G Hemantha Kumar (2010). Multibiometric Systems: A Comparative Study of Multi-algorithmic and Multimodal Approaches. Retrieved from <http://creativecommons.org/licenses/by-nc-nd/3.0/>

Manju R, et al (2012) discussed an effective fusion scheme that combines information from multiple domain experts that show that multiple biometric systems improve accuracy levels as well as providing a wider coverage of the population, reducing failure-to-enroll- rates and preventing spoof attacks. Three distinct unimodal biometric traits ; the iris, fingerprint and face traits combined with the Principal Component Analysis (PCA) and Fisher's linear discriminant(FLD) methods for matching individual traits in combination at the rank level of fusion. The individual traits are combined using the highest rank approach. The PCA and FLD approaches produce precise results for unimodal systems, which is then consolidated at the rank-level fusion to improve recognition accuracy levels. Factors affecting the accuracy of biometric data include noisy fingers due to cuts and residual deposits, for the face, a hazy picture may distort biometric data and a blurred iris may result from loss of focus. The paper concluded that fusion of individual biometric traits at rank level can improve performance levels, even with data quality issues (Manju, R, et al, 2012)¹²

Chate, S, et al (2013) proposed a biometric verification system using hand images. The research wants to integrate hand geometry features at different levels of fusion to improve performance of palm-print based verification system. The research uses finger lengths and widths. Gabor filter based approach is used to extract the palm print features. The biometric samples collected are compared to those already in the database. In this mode, one sensor is used the palm print and hand geometry at the same time, without any additional inconvenience to the user. With a capturing device with a 640 x 480 pixels, results from 300 users clearly indicated the utility of combining the biometric features. The results obtained from the decision level fusion is compared with the score level fusion result to check if there is any increase in performance. It was discovered that decision level fusion produces FAR as low as 0.02% but FRR increased to 9% as two level decisions are made. For score level fusion, FAR% is 0.28% and FRR of 2%, but two decision levels give a FRR% of 9%, though very simple and fast in operation. When a score level normalization scheme call tanh was used, the system produced a FAR% of 0.28% and 2% FRR (Chate S, et al, 2013)¹³

Sumathi S, et al (2013)¹⁴ discussed using hand geometry as a most accepted biometric to develop an accurate and secure authentication system. The proposed method is to use window size palm print features and hand geometry computed from the same image for authentication. This type of integration is expected to increase the robustness of the system.

¹² R.Manju,a A.Rajendran a ,A.Shajin Narguna (2012). International Journal of Engineering Research & Technology (IJERT) Retrieved from <https://www.ijert.org/research/performance-analysis-of-multimodal-biometric-based-authentication-system-IJERTV1IS7032.pdf>

¹³ S.Chate, Suhas & Ubale, Pratik & Joshi, Madhuri. (2013). Person Verification using Fusion of Palm Geometry and Palm Print. International Journal of Computer Applications. 73. 42-48. 10.5120/12836-0163.

¹⁴ S.Sumathi, R.**Rani Hema** Malini (2013). Multimodal Biometrics for Person Authentication using Hand Image. International Journal of Computer Applications (0975 – 8887) Volume 70– No.24, May 2013

Feature extraction is done using *Discrete Wavelet Transform (DWT)* and classification is done with *Support Vector Machine (SVM)*. The proposal is to use hand geometry and asking users to place their hands freely on the scanner as the features needed are the length and width of fingers and the palm width and palm features. A FAR 0% was achieved using a publicly available GPDS Hand database and final decision made at matching score fusion level showing the robustness of the system for application in high security areas. The overall objective is to prove that the integration of palm print and hand geometry features produce performance levels not achievable with a single biometric trait. The results of another research achieved recognition rate of 98.59% and 0% FAR by fusion of palm print and hand geometry features.

(Latha, L et al, 2013)¹⁵ in their research paper “Providing multimodal biometric authentication using five competent traits stated that a single biometric authentication is limited in recognition accuracy and proposes that a multi-modal approach is preferred for identity verification. The paper discusses using five biometric traits – iris, retina, fingerprint, palm print and ear. Each of the biometric trait is analyzed individually, and the matching scores recorded for the feature and the scores are combined using a weighted fusion rule. The entire process included pre-processing, feature extraction and feature matching on each of the iris, retina, ear, and palm print and fingerprint traits using MATLAB

In order to ensure that the system can handle liveness verification, retina blood vessel pattern approach is used. Several experiments were conducted using images obtained from five different datasets to validate the approach. The results showed multimodal biometric systems are more reliable and accurate than single biometric-based verification systems. Iris recognition accuracy rate was 94.8% using publicly available CASIA database, retina recognition rate using VARIA dataset was 97.8%. The USTB ear database was used with 95.2% accuracy, CASIA palm print database with 98% accuracy and FVC2002 fingerprint database with 97.7% accuracy. Overall recognition accuracy rate was 99.3% using the min-max normalization and then the sum fusion method. This indicated a significant improvement in performance levels when compared to a single-trait biometric authentication system.

With the advent of the information technology age, information technology resources must be secured with authentication and authorization techniques. There are many ways to do this, but biometrics has proved most reliable for authentication or authorization of the human being using our unique physiological or behavioural qualities.

Biometrics uses a person’s physical or behavioural trait to identify individuals. Physical traits include the palm, fingerprints, and the iris as they are unique. Behavioural traits include voice, signature, keystroke dynamics and these are referred to as quantifiable characteristics and is also used to protect information resources from unauthorized users. When a combination of two or more biometric traits are used for identification and verification in a biometric-based system, it is referred to as multimodal biometrics.

¹⁵ Latha, L. & Thangasamy, Sangarappan. (2013). Providing multimodal biometric authentication using five competent traits. *The Imaging Science Journal*. 61. 212-218. 10.1179/1743131X11Y.0000000033. Retrieved from <https://www.researchgate.net/publication/272310666>

This is done to improve the recognition accuracy rate and has become an emerging trend. This is possible when the different biometrics being used are statistically independent. The goal of a multimodal system is to fuse two or more physical or behavioural traits. This system being proposed in this research is based on the use of a combination of iris, palm and the fingerprint in a biometric fusion, which is a combination of the classification of the measurements obtained from the different biometric traits for enhancement. Fusion of biometric traits can be at the sensor level, feature level, matching score level and the decision level. At the sensor level, a composite biometric trait is formed from the individual biometric traits taken from the sensors. At the feature level, signals from different biometric channels are pre-processed and the vectors of their features are extracted separately using a selected algorithm. These vectors are then combined to get a composite feature vector and this is used for classification. At the matching score level, feature vectors are processed separately and each matching score is recorded and the individual biometric matching score is used for classification purposes

At the decision level, the first step is to classify each modality independently and then implement any of the fusion strategies or a combination for improved performance. When compared to unimodal systems, a multimodal biometric system takes a longer time, but is more reliable for security purposes. This process can result in a highly reliable security multimodal biometric system if the appropriate normalization and fusion techniques are used. Users with dry fingers or cuts on fingers can provide their iris or palm as an alternative and better biometric indicators. No security is completely foolproof. As we introduce new techniques, we add to the time and cost of implementation. It is known that fingerprints can be forged using touched surfaces and copied using some materials which are easily obtained, but iris-based systems are tough to forge because they are based on physiological reactions to changing conditions of illumination.

However, physical modelling of an iris-based system is expensive. So iris-based systems should be implemented in high-security applications. As a result, iris and retina-based installations are not common when compared to fingerprint and face recognition systems. Biometric applications based on fingerprints and the face are good enough as authentication and access control systems for low security environments. Multimodal systems have solved many issues arising in unimodal systems and are used in different applications like access control, border control, citizens' identification systems, and network security.

Multimodal systems are expected to reduce false acceptance and false rejection rates, provide a secondary enrollment method when sufficient data cannot be obtained from a single biometric sample given by the user and can also be used to protect identification systems from spoofing through the use of non-live data sources such as fake fingers. (Lokeswara Rao Bhogadi et al, 2018)¹⁶

¹⁶ Lokeswara Rao Bhogadi, N. Bhagyalaxmi (2018). **Multimodal biometric authentication**. Journal of Wireless Communication Technology. Whioce Publishing. ISSN 2529-766X.

3. PROBLEM STATEMENT

To maintain the major information security objectives of confidentiality and integrity, the processes leading to the capturing, creation, storage of participant information in identity management systems must be controlled, secured, and subjected to a high level of scrutiny and verification to ensure that only authorized participants are captured in the identity system database. Also, it must be ensured that only authenticated users are given access to the identity database system for high reliance and trust in the system. False acceptance rates and false rejection rates should also be minimal.

This increasing inter-connectivity of systems and dependence on computer and internet-based networks made Cybersecurity and related risks management issues major considerations in designing, developing and managing identity systems. Methods of improving the efficacy of identity systems include biometric-based multimodal authentication. The project will identify Cybersecurity and related risk management challenges in identity management systems from threats and vulnerabilities and present practical and logical solutions to these issues.

4. AIM OF THE STUDY

4.1 AIMS

To investigate Cybersecurity and risk management challenges in Identity Management Systems and proffer an appropriate biometric- based multimodal authentication solution.

4.1 Research Objectives

The specific research objectives of the study are as follows

- (i) Evaluate the processes and steps involved in the capturing and storage of identity information used in identity management systems.
- (ii) Identify the Cybersecurity and risk management issues and challenges affecting identity management systems
- (iii) Identify various biometric-based multimodal authentication systems currently used in Identity Management Systems
- (iv) Design and Implement a biometric-based multimodal authentication system with optimal Cybersecurity and minimized risk management
- (v) Recommend an appropriate framework for implementation

5. CYBERSECURITY CONCEPTUAL FRAMEWORK

Cybersecurity refers to the different techniques used to protect organizational data from cyber-attacks. It also includes techniques used to prevent unauthorized access to systems, networks, applications and devices. Cybersecurity is important because information assets are critical to the success of organizations as decisions are based on data stored in the systems. Cybercrime has become a big business and the cost cybersecurity breaches is high. The consequences of cyber-attacks include loss of revenue, loss of reputation, lawsuits if clients' data are exposed and disruption of business operations.

As we are in the information age where most operations and transactions have a web component or involved a network-based device, organizations must protect their user identification and verification systems. According to (Rishabh R, 2019)¹⁷, a breach of security is also called a cyber-attack.

Examples of cyber-attacks include online identity theft, malware attacks, SQL injection, phishing, spoofing and cross-site scripting etc.

- i. **Online identity theft** – This involve the stealing and use of another person’s personal information like their password, debit or credit card numbers to perpetrate fraud online
- ii. **Malware attack** – Using an unauthorized software to cause damage, disruption or gain access to a system or device which can allow access to sensitive personal information like passwords and usernames.
- iii. **SQL Injection** – In this scenario, malicious SQL statements are used to gain unauthorized access into a database and change the information stored and this can then be used to facilitate fraud
- iv. **Phishing** - Here, a message is sent to a victim designed to trick the victim to release sensitive personal information
- v. **Spoofing** – This happens when communication is made to look like its coming from a trusted source. It could be emails, IP address or a Domain Name Server (DNS)
- vi. **Cross-site Scripting** – An attacker injects malicious software code into an otherwise safe website and provide unauthorized access by bypassing controls and give access to copy sensitive personal information

5.1 Cyber Risk Management

Risk refers to the probability that an adverse event will happen that will affect an entity such as a person or organization. Risk management refers to the processes involved in assessing risks, analyzing them, prioritizing areas of focus and developing strategies to mitigate the effects of the risks on the organization. The Risk Management process include identifying the risk, analyzing the risk and then determine the measure or metric to control it. Risk management strategies include avoidance, mitigation, transfer and acceptance. Risk concepts will include:

- i. **Cybersecurity Risk** - Refers to the probability that a cyber-attack will occur and cause a loss or data breach to a computer system
- ii. **Vulnerability** – A weakness in a system that can be used to gain unauthorized access and steal sensitive personal data like password and PINS
- iii. **Threat** – Any event that can take advantage of a vulnerability in a system to cause disruption, damage, corruption of any information technology asset

¹⁷ Rishabh rajvanshi. 2019. **Cyber-security-ways-to-ensure-identity-protection** Retrieved from <https://tecake.in/cyber-security-ways-to-ensure-identity-protection>

According to Sakthidevi, K.R. (2019)¹⁸, cyber risk management concepts include

- i. **Access Control and password Security** - This is the fundamental ay of protection information stored on a system. This should be one of the first measures in cybersecurity
- ii. **Authentication of Data** – All documents received online must be checked as authentic before being downloaded into our systems.
- iii. **Firewalls** – This can be a software program or hardware used to protect the system from unauthorized access and all documents entering or leaving are checked if they meet specified security criteria.
- iv. **Malware Scanners** – This is used to check files and documents on the systems for viruses and other malicious software like Trojans
- v. **Anti-virus Software** – These are programs that check and detect malicious programs like worms and viruses. Most include features that allow them to be updated automatically when a new version or patch is available online.

5.2 Online Identity Management

As a result of the growth and dependence on the Internet, many individuals, groups, organizations and government conduct their daily interactions and transactions online and this has attracted hackers who intercept these communication and access sensitive information for financial gain, disruption and embarrassment of victims. Any fraudulent activity undertaken to steal sensitive personal information like passwords and debit or credit card numbers, PINS to purchase items or services online without the permission or authority of the original owner is identity theft. Protecting online identities has become a major cybersecurity practice. The methods used to protect network and online identities include conducting cybersecurity awareness training, ensuring that software are continuously updated for patches, securing networks by using virtual private networks (VPN) and using advanced authentication and verification systems.

In the context of identity management, cybersecurity risk management therefore involves using all available techniques and methods to ensure that only authorized users have access to organizational systems with robust identification and verification systems in place. This can be achieved using multimodal biometric traits and fusing them at the match score level with a selected and robust algorithm which provides low False Acceptance Rates (FAR) and low False Rejection Rates (FRR)

¹⁸ **SAKTHIDEVI, K.R (2019). Cyber Risk Management – A Conceptual framework.** International Journal of Scientific Research and Review. Vlume 8, Issue 2, 2019. ISSN No: 2279-543X. Retrieved from <http://www.dynamicpublisher.org/gallery/52-ijssrr-d1465.f.pdf>

6. THORETICAL FRAMEWORKS

In this section we examine applicable theoretical Frameworks.

6.1 Digital Identity Theoretical Framework

Kabwe Felix and Phiri, J (2019)¹⁹ asserted that the growing use of the internet involves many users connecting through different platforms and devices like tablets, laptops, IoT enabled devices, intelligent home device and RFID-enabled systems. This complicates managing identities and creating risk and privacy issues. When identities are stolen, there is a big of risk of asset manipulation or loss of assets. For example, use of online mobile transfer system have resulted in the theft of digital identities and financial loss to victims as the transfers did not reach the intended beneficiaries. Digital identity can be defined as the unique character or personality of an individual and consists of a group of traits used to login to services for verification and authorization by single mode or multimodal identifier for access based on trust. This identity will also include certain characteristics that enable membership of a group or organization and a person may multiple identities for different groups

Soneka, P and Phiri, J (2019) asserted that ease of use, security and usefulness are factors that affect adoption of mobile technology using the **Technology Adoption Model (TAM)** and this model has been well tested and used. TAM actually provides a basis of finding out how external variables influence intention, belief and attitude in using new technology. The conclusion from the model was that when individuals see benefits, easy to implement and use, most people will adopt it

6.2 Cybersecurity Theoretical Framework

Cybersecurity researchers have tried to use behavioural theories to explain behaviour and response to Cybersecurity rules by individuals generally. (Lebek, B et al, 2014)²⁰ focused on four behavioural theories: General Deterrence Theory (GDT), Technology Acceptance Model (TAM), Protection Motivation Theory (PMT) and Theory of Planned Behaviour (TPB) and present salient factors that have significant effect and influence on employee security behaviour.

- i. **General Deterrence Theory (GDT):** GDT summarized that people are rational in decision making and will be discouraged from committing offences based on the punishment attached to such.

¹⁹ Kabwe, Felix & Phiri, Jackson. (2019). A Framework for Digital Identity Management. Management.Proceedings of the International Conference In ICT (ICICT2019) - Lusaka, Zambia (20th - 21st November 2019). ISBN: 978-9982-70-985-9. Retrieved from <https://www.researchgate.net/publication/337856516>

²⁰ Lebek, Benedikt & Uffen, Jrg & Neumann, Markus & Hohler, Bernd & Breitner, Michael. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review. 37. 1049-1092. 10.1108/MRR-04-2013-0085. Retrieved from <https://www.researchgate.net/publication/280197278>

Fig. 15: The General Deterrence Theory

Source: <https://study.com/academy/lesson/what-is-general-deterrence-definition-theory-examples.html>

- ii. **Technology Acceptance Model (TAM):** Employees will comply with information security measures when it is easy to follow and comply with and the benefits of using the technology are visible.

Fig. 16: The Technology Acceptance Model

Source: https://commons.wikimedia.org/wiki/File:Technology_Acceptance_Model.png

- iii. **Protection Motivation Theory (PMT):** PMT is used to determine how employees respond to security risks by forming attitudes towards such threats and punishment and developing a coping mechanism.

Fig. 17: The Protection Motivation Theory

Source: <https://bmcp psychology.biomedcentral.com/articles/10.1186/s40359-017-0182-3>

- iv. **Theory of Planned Behaviour (TPB):** TPB links our beliefs to our behaviour. Therefore, an employee is likely to comply with information technology security directives if he/she believes in having an error and stress free working environment.

Fig 18: The Theory of Planned Behavior

Source: <https://sphweb.bumc.bu.edu/behavioralchangetheories>

All the four theories were used and combined in meta-model to explain the behavioural intention (BI) or actual behaviour (AB) of employees in relation to complying with information security measures in organizations using different causal factors. The research concluded that several behavioural factors should be considered in developing effective security awareness programs.

These factors include the following categorized by their source theory

- i. Perceived usefulness (PU), Perceived ease of use (PEOU) from Technology Acceptance Model (TAM),
- ii. Subjective norms (SN), perceived Behavioural Control (PCB) from the Theory of Planned Behaviour (TPB)
- iii. Perceived severity of sanctions (PSOS), Perceived Certainty of Sanctions (PCOS) from General Deterrence Theory (GDT)
- iv. Attitude Towards Information security (ATT), Threat Appraisal (TA), Coping Appraisal (CA), Perceived Vulnerability (PV), Perceived Severity (PSOT) and Response Efficacy (RE) from Protection Motivation Theory (PMT)

The overall goal is to raise the level of information security awareness (ISA) of members, groups and organizations and reduce the gap between behavioural intention (BI) and actual behaviour (AB) with the specific objective to ensure compliance with information security policies and procedures.

7. METHODOLOGY

The goal of this research is to develop a safe and highly efficient biometric-based multimodal authentication system for identity management that takes into consideration Cybersecurity and related risks. The research methodology will be descriptive, analytical and empirical. As a first step, a comparative study of individual biometric traits will be done to determine the strengths, weaknesses and limitations of commonly used biometric traits in identity management systems. Secondly, an assessment of different combinations of biometric multimodal systems and solutions currently in use in identity management systems will be carried out to identify their strengths, weaknesses and limitations.

The results from this analyses would enable the selection of appropriate biometric traits like the face, iris and fingerprints. Fingerprints, palm print and face recognition have been found to be popularly used based on universality, ease of collection and public acceptability.

The following steps will be followed:

- i. **Modality** - The biometric traits to be used to build the multimodal model will be selected.
- ii. **Level of Fusion** - These traits would then be combined at the matching score fusion level
- iii. **Fusion Strategy** - A reliable cryptographic-based algorithm will then be used to further combine the traits

8. EXPECTED RESULTS

The results is to produce give a risk-optimized and secure multimodal identification and authentication system with high accuracy rates and minimal false acceptance and false rejection rates. The research will provide further insights on Cybersecurity risk management challenges related to identity management systems, identify the strengths, weaknesses and limitations of biometric traits.

The results from this will provide data from which an optimal combination of selected biometric traits can be selected and used to develop a reliable biometric-based multimodal authentication system with integrity and that can be relied on by all users and stakeholders with complete confidence. The study will contribute significantly to the body of knowledge in the area of identity management and provide a solution that can be used in different identity management applications and schemes.

REFERENCES

1. Al-Mahafzah, Harbi & Alrawashdeh, Ma'En. (2012). A Survey of Multi-biometric Systems. International Journal of Computer Applications. 43. 10.5120/6182-8612. Retrieved from <https://www.researchgate.net/publication/231537573>
2. Chate, S, Suhas & Ubale, Pratik & Joshi, Madhuri. (2013). Person Verification using Fusion of Palm Geometry and Palm Print. International Journal of Computer Applications. 73. 42-48. 10.5120/12836-0163.
3. Garg, Suneet & gupta, Renu. (2017). Multimodal Authentication System: An Overview. International Journal of Control Theory and Applications
4. Ibikunle, Francis. (2013). Approach to cybersecurity issues in Nigeria: Challenges and solution. International Journal of Cognitive Research in Science, Engineering and Education
5. Ilugbusi, Abiodun & Adetunmbi, Adebayo. (2017). Development of a multi-instance fingerprint based authentication system. International Conference on Computing Networking and Informatics (ICCNI) 1-9. 10.1109/ICCNI.2017.8123780
6. Kabwe, Felix & Phiri, Jackson. (2019). A Framework for Digital Identity Management. Management .Proceedings of the International Conference In ICT (ICICT2019) - Lusaka, Zambia (20th - 21st November 2019). ISBN: 978-9982-70-985-9. Retrieved from <https://www.researchgate.net/publication/337856516>
7. Kumar, Munish. (2018). Fingerprint Recognition System: Issues and Challenges. International Journal for Research in Applied Science and Engineering Technology. 6. 556-561. 10.22214/ijraset.2018.2080
8. Latha, L. & Thangasamy, Sangarappan. (2013). Providing multimodal biometric authentication using five competent traits. The Imaging Science Journal. 61. 212-218. 10.1179/1743131X11Y.0000000033.
9. Lebek, Benedikt & Uffen, Jörg & Neumann, Markus & Hohler, Bernd & Breitner, Michael. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review. 37. 1049-1092. 10.1108/MRR-04-2013-0085. Retrieved from <https://www.researchgate.net/publication/280197278>

10. Lokeswara Rao Bhogadi, N. Bhagyalaxmi (2018). **Multimodal biometric authentication**. Journal of Wireless Communication Technology. Whioce Publishing. ISSN 2529-766X. Retrieved from <http://www.ipindexing.com/article/24536>
11. Manivannan, S. & Padma, E.. (2011). Comparative and Analysis of Biometric Systems. International Journal on Computer Science and Engineering. 3. 2156-2162.
12. Manju, R ,A.Rajendran a ,A.Shajin Narguna (2012). International Journal of Engineering Research & Technology (IJERT) Retrieved from <https://www.ijert.org/research/performance-analysis-of-multimodal-biometric-based-authentication-system-IJERTV1IS7032.pdf>
13. Mohammad Imrana, Ashok Raob , G Hemantha Kumar (2010). Multibiometric Systems: A Comparative Study of Multi-algorithmic and Multimodal Approaches. Retrieved from <http://creativecommons.org/licenses/by-nc-nd/3.0/>
14. Mwaura, Grace. (2017). Multimodal Biometric System:-Fusion of Face and Fingerprint Biometrics At Match Score Fusion Level. International Journal of Scientific & Technology Research. 6. 41
15. Parkavi, K. R. Chandeesh Babu and J. A. Kumar, "Multimodal Biometrics for user authentication," (2017) *11th International Conference on Intelligent Systems and Control (ISCO)*, 2017, pp. 501-505, doi: 10.1109/ISCO.2017.7856044
16. Parvathy. J, Dr. Poornima G. Patil. (2018). A Survey on Fingerprint Identification Techniques. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887. Volume 6 Issue I, January 2018-
17. Ramadan Gad, Nawal El-Fishawy, AYMAN EL-SAYED and M. Zorkany, "Multi-Biometric Systems: A State of the Art Survey and Research Directions" International Journal of Advanced Computer Science and Applications (IJACSA), 6(6), (2015). <http://dx.doi.org/10.14569/IJACSA.2015.060618> Journal on Computer Science and Engineering. 3. 2156-2162. Retrieved from <https://www.researchgate.net/publication/272310666>
18. Rishabh rajvanshi. 2019. **Cyber-security-ways-to-ensure-identity-protection** Retrieved from <https://tecake.in/cyber-security-ways-to-ensure-identity-protection>
19. SAKTHIDEVI, K.R (2019). **Cyber Risk Management – A Conceptual framework**. International Journal of Scientific Research and Review. Volume 8, Issue 2, 2019. ISSN No: 2279-543X. Retrieved from <http://www.dynamicpublisher.org/gallery/52-ijssr-d1465.f.pdf>
20. Shameem, Z.A., Mohite, J.N., & Sharmin, S (2017). **A Review on Advance Biometric Fingerprint Based Security Systems**. International Journal for Research in Applied Science & Engineering Technology (IJRASET). ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887. Volume 5 Issue X1, November 2017
21. Sumathi, S, R.Rani Hema Malini (2013). Multimodal Biometrics for Person Authentication using Hand Image. International Journal of Computer Applications (0975 – 8887) Volume 70– No.24, May 2013