With the development of technology, personal data security and privacy is considered as a major challenge for all over the world. Biometrics systems are used to protect data and identity verification [1]. The safety issues of biometric information cannot be compromised. Where the issues have appeared, it may effect on the quality and users reliability. Some published research papers are related to biometric information privacy [2] and few define the critical issues of biometric information security [3]. A good reliability rate can increase biometric system users rather than using passwords or pin codes and poor reliability will reduce users.

Online banking service [4], employee attendance, employee time tracking device and other identity verification systems are frequently used in Bangladesh. The most common methods of verifications fingerprint and face recognition. On 2nd October 2016 Bangladesh government launched the Smart National ID card [5] and started collecting biometric information from the citizens. Recently to digitalize government services, NID verification gateway server is getting under way [6]. As the large possibility of using biometric technology, it is very important to study on the reliability and the trustworthiness of all biometric systems which are used in Bangladesh at users’ point of view.

Most of the biometric systems are integrated with hardware and software. The biometric system market will increase by 15% compound annual growth rate between 2017 and 2023 [7]. The market demand for new biometric systems can be visualized by analyzing adoption, satisfactoriness and reliability reviews.

**Aim:**

The aim is to evaluate which system is more efficient and acceptable to users by exploring the users' reliability and satisfactoriness of biometric systems.

**Objectives:**

1. To interpret user reviews about the quality and reliability of biometric systems.

2. To compare different biometric systems based on users aptitude.

3. To study users demand for biometric systems.

**Background:**

Traditional way of assure safety and security password protocol system is used. But this protocol has some drawbacks: it can be stolen, user can forget their password. As this security issue has become a talk of topic all over the world, the UK government started using biometric trait for identification in 1960. After this several study took place for designing biometric system and having a good recognition accuracy [8]. This technology uses physical or behavioral traits of user to solve the problem of authentication. Biometric system is consisting of four modules which are sensor module, feature extraction module, template database and a matching module. The process of authentication goes through in two stage: Enrollment stage and verification stage. When a user put his thumb on the sensor a picture of fingerprint is taken by the sensor module. Further from this picture the system extracted some data and make it suitable to generate template data and save them in a database for the verification stage. After that a query is made for matching the data with the template database to make sure that the user is a valid person. Imposing this for solving the security issue there arises two concern one is biometric traits cannot be revoked and reissued when the biometric information of a person is compromised. If a person fingerprint image is stolen it cannot be replacing in the template database as this information is unique.

Ratha et al. [9] has detected eight point from where this biometric information can be stolen or tempered. Namely, attacks on the interface, attacks on the modules: feature extraction module and matching module, attacks on the template database and also the channels from where the biometric information is flowing. One of the attack is spoofing which is an interface level attack occurs because of the fake biometric presentation. An experiment was taking place by attacking with the fake fingerprints. The result showing that the acceptance rate of fake fingerprint 67%. Liveness detection is a well-known countermeasure to distinguish between the fake fingerprint and the real fingerprint. Two scientist proposed to detect the perspiration phenomenon to differentiate the living fingers from the fake non – living fingers. Another researcher coli er al. utilized the static feature as well as the dynamic features of a fingerprint image which to prevent the spoofing attack.

Galbally et al. [10] proposed a method which use fingerprint parameterization based on the quality of fingerprint images. He proposed it as a classification problem where the result will be real or fake. Kim, a researcher proposed to design an image descriptor to handle liveness detection. He used a property of image which is dispersion. The difference of dispersion in the image gradient field will be different if the fingerprint is being faked.

This accuracy of a biometric system can be measured by using three factor: False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (ERR). This accuracy depends on the image quality and the matching algorithms. There is a platform which is FVC-ongoing where researcher can upload their matching algorithm to evaluate the FAR, FRR and ERR. At present the best matching algorithm which name is HXKJ and ERR = 0.022% [8].

Among 4.6 billion mobile users 52.7% browse Internet which increases cybercrimes rapidly. Bangladesh Government initiated biometric SIM registration program in December, 2015. Aim of this program has to verify the real owner of SIM using NID and help to unearth the real criminal. S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell demonstrate about the ownership, user identity, exploitation, also security and safety concerns that challenged this program. Western world preserve users privacy rights where Bangladesh is lagging behind. Their online survey concluded that 77% participants dislike the SIM registration system. Only 15% supported and 4% ignored the survey [2].

V. Andronikou, D. S. Demetis, T. Varvarigou, I. Group, and H. Street [3] described the design complexity, security issues, personal attacks (PA), indicators and factors of biometric systems. How biometric encryption works, what concepts are identified by Electronic Privacy Information Centre (EPIC) and the panacea of those are also covered and highlighted here. The result of this study shows that more research needed to focus on technical domain and biometrics are not only the part of solution but also problem. The real life challenges and their linkage to social, economic and political era are still untouched in this study.

Marcos [11] defined the difficulty of a biometric system with a study. To detect the vulnerability of biometric system two situations are intensely focused. First one is impostor’s try to access the system as a substitute of real user and another one is when a person avoid his identity which is suspenseful. Sensor, Transmission Between the sensor and the Feature Extractor, Feature Extractor, Transmission of the Extracted Features, Classifier, Data Base, Transmission of the Database Templates to the classifier, Decision are the eight attack levels. Three main authentication methods handheld token (card, ID, passport, etc.), knowledge based (password, PIN, etc.) and Biometrics have some advantages and drawbacks also. Biometric technologies like fingerprint, voice, iris, face reflects some vulnerabilities and there are also solutions. Data encryption and time stamp watermarking are two methods for solution. Although once the data are decrypted in encryption there are no further data protection. Adobe Photoshop and Corel Draw with Digimac technology introduces an information which cannot be erased without hampering the image standard & this can be fruitful for time stamp data.

By examining the existing legal and academic debates, the privacy concerns and debate of biometrics in the biometric context is much important issue nowadays. Many countries like Norwegian, Swedish and US follow the law to protect data from a legal perspective [12]. To embrace the latest technology, government and commercial organizations plays a powerful role. Many countries and entities have begun including the biometric technologies like fingerprint reader, facial recognition, RFID chips in different sectors to resolve the unauthorized use. To minimize fraud and improve national security by using biometric technology, several legislative and regulatory initiatives has been adopted. To store information on a portable token is welcomed by data protection advocate but there are some security concerns still exists. By using various biometric applications many controversial legal problems arises. Biometric privacy should be protected or what extend it should be protected depends on the context in the biometric domain. Although the legal measures are improving with widespread implementation, still need some clue for shaping provided by current initiatives.

**Main Question**

How does user reliability effect for consuming the biometric authentication system in Bangladesh?

**Sub questions**

1. What type of biometric systems are frequently used in Bangladesh?
2. What are the problems experienced by users?
3. What are the demands of users?

**References:**

[1] R. E. O. Paderes, “A Comparative Review of Biometric Security Systems,” *Proc. - 8th Int. Conf. Bio-Science Bio-Technolocgy, BSBT 2015*, pp. 8–11, 2016.

[2] S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell, “Privacy, security, and surveillance in the global south: A study of biometric mobile SIM registration in Bangladesh,” *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2017-May, pp. 906–918, 2017.

[3] V. Andronikou, D. S. Demetis, T. Varvarigou, I. Group, and H. Street, “Biometric Implementations and the Implications for Security and Privacy,” *1st in-house FIDIS J. Issue*, no. 1, pp. 1–20, 2007.

[4] “Standard Chartered Bank - Touch Registration and Login.” [Online]. Available: https://www.online-banking.standardchartered.com/login/IBank?ser=100&act=TouchIdRegistration.jsp&cntry=BD. [Accessed: 24-Sep-2019].

[5] “Bangladesh Introduces ‘Smart’ National Identity Cards - Global Voices Advox.” [Online]. Available: https://advox.globalvoices.org/2016/10/07/bangladesh-introduces-smart-national-identity-cards/. [Accessed: 24-Sep-2019].

[6] “Joy launches NID verification gateway server | Dhaka Tribune.” [Online]. Available: https://www.dhakatribune.com/bangladesh/government-affairs/2019/07/17/joy-to-launch-nid-verification-gateway. [Accessed: 24-Sep-2019].

[7] “Global Biometric System Market Research Report- Forecast 2023 | MRFR.” [Online]. Available: https://www.marketresearchfuture.com/reports/biometric-system-market-3754. [Accessed: 24-Sep-2019].

[8] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and accuracy of fingerprint-based biometrics: A review,” *Symmetry (Basel).*, vol. 11, no. 2, 2019.

[9] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[10] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, Jan. 2012.

[11] M. Faúndez-Zanuy, “On the vulnerability of biometric security systems,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 19, no. 6, pp. 3–8, 2004.

[12] Y. Liu, “Identifying legal concerns in the biometric context,” *J. Int. Commer. Law Technol.*, vol. 3, no. 1, pp. 45–54, 2008.