

# COST-EFFECTIVE BIOMETRIC HANDPRINT VOTING SYSTEM

# ACKNOWLEDGEMENTS

I would like to express my sincere gratitude and appreciation to the following individuals for their invaluable contributions to my research on a "Cost-Effective Biometric Handprint Voting System":

First and foremost, I would like to thank the University of West London for presenting us with the opportunity to undertake such a challenging task; and their representative judging panel for their time and attention in evaluating our findings. Their feedback and insights have helped us refine our work and have provided valuable perspectives for future development.

I am also deeply grateful to the faculty and staff at ANC Education for granting me permission to use whatever resources available at their disposal to conduct this research within the premises. Their support and cooperation have been vital in ensuring the success of this research project.

I further extend my heartfelt thanks to my family, friends and batch mates at ANC Education who took the time to participate in this study. Their willingness to fill out questionnaires and share their feedback has been instrumental in gathering the necessary data for this research.

Lastly, I would like to express my deepest appreciation to Mr. Mahen Jayalath, my Project Supervisor. His guidance, expertise, and unwavering support throughout every stage of the research have been invaluable. His insights and feedback have significantly enhanced the quality of this study.

Without the contribution and support of these individuals, this research would not have been possible. Their assistance has been crucial in deepening my understanding of biometric voting systems and how cost effective solutions can be implemented using handprints. I am truly grateful for their involvement and assistance in this endeavor.

## ABSTRACT

This paper presents the conceptual development and designing of a cost effective biometric voting system and means of implementation that effectively utilizes handprint recognition technology to enhance the security, accuracy, and accessibility of the entire voting process as well as the voting experience. The system is designed to focus on addressing and overcoming the many common challenges faced by the traditional voting methods such as vote rigging, fraud and impersonation just to name a few.

The biometric voting system comprises a combination of both hardware and software consisting of a handprint scanner built and integrated into the vote casting machine itself, allowing for voters to verify themselves prior to casting their vote and then later onwards for confirmation of their vote. The system will consist of an inclusively secured backend database management software that stores the biometric data of previously registered voters against which their prints will be cross checked with using specialized software for a more thorough process of voter identity verification allowing for increased confidence in the electoral process.

The complete physical development of a fully functional system however has been faced with a great many issues solely due to financial and time constraints and therefore will not be able to be fully practically tested. Instead practical tests of a prototype and several in-depth conceptual analyses of previous researches on similar systems have been performed in a comprehensive literature review; as well as reviews on the discussed system's practicality have been thoroughly conducted and have indicated that the biometric handprint voting system has the potential to improve the integrity, accuracy and convenience of the entire voting process whilst greatly cutting down on the electoral costs associated with the traditional paper based system in the long term. Based on these results it has proven definitively that the biometric voting system additionally has the potential to substantially increase voter confidence and trust in the electoral process as a whole, thereby increasing voter turnout as well.

In conclusion, although financial and time constraints prevent the building and testing of a physical system, at its current phase of development the biometric voting system represents a noteworthy stride towards the ongoing efforts to improve the security, accuracy, accessibility and costs of the voting process in its entirety. Future research on this topic should be initially focused on mirroring the developed system and testing it for functionality then physically building it and thoroughly testing the physical model in real-world settings to assess its effectiveness and feasibility even further.

# TABLE OF CONTENTS

1	Introduction .....	07 - 09
2	Literature Review .....	10 - 21
2.1	Introduction	10
2.2	Abdelwhab, A. and Viriri, S. (2018). <i>A Survey on Soft Biometrics for Human Identification. Machine Learning and Biometrics.</i>	10 - 13
2.3	Ellena, K. and Petrov, G. (2018). <i>Cybersecurity in Elections Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies.</i>	14 - 17
2.4	Krimmer, R., Volkamer, M., Cortier, V., Gore, R. and Hapsara, M., (2018). <i>Electronic Voting.</i>	18 - 21
2.5	Conclusion	21
3	Requirements Analysis .....	22 - 32
3.1	Functional Requirements	22 - 23
3.2	Non-Functional Requirements	24
3.3	Project Constraints	25
3.4	Factors Influencing the Project	26
3.5	Resources and Materials Used	27

<b>4</b>	<b>  Methodology .....</b>	<b>28 - 32</b>
4.1	Research Philosophy and Approach	28
4.2	Data Collection and Sampling Methods	28 - 31
4.3	Ethical Considerations and Limitations	32
<b>5</b>	<b>  System Design and Testing .....</b>	<b>33 - 42</b>
5.1	Introduction to the System	33
5.2	System Architecture	34
5.3	System Use Case	35
5.4	Developed Prototype	36 - 46
5.4.1	Website (GUI)	36 - 41
5.4.2	Finger/Handprint Matching Algorithm	42 - 46
5.5	Prototype Testing and Evaluation	47 - 57
5.5.1	Website (GUI) Test Logs	49 - 52
5.5.2	Matching Algorithm Test Results	53 - 57
<b>6</b>	<b>  Conclusion .....</b>	<b>58 - 59</b>
<b>7</b>	<b>  Bibliography .....</b>	<b>60 - 62</b>

# I | INTRODUCTION

Ever since the COVID-19 pandemic took the world by storm back in December 2019 it brought along with it a global wave of economic distress causing many countries worldwide to prioritize survival more than most by any means necessary whether it be raising taxes or borrowing from others to make up for the many losses suffered during this period of instability. However the issue with this form of temporary short term stability is that countries with already struggling economies only fail to see the decades of debt lying in wait for their future.

This brings us to the current situation Sri Lanka has been in and is in at present; ensnared in a debt trap (Moramudali, 2017). As of today Sri Lanka owes about US \$7 billion to China and around US \$1 billion to India (Perera, 2022). Having already borrowed billions worth of foreign currency from many other countries as well, the unexpected pandemic only further worsened the situation for the country. As a result the government has had to resort to giving China a controlling equity stake and a 99-year lease for Hambantota port (Hillman, 2018), whilst the Western Terminal has been handed over to an Indian company (Farzan, 2021); all for the sake of maintaining its relationships with these countries and extending debt deadlines to stay afloat; given that its damaged reputation with lenders following its failure to make an interest payment on its foreign debt for the first time, made it even harder to borrow money on the international markets (Perera, 2022). As Moramudali (2017) said it best “Sri Lanka, in fact, had no option but to reach out for money and was in no position to refuse these offers which ultimately had placed the Sri Lankan government between a rock and a hard place.”

After careful assessment of the country's state of emergency and past expenditures that may have majorly contributed to this current situation a statistic that was quite hard to overlook has been the election costs; with at least LK Rs.7 billion spent for the last parliamentary elections in 2020 and the upcoming elections estimated to cost a minimum of LK Rs.10 billion (Bandara, 2022). Additionally according to Jayasinghe (2020) it has been stated that the money spent per voter by a party or an individual candidate has increased from LK Rs.67 to about LK Rs.600; almost ten times as much as it used to be back in 2004. The issue with this increment is that the election process on its own has undergone little to no noticeable changes whatsoever despite the higher costs and increased budget allocations. A driving factor behind this surge in expenditure could be the exploitation of the fact that Sri Lanka still lacks a campaign finance law, therefore the political parties are not legally bound to present a financial statement on poll related expenditures to the Election Commission; explaining why parties fearlessly spend as they please to make sure they secure the win. It is further stated that the shared value of LK Rs.1.3 billion in campaign expenditures amongst the three main contenders of the 2019 elections were based on the minimum figures, so the actual expenditures would be much higher than those in the reports (Fernando, 2019).

Hence why not only a biometric voting system has been proposed but a cost effective means of implementing it as well. The cost effective method of implementation stems from the age-old proverb that "slow and steady wins the race". Moralizing the very principle that one is better off being methodical than rushing into something unprepared (Poem Analysis, n.d.), is one that fits perfectly with the current cards the country has been dealt - with little to no room for investing in projects with diminishing returns.



As for the system itself, it is set to replace one of the single handedly most costly and recently outdated traditions the country still follows up to this day: the paper based elections. The reason being as Sherlan Benedict said it best is because “A vote is precious. It is the most powerful non-violent tool that we have in a democratic society to express our intentions” (Newsfirst Sri Lanka , 2021), therefore leaving it as exposed as it is, to fraud and various other forms of tampering is a much greater danger than mere negligence. Which is why the discussed biometric voting system is key as it puts the safety of the peoples’ votes in their own hands. This consensual, non-intrusive form of voting optimizes the use of handprints as a means of identification, verification and confirmation of the voter’s identity and choice. Moreover the system is paper-free and therefore entirely negates the cost of printing ballot papers saving the country an estimated full cost of about Rs.2 billion worth in printing expenses alone (NDTV). The system is further uniquely designed to be able to match a fingerprint to the owner of a handprint stored in its database, regardless of the fingerprint input being altered; swiftly identifying the owner of the input fingerprint and therefore nullifying the need for the unnecessary and constant re-registration process that is usually the case with these types of systems. By incorporating this technology, the voting process can be made more secure, accurate, and efficient whilst making it more accessible and transparent, promoting greater democratic participation and contributing to the overall improvement of the democratic process.

This paper outlines the existing literature on biometric voting systems; their costs, technical and logistical obstacles, privacy and security concerns and regulatory difficulties. This literature is then applied to discuss the system’s functionality, security and ability to perform under the many various circumstances associated with the voting process. This system is important, as the use of biometrics in voting has become more widespread, with implementations in countries including India, Brazil, Ghana, and Indonesia as well; however, as technology improves and the cost of biometric systems decreases, many other developing democracies are also considering and will be willing to use election technologies as such. Finally, the paper introduces the biometric voting system as a holistic tool for the government and people alike with increased accuracy, efficiency, transparency and overall security in elections at a lower price over the long term.

## 2 | LITERATURE REVIEW

### 2.1 INTRODUCTION

In the recent years that have passed, the topic on the development of biometric voting systems as a means of enhancing the security, efficiency, and accessibility of the electoral process as a whole has only grown in terms of interest generated ever since it gained traction. As it is, biometric methods of authentication have gained significant attention due to their potential to address the many various challenges associated with the traditional paper-based voting methods be it impersonation, multiple voting, voter fraud or ballot stuffing. This literature review aims to extensively investigate the existing research and advancements that have been made in the field of biometric voting systems. After having analyzed the current state of the field, this review has been purposed to identify the strengths and weaknesses of these systems; highlight the key technological innovations that have been made in the field; and provide meaningful insights into the potential of future prospects of implementing such systems in electoral settings.

### 2.2 Abdelwhab, A. and Viriri, S. (2018). *A Survey on Soft Biometrics for Human Identification. Machine Learning and Biometrics.*

Firstly, the survey conducted by Abdelwhab and Viriri (2018), on the topic of soft biometrics for human identification; the performance of various biometric systems were examined in particular, allowing for the authors to identify that one of the key factors associated with assessing the performance of any biometric system was the false acceptance rate (FAR). This is expanded upon, and described as the rate at which an impostor was mistaken for, and accepted as a genuine user; adding that a high FAR correlates to poor performance of the tested system whilst interpreting this as a result of the system failing to accurately distinguish between impostors and genuine users.

Furthermore, it has been noted by the authors that this performance statistic is a variable that is not only dependent on the system used but is heavily dependent on the type of biometric trait used as well. The research carried out has proven to show that fingerprint recognition technology has been found to have a low FAR value of 0.1% indicating that it is highly capable of being able to effectively distinguish between genuine users and frauds with high accuracy; while on the other hand, face recognition technology has had a relatively higher FAR value of 1%, which is attributable to the fact that faces; the biometric subject to being scanned, is contingent on and can be affected by several factors such as variations in pose, and expression amongst many others during the scan.

Therefore, in order to tackle this issue and greatly improve the performance of the biometric systems considered for use, researchers have suggested the usage of a multi-modal biometric system, in which two or more biometric traits have been used in combination. This method of recognition has been found to conclusively and significantly improve the accuracy of the system whilst keeping its FAR value to a minimum, solely due to the fact that the different traits used, impeccably complement each other in terms of their individual strengths and weaknesses. For instance, a trial integrating the use of both face and iris recognition technology together have been found to produce a resulting FAR value of 0.0004%, which is remarkably lower than either of the two traits have ever been when used in separation.

Adding to this, the authors Abdelwhab and Viriri (2018), have prominently stated in their research that the performance of any biometric system taken into consideration is strongly influenced by many various other factors such as the quality of the biometric samples collected during both registration and voting periods; as well as the types of different sensors used by each biometric system; along with the nature of the matching algorithm integrated into the authentication process of the system. As a result researchers have started to shift their focus on the topic, more towards enhancing and refining the development of better sensors and matching algorithms in order to boost the accuracy and reliability of these biometric systems.

Whilst Abdelwhab and Viriri (2018) provided an extensive survey regarding the usage of soft biometrics for human identification and probed deeper into the performance aspect of the various related biometric systems out there, the literature produced did indeed have a few gaps worth addressing. One such gap is the fact that the survey was solely focused on soft biometrics ; which by definition, are the physical or behavioral characteristics of a person which can be used for identification, however, are not unique to any one individual. While the survey did touch up on some hard biometrics, namely: fingerprint, facial and iris recognition technology; more detailed exchanges pertaining to the performance of these systems are required. Another gap that has been found in the literature, is the lack of extensive coverage on the environmental factors and the impact that they may have on the performance of the biometric systems reviewed. Such examples are inclusive of, but not limited to the changes in lighting, background and weather that result from the many different times and states of day; which may potentially affect the accuracy of systems using facial recognition technology which had not been dealt with in detail.

Also, the research made no mention of the potential ethical and privacy concerns applicable to systems utilizing biometric recognition tools. Due to the nature of the data collected biometric data has been classified as a highly sensitive type of data, which in the wrong hands, could be misused in several ways, leading to identity theft and other privacy breaches as well. Therefore, it is essential to handle these concerns with the utmost care in order to ensure that these biometric systems and the information they collect is used responsibly and ethically while conforming to the laws of the countries that they may be implemented in.

Finally, the survey only briefly touched upon the potential limitations and challenges affiliated with the systems that use biometric recognition technology and failed to go into further detail regarding the possibility of spoofing attacks. This is where an impostor tries and makes attempts at fooling and tricking the system into falsely accepting them as genuine users by presenting fake biometric data to it.

Overall, the survey conducted by Abdelwhab and Viriri (2018), on the performance of biometric systems provides indispensable support to the existing literature on the topic. Their insights regarding these systems help in understanding that the performance of biometric systems vary greatly depending on the type of biometric traits used for identification. These findings have then skillfully been used to explore the many various strategies developed by many other researchers who have prioritized the improvement of accuracy and minimizing the FAR even further. This process has been stated by the authors to become even less daunting as technological advancements keep frequenting; increasing the likeliness of these systems becoming even more reliable as their accuracy increases altogether making them an increasingly popular tool for human identification.

Gaps in the literature provided by Abdelwhab and Viriri (2018), have been identified in order to guide future research towards efficiently addressing these gaps. Further investigation into this topic of soft biometrics for human identification could involve the use of a biometric system utilizing soft and hard biometric recognition technologies individually, with the whole process as well as the FARs of these systems documented as a performance indicator. These results could then be compared against the performance of the integration of these two different biometric recognition technologies, together in a single system that identifies users according to both their soft and hard biometrics in combination. This research could then be performed using different trait combinations in order to check for the most effective trait combination with the lowest FAR; which in turn would be an indicator of the highest in performance and accordingly aid in reproducing a system with the highest accuracy.

### 2.3 Ellena, K. and Petrov, G. (2018). *Cybersecurity in Elections Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies.*

Secondly, the research conducted by Ellena and Petrov (2018) is heavily focused on the context of cybersecurity in elections and offers a Holistic Exposure and Adaptation Testing (HEAT) process to effectively identify and mitigate these risks. The authors identify the underlying problem to be directly linked to the constant progression in the field of technological advancements and enhancements, arguing that this is where the issue stems from. Moreover, they state that with each step further towards the digital age, the world becomes more interconnected, and therefore the risks associated with cyber threats to the electoral processes have also increased. As a result the urgency for Electoral Management Bodies (EMBs) to implement extensively strong and resilient cybersecurity systems and protocols to safeguard the integrity and legitimacy of the electoral process cannot be overstated. It is of vital importance that these measures are in place to ensure the credibility and authenticity of the election.

Hence why the proposed HEAT process has been carefully formulated by the authors, to address the many various aspects of cybersecurity in detailed steps; inclusive of threat modeling, vulnerability assessment, penetration testing, and incident response planning. The process is then explained to aid EMBs in the swift identification of potential cyber threats; careful assessment of the vulnerabilities of the current systems in place; as well as effectively test the system's response rate, as a measure of its ability to respond to such cyber incidents. The authors have greatly emphasized that the HEAT process, if put into use, must be carried out in a holistic manner in order to productively be able to reap the most benefits from its coverage, which takes into account all influential aspects of the electoral process, involving the technological, organizational, and human factors associated with the elections.

However, the proposed cybersecurity framework is not without its flaws as acknowledged by Ellena and Petrov (2018), for they have discussed the many challenges linked with the implementation of the HEAT process, solely pertaining to the lack of technical expertise and several resources amongst EMBs themselves; the need for collaboration between various stakeholders to make up for the lack of resources; and the difficulty of conducting such critical tests in a realistic and controlled environment where vulnerabilities could be easily identified and ultimately mitigated prior to the actual deployment of the system, where an exploitation could cost far more than the process itself. Regardless of the many issues the process is faced with, the authors still argue for their HEAT process, reassuring that their proposed framework is guaranteed to be a priceless tool that is dedicated to actively help refine an EMB's cybersecurity posture whilst thoroughly and conclusively mitigating the countless risks affiliated with cyber threats to the greatest extent.

Although, Ellena and Petrov (2018) presented a comprehensive framework, it is important to acknowledge that even well-researched topics can have areas that require further attention. As such, there are a few minor gaps in the literature that may be worth looking into for further consideration due to some of them being under-explored aspects of the topic that have not yet been discussed by the authors themselves; and could prove useful for a probable full-scale implementation of the HEAT process.

The first gap in the literature is solely due to the generalization of the entire framework for any EMB regardless, to make use of - the political and social context in which cybersecurity measures are implemented. With this jack-of-all-trades approach, the authors refrain from going into further detail in these areas as different countries are governed and operate by different laws; for example, potential issues such as the concern of the general public's trust and confidence in the country's electoral processes or the issue of political interference with the entire electoral process. If any attempt was made to discuss these issues in detail, it would prove to be inapplicable to one country or the other and so on and so forth.

Moreover, the lack of any real test data showcasing the effectiveness of the HEAT process in an actual election scenario has not been mentioned or discussed in detailed and is another potential gap in the literature provided by Ellena and Petrov (2018). While a detailed cybersecurity framework has been designed for the process there has been no conversation whatsoever on the results of the system's performance and effectiveness in a test scenario simulating the electoral processes, let alone a real-world implementation of the approach by any EMB. This may be due to the fact that the process was developed based off of conceptual theory, which would seem highly effective if put into practice, however, possibly due to the lack of the publication's reach, the process, regardless of how effective it potentially could be; might not have been implemented by EMBs who may have been willing to test the framework out for themselves. In order to ensure the framework is put into use, a collaboration with an EMB capable of carrying out the process to its last detail could be in order, with the results and findings documented every step of the way; which in turn would enlighten other EMBs, as well as help promote the reliability of the framework with its effectiveness exhibited in a more tangible form of data; as a measurable statistic provided as proof of trial. These findings could prove key to evaluating the worth of the HEAT process as it would generate interest and let other EMBs already interested in it to determine whether implementing it would be worth its costs.

Finally, the research conducted is lacking in a review of the specifics regarding the various types of cyber threats and attacks that exist and have the potential to pose a significant challenge that an EMB may have to face and overcome which is a separate potential gap in the literature. The authors have not gone into detail on this topic as well, as the cyber threat index keeps expanding owing to the continued progression of modernization in the digital age. On the contrary, probably because certain threats would be inapplicable to certain countries, (for ex: Third World Countries), where the implementation of technological advancements have not been prioritized as much. Based of the saying "prevention is better than cure", a comprehensive guide explaining these threats; the vulnerabilities exploited by each threat; and the effects of each in detail; would help EMBs understand the severity of these threats, and how to avoid falling victim to such threats which in turn would have them better prepared in advance to defend against these cyber attacks.



Overall, Ellena and Petrov's (2018) article provides an invaluable contribution and insight to the existing literature regarding the countless cybersecurity issues and concerns linked to the electoral processes. The proposed HEAT process constructed by the authors is a well-thought-out, methodical and practical framework allowing for EMBs worldwide to accurately and efficiently assess and enhance their cybersecurity posture. Furthermore the authors' emphasis on a uniquely holistic approach accounts for all aspects of the election process which is particularly noteworthy as it highlights the importance of addressing not only technological but also organizational and human factors in ensuring the security of electoral processes.

There are gaps in the literature that have been identified to guide future research on this topic to focus on testing the conceptualized HEAT process using simulation and modeling techniques. If the implemented framework is proven to effectively identify and mitigate risks in these simulations; the focus of the research should then shift to incorporating it into an electoral process in the real world for thorough testing of the discussed cybersecurity framework alongside heavy documentation of the entire process; with the results compared against the electoral process prior to the implementation of the HEAT process test, in order to determine its effectiveness and feasibility even further.

## 2.4 Krimmer, R., Volkamer, M., Cortier, V., Gore, R. and Hapsara, M., (2018). *Electronic Voting*.

Thirdly, according to Krimmer et al. (2018), the general implementation of any sort of electronic voting system comes with its own unique set of opportunities and challenges to overcome as well; with the research produced, carefully providing a detailed overview of electronic voting systems in general. It has been highlighted that one of the key deciding factors concerning the implementation of any such electronic voting system is the costs associated with it more than most. These cost as discussed further by Krimmer et al. (2018), have been broken down into two very broad categories namely, direct and indirect costs.

The direct costs mentioned before by the authors refer to those incurred in the purchase, installation, and maintenance stages of the electronic voting system considered for implementation. This is further simplified to be inclusive of the obvious basic costs that involve the purchasing of the necessary hardware and software required to run the desired electronic voting system; the costs that come with training staff to bridge the knowledge gap that will help them to swiftly adapt to the implemented system and be able to efficiently use the system as intended; and the unavoidable expenses linked to the constant upgrading of the system and maintenance that it should, and will be subject to for the continued use of the installed system. The paper by Krimmer et al. (2018) also indicates that the costs discussed above can greatly vary, mainly attributing to the type of electronic voting system considered for implementation; adding that the level of customization required to suit the needs of the electoral management bodies that intend to use it; and the specific voting environment the system is to be implemented in, can cause these direct costs to differ accordingly. An example regarding contextual settings that displays this best, is the costs of implementation incorporated with a system for a small community, against one purposed for a much larger city or state, where the costs could be relatively low as opposed to much higher respectively.

Indirect costs, on the other hand, are said to refer to those that concern the voting process as a whole and how it will be affected, subsequent to the implementation of an electronic voting system and the many changes it brings with it. As per the authors, these costs comprise of any and every concern regarding the electronic voting system that must be addressed and is inclusive of, but not limited to; its security and accuracy, along with several other potential legal issues that may arise as a result of the change as well. Such costs have been deemed to be one of the most problematic, in terms of difficulty to predict, as they are dependent on several varied factors that can easily be influenced such as the complexity of the system; the level of public trust in the electoral system; the gap that needs to be bridged between the public's understanding of the system and the electronic voting system itself; and the political environment in which the system is being implemented.

Despite the many challenges that these systems constantly face the potential benefits that they offer are far greater as mentioned in the piece by Krimmer et al. (2018), stating that electronic voting systems aid in successfully enhancing the voting process by substantially increasing the efficiency and accuracy of the voting process, whilst effectively mitigating and minimizing the likelihood of human error and tampering in the voting process whilst providing a more user-friendly and accessible voting experience for voters with disabilities or limited mobility.

As detailed as the research by Krimmer et al. (2018) is, there are a few gaps in the literature that are worth taking into consideration regarding the inspection into the many costs associated with the implementation of electronic voting systems; with the first being the lack of a detailed cost analysis having been conducted for the specific types of electronic voting systems. While the general cost estimations for the hardware and software required; staff training necessary for implementation; and system maintenance aspects of electronic voting systems in general have been discussed in detail, the authors have missed out on the topic of costs correlating to specific types of systems such as biometric voting systems or internet voting systems. Therefore, further research into this topic will be necessary to uncover these costs so that they can be compared against more traditional voting systems in order to assess the financial efficiency of using one system over the other.

Adding to this, is another gap in the literature, regarding the lack of in-depth information on the long-term costs linked to the implementation of any electronic voting system. Although the authors have thoroughly discussed the upfront costs associated with the initial stages of implementing an electronic voting system, such as the purchasing and installation of the desired electronic voting system; they have failed to provide adequate data on the long term costs concerning the constant upgrading and maintenance that these systems will be subject to. Thus, further research conducted into this area would prove to be highly useful in assessing and determining the costs associated with the implementation of electronic voting systems and how they compare to the traditional method of paper-based voting systems.

Finally, the study produced by Krimmer et al. (2018) fails to explore the costs required to address the many potential security concerns that come with the implementation of an electronic voting system. Despite only touching the surface of the topic, the authors fail to delve deeper into the estimations of the indirect costs required to address the many potential security issues and concerns that may form around the implemented system's accuracy and reliability. This in turn, would encouragingly merit further investigation in order to be able to effectively assess the costs of implementing powerful security measures for these electronic voting systems and then determine how these costs would compare against the potential risks associated with these systems as well.

Overall, the article by Krimmer et al. (2018) provides significant input towards the existing literature of the various cost analyses performed on electronic voting systems in general, offering fresh insights and perspectives into the topic reviewed. The authors have found that these systems, when implemented, will consist of great costs, both direct and indirect, but continue to argue for the implementation of these electronic voting systems; elaborating that the benefits these new systems will bring, can cancel out and justify these costs. They further explain that in order to relish the basic benefits of increased efficiency and accuracy amongst many others in the voting process; careful planning and a thorough understanding of the requirements and challenges of the voting environment must be in order, to ensure that the implementation costs are minimized and the electronic voting system's benefits are maximized.

A few gaps in the literature have been identified to guide future research on the topic of costs, in relation to the implementation of electronic voting systems. Future research on this topic should focus on gathering the cost specifics to the different types of globally tried and tested systems and then should be compared to the costs of the traditional system that was in place prior to its implementation. This information should be documented and discussed in detail, with additional supplementary research then comparing this data to how the implementation of each of the different systems differed across other countries that implemented the same type of electronic voting system; keeping in mind the differences accompanying maintenance cost specifics and many various other factors influencing the costs associated with these systems as well; such as, unexpected breakdown costs for example in order to conclusively be able to determine the cost effectiveness of electronic voting systems as a whole.

## 2.5 CONCLUSION

In conclusion, this literature review has clearly demonstrated the increasing relevance and potential of biometric voting systems. The findings from the studies evaluated, indicate that this technology offers a viable solution, that if implemented properly has the ability to meticulously address the security and performance concerns that keep emerging regarding these systems; whilst simultaneously being able to successfully keep costs to an acceptable bare minimum. The studied research features the many advancements that have been made in regards to recognition algorithms, hardware and software technologies, all of which contribute to the development of robust and scalable biometric voting systems. However it is very important to acknowledge the existing challenges, including concerns related to the privacy of data, accuracy of the system and the implementation of these systems themselves. Future research should focus on addressing these limitations and conducting comprehensive pilot studies that validate the effectiveness and feasibility of these biometric voting systems. Ultimately, the successful integration of effective biometric solutions in the voting process has the potential to strengthen democratic practices and instill greater confidence in electoral outcomes.

## 3 | REQUIREMENTS ANALYSIS

### 3.1 FUNCTIONAL REQUIREMENTS

#### **Handprint Registration Algorithm - Handprint Scanner Software**

Should be able to scan and read voter handprints prior to the election at a high quality and seamlessly be able to integrate with the registration logic to save the original handprint and create a copy of the original handprint; separate the copied handprint image into individual fingerprint images that will be assigned to each corresponding finger, alongside details identifying which print belongs to which finger, into the handprint database under the rightful owner's NIC and other details.

#### **Handprint Verification Algorithm - Handprint Scanner Software**

Should be able to scan and read voter handprints regardless of quality on the day the election is live, and swiftly and effectively be able to search amongst the previously registered original fingerprint and handprint images in the handprint database using the matching algorithm, that assigns key points to both the input fingerprint/handprint and each original being searched against within the database whilst assigning similarity scores to all files and retrieving the original fingerprint/handprint file with the highest match score as the best match in the entire database alongside the rightful owner's NIC and other details.

#### **System Administrator Privileges - Admin Dashboard**

Provides control over all features the biometric handprint election management system consists of such as registering users and the setting up of other administrator accounts, creating elections and adding election candidates, viewing election history and real-time vote casting history as well as live results.

### **Candidate Display - Voter Panel**

Voters must be able to see who they will be voting for therefore pictures of each candidate must be displayed appropriately with a short description consisting of their respective parties alongside the candidate number assigned to them by the Election Commission.

### **Biometric Login and Registration - User Login and Registration**

Administration staff must be able to register voters using their handprints for a voting account exclusive to their NIC. Once registered, voters must be able to log in to their newly created account to cast their vote using any of their registered fingerprints come election time.

### **Regular Login and Registration - User Login and Registration**

An option created for the differently-abled, in order to prevent vote exclusion; and for emergency use in the rare case that the handprint scanner malfunctions or breaks down; that does not require handprints. This is an exclusive option that is only permissible by administration staff to enable if the circumstances deem it necessary and will be disabled by default for those that do not fit this category.

### **Biometric Vote Casting - Voter Panel**

Voters must be able to cast and lock their vote in for their desired election candidate by confirming their choice using any of their pre-registered fingerprint/handprints. After voting, voters will not be able to vote again for other candidates and an image assuring their vote has been cast will appear on the candidate they voted for.

### **Regular Vote Casting - Voter Panel**

An option created for the differently-abled, in order to prevent vote exclusion; and for emergency use in the rare case that the handprint scanner malfunctions or breaks down; that does not require handprints. This is an exclusive option that is only permissible by administration staff to enable if the circumstances deem it necessary and will be disabled by default for those that do not fit this category.

### **Live Vote Count - Voter Panel**

Voters should be able to see the live accumulated vote totals for each candidate at all times during their vote casting period; both prior to voting and after having cast and confirmed their vote.

## 3.2 NON-FUNCTIONAL REQUIREMENTS

**Scalability** - The system should be capable of handling increased user load and data storage requirements as implementation expands in order to accommodate a growing number of voters and polling stations without compromising performance.

**Security** - The system should provide robust security measures to protect the integrity and confidentiality of voter information and comply with privacy regulations in order to protect the personal data of voters and prevent unauthorized access or tampering, thus safeguarding voter privacy and rights.

**Performance** - The system should be able to process a large number of handprint scans within an acceptable time frame during peak voting periods. It should handle simultaneous requests efficiently and maintain responsiveness to avoid delays or disruptions.

**Maintainability** - The system should be easily maintainable and should be able to be quickly, easily and safely updated or fixed by administration staff themselves with minimal training.

**Accountability** - The system should keep track of all interactions including the identification, verification and vote casting processes. This allows for post-election analysis and ensures accountability of system users.

**Fault Tolerance** - The system should be resilient to failures, both in hardware and software components, to ensure continuous operation during the election period. It should have backup systems in place to minimize disruptions during elections.

**Regulatory Compliance** - The system should adhere to the relevant legal and regulatory requirements, such as data privacy and protection laws; and election regulations. Compliance with industry standards and best practices is essential to maintain public trust in the election process.



### 3.3 PROJECT CONSTRAINTS

**Time** - One of the key constraints of this project is the limited time there is available to complete the project to its desired state. In order to make sure that the project reaches this stage well before the deadline a project timeline with realistic timescales are ensured for each task that must be completed in order to ensure the successful completion of this project to its desired state.

**Knowledge** - Is critical to the understanding of, and the steady advancement of the project that has been undertaken. At the time of taking on this project however, it is undeniable that the knowledge required for developing a fully fledged system to the extent required by the assessment is lacking. However, invaluable resources such as Google Scholar and several others that are accessible on the Internet help produce guidance and insight through various referential solutions on how to successfully complete the project.

**Resources** - Are also greatly limited for the completion of this project. The project has no funding to it for the acquisition of resources therefore completion is limited exclusively to the prototype stage which too was only achievable due to the Internet as a resource to help with the project completion.

**Situational Circumstances** - Ever since the state of pandemic worldwide back in late 2019, the uncertainty of a COVID-19 resurgence prevented gatherings from taking place even three years since the incident first occurred and this was inclusive of supervisor meetings and affected research data gathering methods through means of focus groups as well. Therefore, we were left to heavily rely on self-conducted extensive research and other alternatives in order to complete the project with the limited time there was available.

### 3.4 KEY FACTORS INFLUENCING THE PROJECT

#### **Cost Effectiveness**

Given the extremely high costs of the currently used paper based election system a cheaper alternative solution negating the need for any paper is proposed cutting costs down to a minimum to relieve the country from its economic crisis.

#### **Convenience**

The traditional voting process is lengthy and requires hours for a single voter to cast their vote. The proposed solution is simplified to a three step process of logging in, casting a vote, and logging out; therefore greatly cutting down on time spent in line for voters to cast their vote.

#### **Reliability**

The machine planned for use in fingerprint/handprint matching is programmed to find matches to the pre-registered original regardless of how altered voters' input fingerprints/handprints are therefore assuring users of its reliability at all times during the election period.

#### **Security**

The voting process is heavily secured using handprint verification and data encryption protocols to prevent the misuse of data, negate multiple vote casting instances and minimize the likeliness of vote tampering.








#### **Usability**

The system is designed to be user-friendly, ensuring that election officials and staff can easily operate the handprint biometric recognition technology with minimal training.







#### **Transparency**

The votes are tallied as votes are cast allowing for people to be assured of the process and fully trust it

### 3.5 RESOURCES AND MATERIALS USED

- Software Used -
-  Draw.io  
Version 21.4.0
  -  Google Chrome  
Version 114.0.5735.134
  -  Microsoft Visual Studio Code  
Version 1.64.2
  -  Microsoft Project Professional 2013  
Version 15.0.4420.1017
  -  PyCharm Community Edition 2023.1  
Version 231.8109.197
  -  WPS Office  
Version 11.2.0.10323
  -  XAMPP  
Version 8.2.4-0

Hardware Used - HP Laptop  
Windows 10 Home  
Intel Core i5-7200UCPU @ 2.50 GHz 2.70 GHz  
8GB RAM, 1TB HDD

- Languages Used -
-  HTML5
  -  CSS3
  -  Bootstrap
  -  JavaScript / JQuery
  -  PHP
  -  MySQLi

## 4 | METHODOLOGY

### 4.1 RESEARCH PHILOSOPHY AND APPROACH

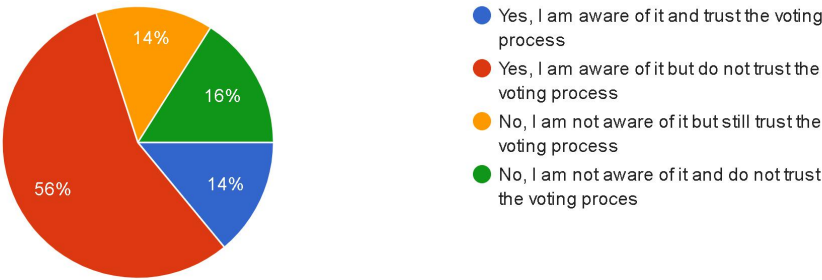
This research adopted a philosophy of theoretical pragmatism in a mixed methods approach allowing for the integration of both quantitative and qualitative research. The quantitative data gathered provided an overall understanding of voter satisfaction with the current paper-based voting system and process; alongside what concerns they had and changes they would like to see if the existing system were to be replaced with a biometric handprint voting system. Qualitative data was used to gain insights into various other biometric voting systems and how they were implemented successfully into the election process. This philosophy acknowledged the need to combine objective analysis with subjective insights to gain a holistic view of the research topic.

### 4.2 DATA COLLECTION AND SAMPLING METHODS

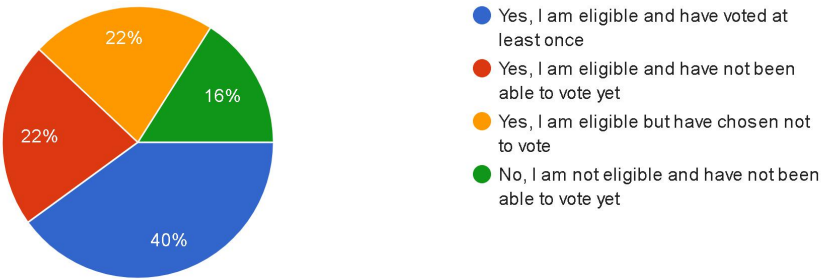
Random sampling was used to select participants for this study, with close-ended questionnaires sent out to voters at random from various backgrounds included, to collect a sample size of 50 responses. The selection criteria ensured that the participants were either citizens of Sri Lanka or present in the country during an election, and had general ideas of what biometric voting systems were and had achieved in election processes in other countries. However, due to the limitations imposed by the aftermath of the pandemic, the data collection methods primarily consisted of questionnaires only. Focus groups were initially planned but were not feasible given the situational circumstances. Questionnaires were chosen as they allowed for more remote participation, enabling people from anywhere to participate conveniently.

The following data is representative of the responses obtained through the conducted questionnaire:

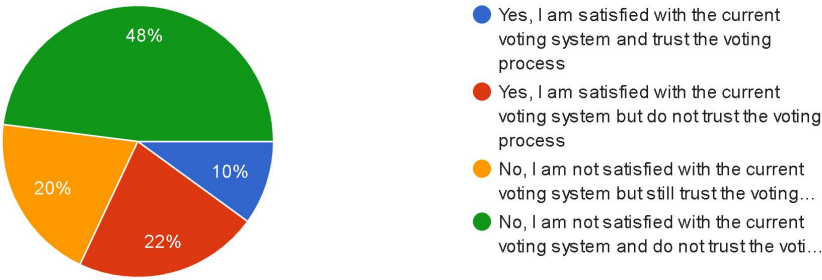
Are you aware of and trust the voting process?  
50 responses



Are you eligible to vote and have you voted yet?  
50 responses

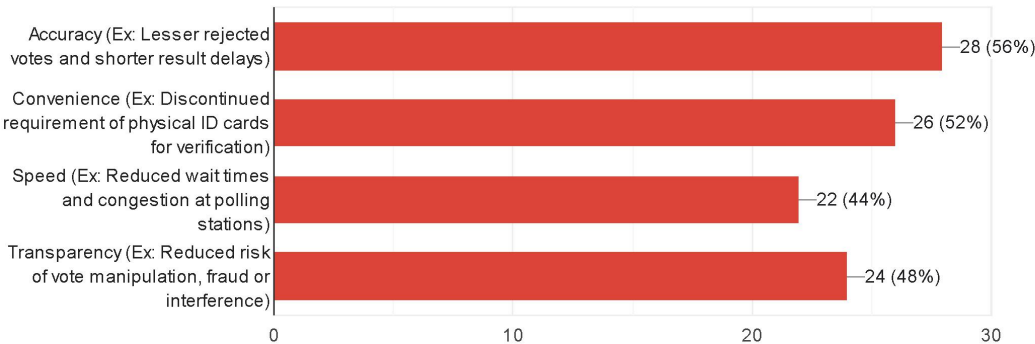


Are you satisfied with the current paper-based voting system and the process behind casting a vote?  
50 responses



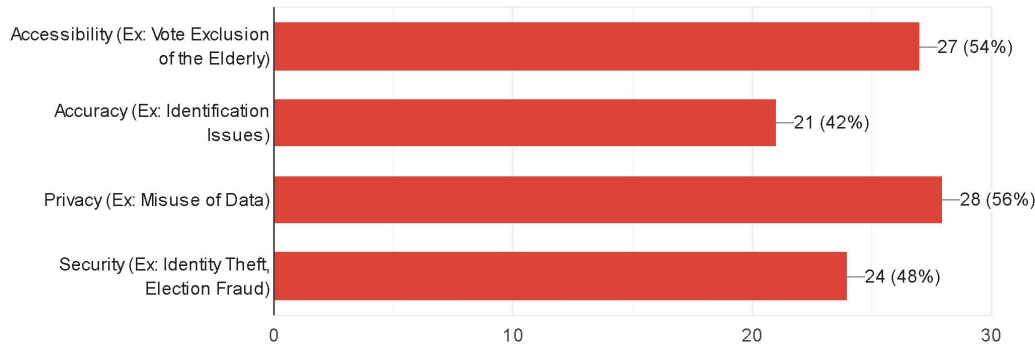
What would you most look forward to if there was a shift from the traditional paper-based voting system to a digital biometric voting system? (Select up to 2 options only)

50 responses



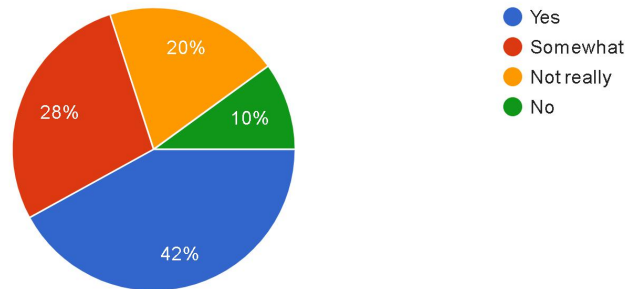
Regardless of the current system's flaws; what are your biggest concerns regarding a shift from the traditional paper-based voting system to a digital biometric voting system? (Select up to 2 options only)

50 responses



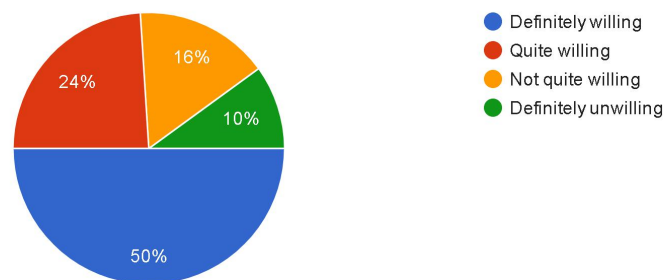
In your opinion do the pros outweigh the cons that come with the change in systems?

50 responses



How willing are you to a complete change of systems from the traditional paper-based voting system to a digital biometric voting system?

50 responses



The above survey indicates that a majority of the people show general distrust and dissatisfaction towards the current use of the traditional paper-based voting system and would opt for a more trustworthy and reliable alternative that is both accurate and enhances the efficiency of the current electoral process.

The information gathered as shown earlier helped ensure that the system to be developed accommodated voter requirements; and also proved invaluable in making informed decisions regarding the development and designing of the finalized system's prototype.

### 4.3 ETHICAL CONSIDERATIONS AND LIMITATIONS

Several ethical considerations and limitations have been acknowledged in this study. Firstly, The research is specific to handprint and fingerprint biometrics only, and as a result may not be generally applicable to other systems optimizing different biometric traits such as facial features, iris patterns or vocal characteristics. Moreover, the study is entirely based on the usage of said system in the context of electoral processes, hence the requirements of the system may vary in comparison to the usage of the same system in other contexts. It is also important to note that self-reported data may introduce the possibility of bias or errors, and other external factors that may have been likely to have influenced voter responses during the pandemic aftermath, which may not be fully controlled for. Therefore, conducting research during this period presented several challenges in accessing data and engaging participants.



## 5 | SYSTEM DESIGN AND TESTING

### 5.1 INTRODUCTION TO THE SYSTEM

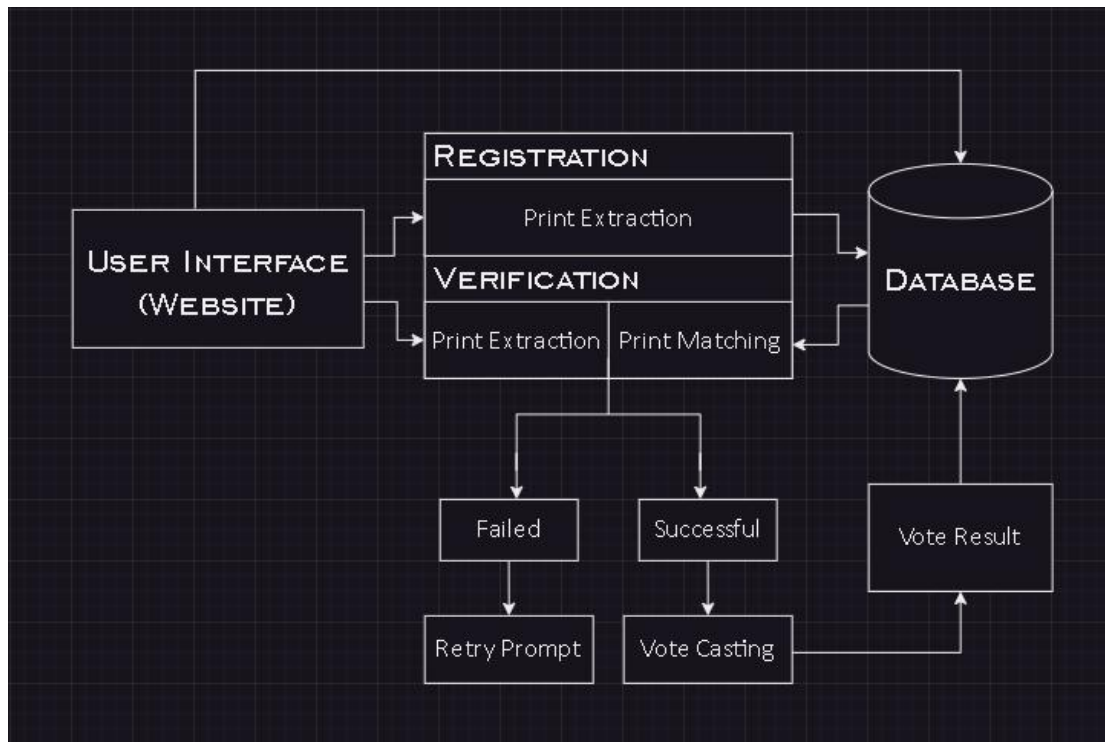
The proposed system comprises of two components that have been developed. The first being a prototype website for carrying out elections and the other being a heavily back-ended software purposed for a fingerprint/handprint scanner.

The website developed, contains the visual element of the system, better known as the user interface, on which prompts and other guidelines will be displayed to guide users through the new and unfamiliar voting process. Besides guidance the website will consist of a number of functionalities necessary in enabling the election commission to successfully manage the election processes, namely, the creation of elections, addition of candidates and monitoring of election results amongst many others.

As for the software developed; the scanner expected to host it, is intended to be one that comes without a Software Development Kit (SDK). Since the software has been developed to accommodate both the registration and verification processes, the purchasing of an SDK as well would be unnecessary. This adds to feasibility in terms of cost-effectiveness as these types of scanners are usually almost half their price when sold separately without the SDKs that they are usually bundled with. However, to not compromise on quality in the name of cost-effectiveness, the software developed will be thoroughly tested using a reliable sample set of data from a published database of sample fingerprints to rigorously test the ability of the matching algorithm developed for the verification process. Testing based on the registration process has been rendered highly improbable due to the unavailability and high costs associated with the acquisition of a fingerprint/handprint scanner at the time of conducting this research.

To assess the feasibility of the proposed system, both components will be heavily tested using simulations in which the effectiveness of the proposed solution will be evaluated.

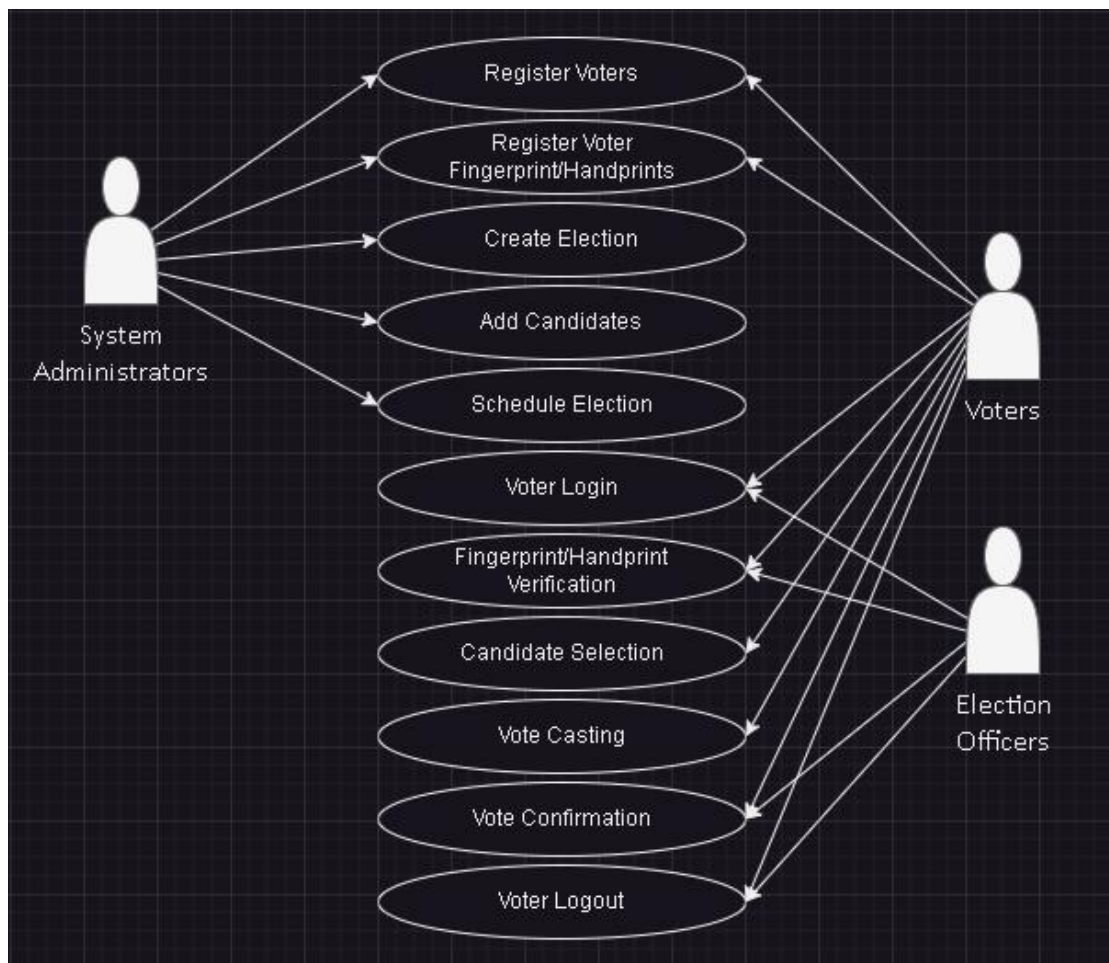
## 5.2 SYSTEM ARCHITECTURE



The aforementioned architecture is a simplistic low-level diagram which effectively showcases how the planned system is intended to work. The system consists of three main components, namely: the website to be developed which acts as the system's user interface and is responsible for capturing voter inputs; the fingerprint/handprint scanning machine comprising of the developed algorithms that were custom-made to accommodate both the registration and verification processes for validating voter identities; and finally the dedicated database which facilitates the creation and secure storage of voter information for the registration process by utilizing SHA-1 encryption methods for the protection of sensitive voter data; and the retrieval of voter information for the verification process. The arrows used to link each element displays the direction in which data flows between each unit, and indicates the exchange of information and dependencies that exist between subsystems. Following the architecture shown above, the primary objective of the system is to deliver a seamless voting experience that prioritizes accuracy, confidentiality, integrity and transparency of the voting process.

### 5.3 SYSTEM USE CASE

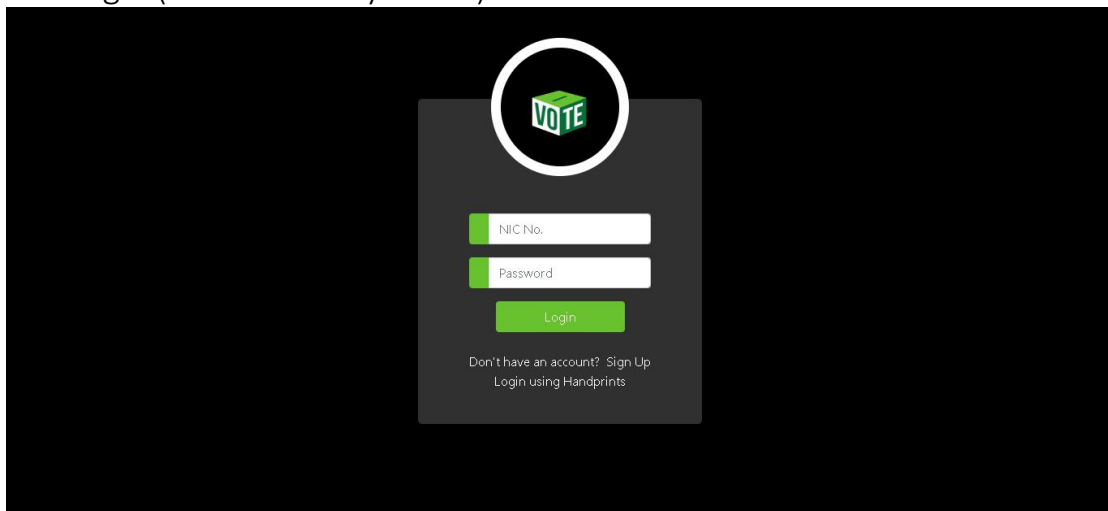
The diagram below is used to provide a visual representation of the system's functional requirements and the interactions that take place between its users. The use cases and functionalities of the system have been portrayed using ovals; with arrows connecting to specific actors at different stages of interaction; denoting which individuals are involved in each phase. The addition of election officials in certain use cases indicate their active involvement in the voting process as well, however, their involvement is limited solely to the assisting of users in processes usually unfamiliar to them. The following system use case diagram provides a clear and concise overview of the system's functionality, and has proven to be a beneficial aid in the performing of requirements analysis and the identification of system boundaries and dependencies.



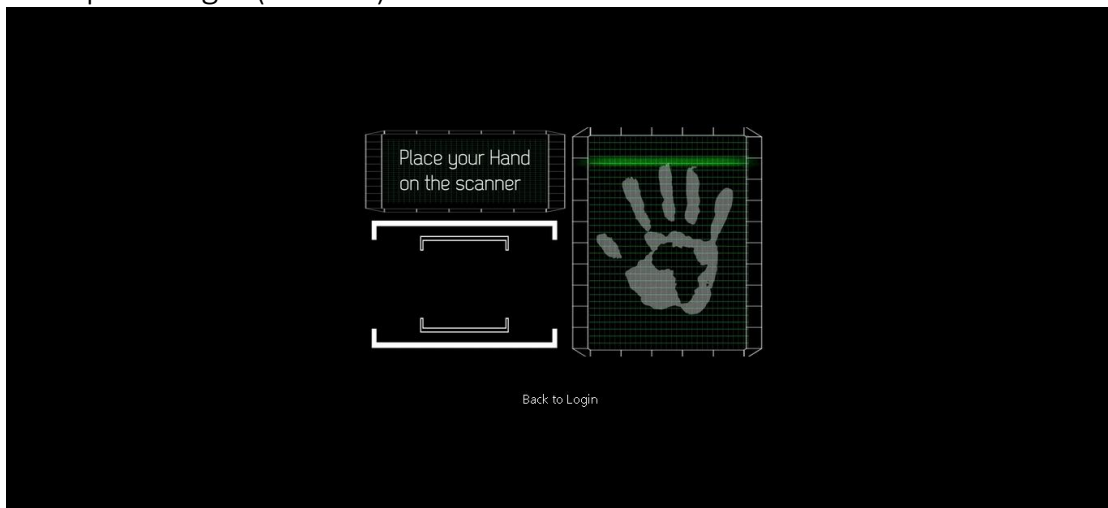
## 5.4 DEVELOPED PROTOTYPE

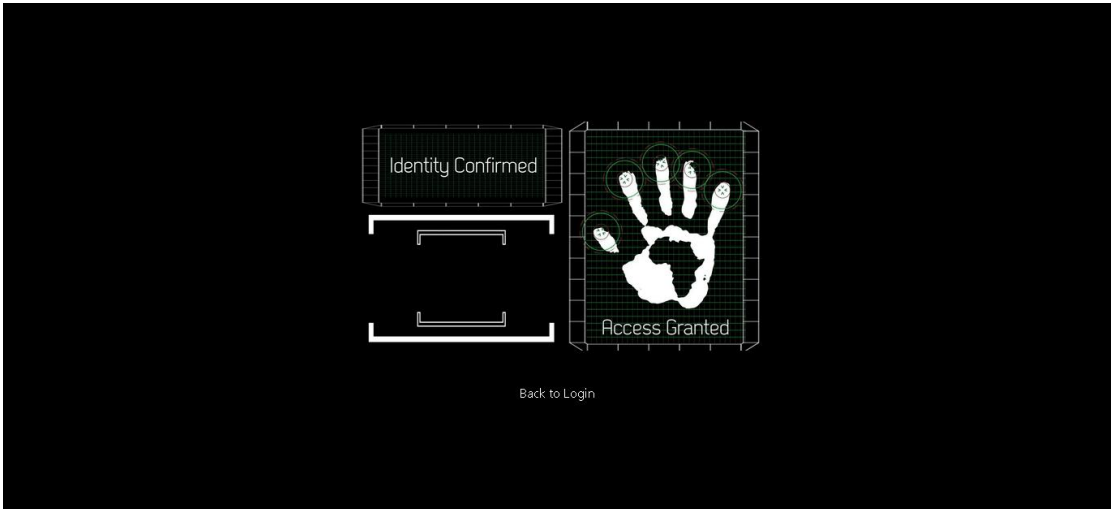
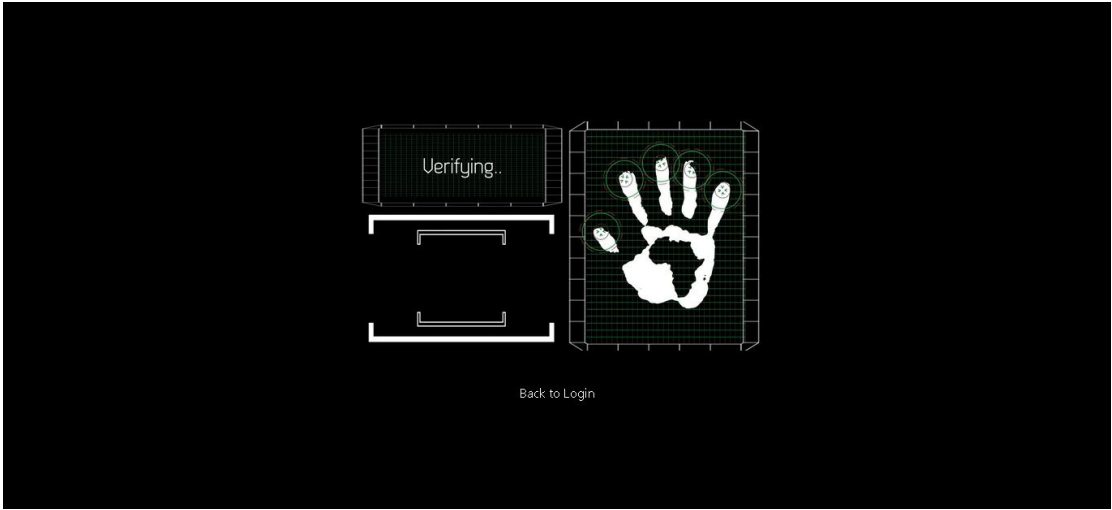
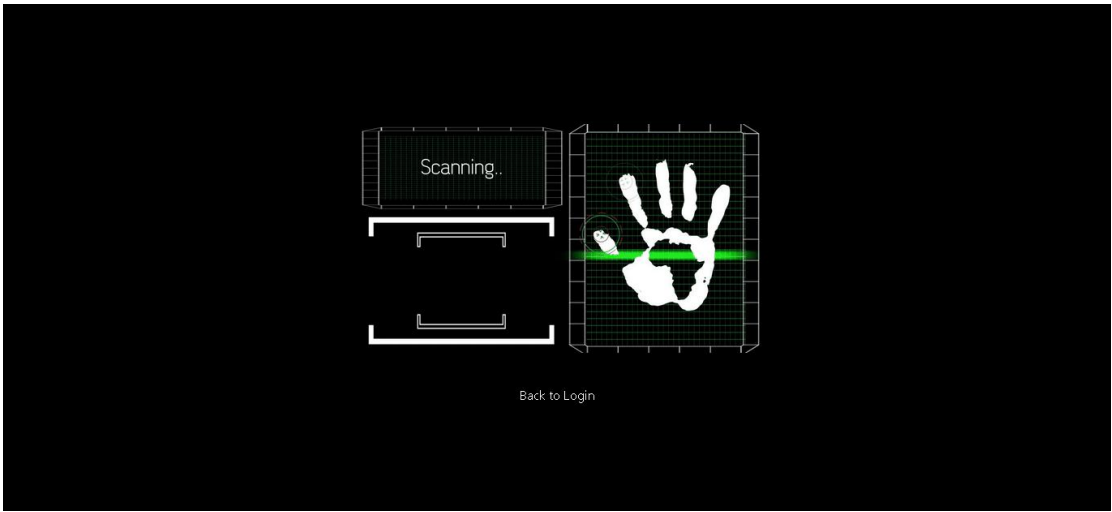
### 5.4.1 WEBSITE (GUI)

NIC Login (For differently-abled)

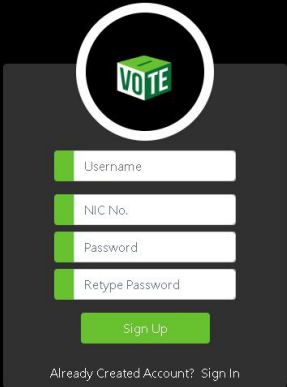


Handprint Login (Default)



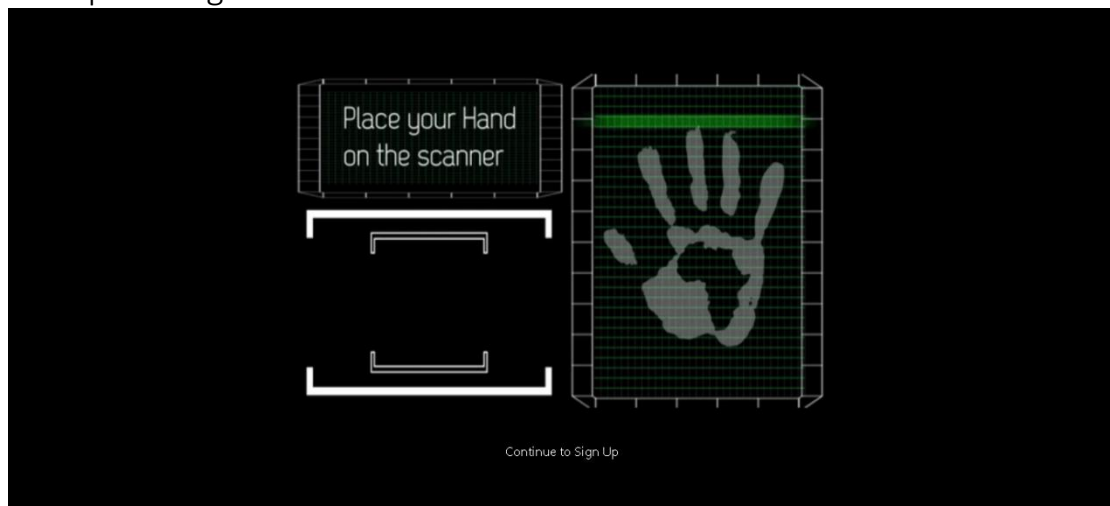


## Registration




The registration form is centered on a black background. At the top is a circular logo with a green cube containing the word 'VOTE' in white. Below the logo are four input fields, each with a green indicator bar on the left: 'Username', 'NIC No.', 'Password', and 'Retype Password'. A green 'Sign Up' button is positioned below these fields. At the bottom, the text 'Already Created Account? Sign In' is displayed.

## Handprint Registration



## Admin Dashboard

 **BIOMETRIC HANDPRINT VOTING SYSTEM** - Welcome Admin


Home Add Election Add Candidate Logout

### Election Results

S.No	Election Name	# Candidates	Starting Date	Ending Date	Status	Action
1	Presidential Elections	3	2023-06-16	2023-07-31	Active	<a href="#">View Results</a>
2	Parliamentary Elections	196	2020-04-25	2020-04-27	Expired	<a href="#">View Results</a>
3	Local Government Elections	340	2018-02-10	2018-02-12	Expired	<a href="#">View Results</a>

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved

## Election Addition

 **BIOMETRIC HANDPRINT VOTING SYSTEM** - Welcome Admin

Home Add Election Add Candidate Logout

### Add New Election

Election Topic

No. of Candidates

Starting Date

Ending Date


Add Election

### Election History

S.No	Election Name	# Candidates	Starting Date	Ending Date	Status	Action
1	Presidential Elections	3	2023-06-16	2023-07-31	Active	<a href="#">Edit</a> <a href="#">Delete</a>
2	Parliamentary Elections	196	2020-04-25	2020-04-27	Expired	<a href="#">Edit</a> <a href="#">Delete</a>
3	Local Government Elections	340	2018-02-10	2018-02-12	Expired	<a href="#">Edit</a> <a href="#">Delete</a>

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved

## Candidate Addition

 **BIOMETRIC HANDPRINT VOTING SYSTEM** - Welcome Admin

Home Add Election Add Candidate Logout

### Add New Candidates

Select Election




Candidate Name

Choose File No file chosen

Candidate Details


Add Candidate

### Candidate Details

S.No	Photo	Name	Details	Election	Action
1		Maithripala Sirisena	No.1, SLFP	Presidential Elections	<a href="#">Edit</a> <a href="#">Delete</a>
2		Mahinda Rajapaksa	No.2, SLPP	Presidential Elections	<a href="#">Edit</a> <a href="#">Delete</a>
3		Sajith Premadasa	No.3, SJB	Presidential Elections	<a href="#">Edit</a> <a href="#">Delete</a>

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved




## Voter Panel (Prior to Casting Vote)

 BIOMETRIC HANDPRINT VOTING SYSTEM - Welcome Test3

[Home](#) [Logout](#)


### Voter Panel

PRESIDENTIAL ELECTIONS

Photo	Candidate Details	# of Votes	Action
	<b>Maithripala Sirisena</b> No.1, SLFP	0	<a href="#">Vote</a>
	<b>Mahinda Rajapaksa</b> No.2, SLPP	2	<a href="#">Vote</a>
	<b>Sajith Premadasa</b> No.3, SJB	1	<a href="#">Vote</a>

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved




## Admin Results Display (Prior to Casting Vote)

 BIOMETRIC HANDPRINT VOTING SYSTEM - Welcome Admin

[Home](#) [Add Election](#) [Add Candidate](#) [Logout](#)

### Election Results

ELECTION TOPIC: PRESIDENTIAL ELECTIONS

Photo	Candidate Details	# of Votes
	<b>Maithripala Sirisena</b> No.1, SLFP	0
	<b>Mahinda Rajapaksa</b> No.2, SLPP	2
	<b>Sajith Premadasa</b> No.3, SJB	1


### Voting Details

S.No	Voter Name	NIC No	Voted For	Date Voted	Time of Vote
1	Test	000	Mahinda Rajapaksa	2023-06-16	09:47:46
2	Test1	111	Mahinda Rajapaksa	2023-06-16	09:53:38
3	Test2	222	Sajith Premadasa	2023-06-16	09:54:05

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved







## Voter Panel (Post to Casting Vote)

 BIOMETRIC HANDPRINT VOTING SYSTEM - Welcome Test3

Home Logout


### Voter Panel

ELECTION TOPIC: PRESIDENTIAL ELECTIONS

Photo	Candidate Details	# of Votes	Action
	<b>Maithripala Sirisena</b> No.1, SLFP	0	
	<b>Mahinda Rajapaksa</b> No.2, SLPP	3	
	<b>Sajith Premadasa</b> No.3, SJB	1	

Developed by Muthazz  
© Copyright 2023 - All Rights Reserved




## Admin Results Display (Post to Casting Vote)

 BIOMETRIC HANDPRINT VOTING SYSTEM - Welcome Admin

Home Add Election Add Candidate Logout

### Election Results

ELECTION TOPIC: PRESIDENTIAL ELECTIONS

Photo	Candidate Details	# of Votes
	<b>Maithripala Sirisena</b> No.1, SLFP	0
	<b>Mahinda Rajapaksa</b> No.2, SLPP	3
	<b>Sajith Premadasa</b> No.3, SJB	1

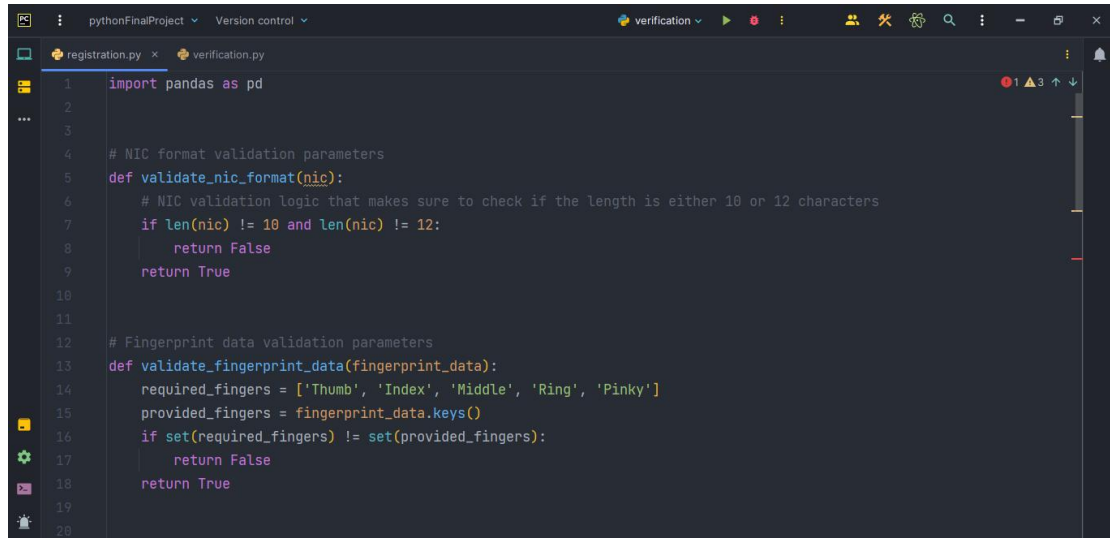
### Voting Details

S.No	Voter Name	NIC No	Voted For	Date Voted	Time of Vote
1	Test	000	Mahinda Rajapaksa	2023-06-16	09:47:46
2	Test1	111	Mahinda Rajapaksa	2023-06-16	09:53:38
3	Test2	222	Sajith Premadasa	2023-06-16	09:54:05
4	Test3	333	Mahinda Rajapaksa	2023-06-29	06:57:46

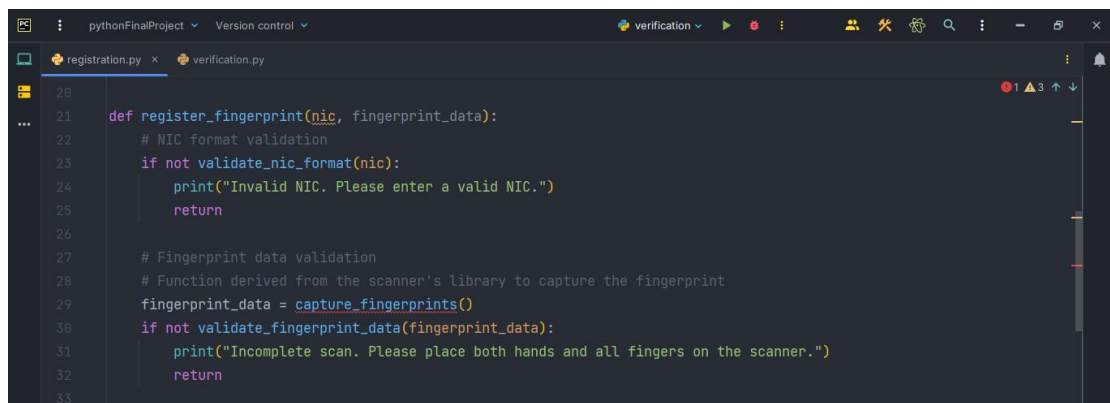
Developed by Muthazz  
© Copyright 2023 - All Rights Reserved

## 5.4.2 FINGER/HANDPRINT MATCHING ALGORITHM

### Registration Process

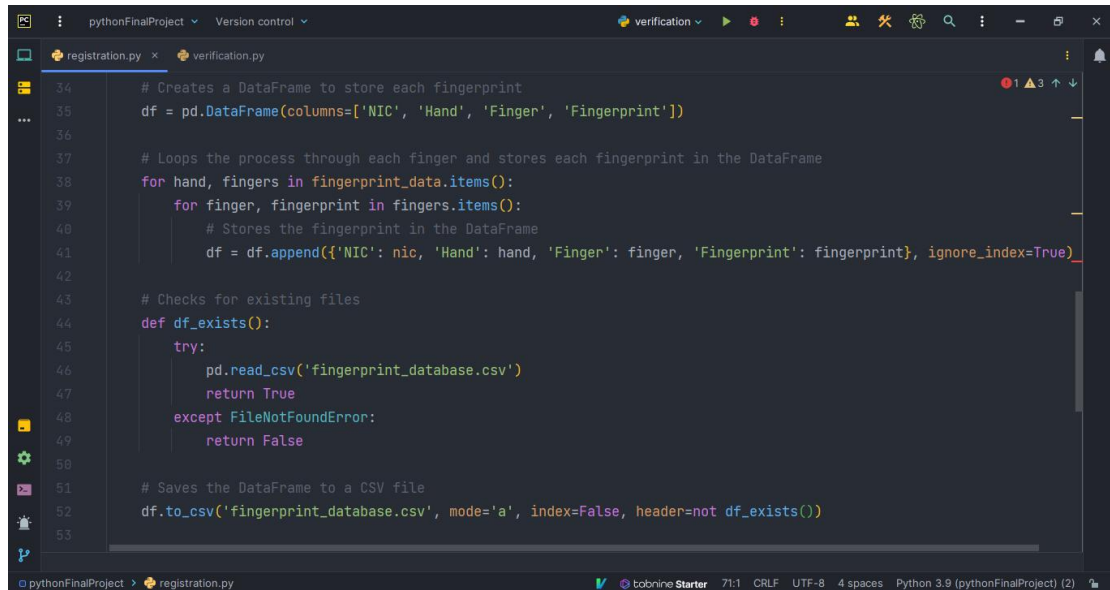


```
1 import pandas as pd
2
3
4 # NIC format validation parameters
5 def validate_nic_format(nic):
6     # NIC validation logic that makes sure to check if the length is either 10 or 12 characters
7     if len(nic) != 10 and len(nic) != 12:
8         return False
9     return True
10
11
12 # Fingerprint data validation parameters
13 def validate_fingerprint_data(fingerprint_data):
14     required_fingers = ['Thumb', 'Index', 'Middle', 'Ring', 'Pinky']
15     provided_fingers = fingerprint_data.keys()
16     if set(required_fingers) != set(provided_fingers):
17         return False
18     return True
19
20
```



```
20
21 def register_fingerprint(nic, fingerprint_data):
22     # NIC format validation
23     if not validate_nic_format(nic):
24         print("Invalid NIC. Please enter a valid NIC.")
25         return
26
27     # Fingerprint data validation
28     # Function derived from the scanner's library to capture the fingerprint
29     fingerprint_data = capture_fingerprints()
30     if not validate_fingerprint_data(fingerprint_data):
31         print("Incomplete scan. Please place both hands and all fingers on the scanner.")
32         return
33
```

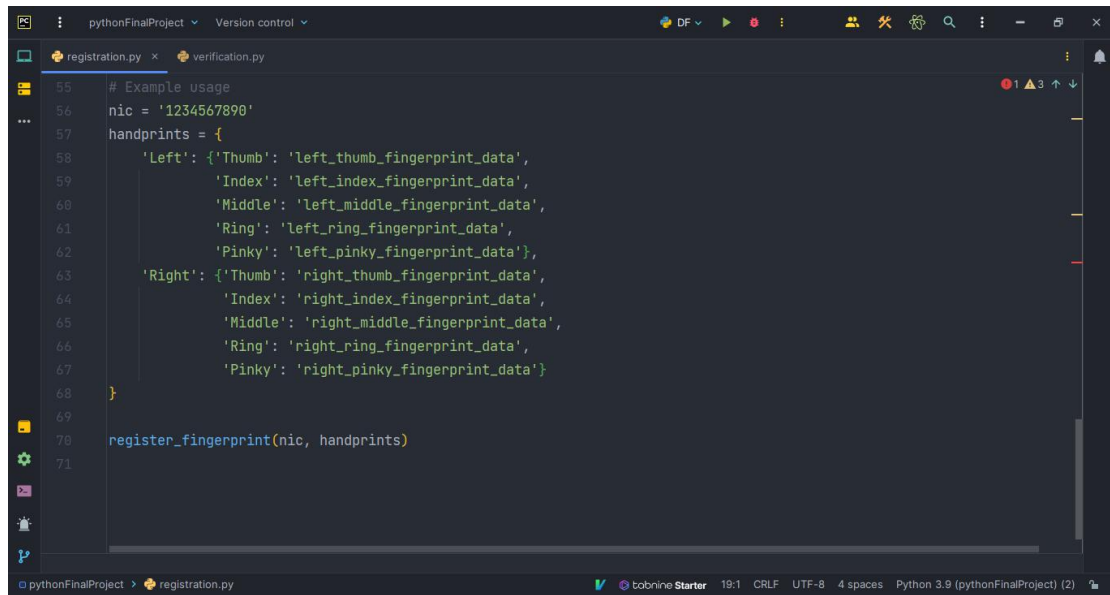
The system begins the registration of users by first validating the input NIC by using the 'validate\_nic\_format' function. This function checks if the NIC number has a length of either 10 or 12 characters. If the NIC format fails to meet these requirements it is deemed invalid, an error message is displayed, and the user is prompted to retry. Next, the system validates the fingerprint data input by users that is detected by the scanner using the 'validate\_fingerprint\_data' function. This function checks if the provided fingerprint data includes fingerprints for all fingers. If any of the required fingers are missing, the system displays an error message indicating that the fingerprint scan was incomplete and the user is prompted to try again.

A screenshot of a code editor window titled 'pythonFinalProject'. The editor shows two files: 'registration.py' and 'verification.py'. The 'registration.py' file is open, displaying Python code for creating a pandas DataFrame and saving it to a CSV file. The code includes comments and a loop for processing fingerprint data. The status bar at the bottom indicates the file is 'tobinone Starter' with settings like '71:1 CRLF UTF-8 4 spaces Python 3.9 (pythonFinalProject) (2)'.

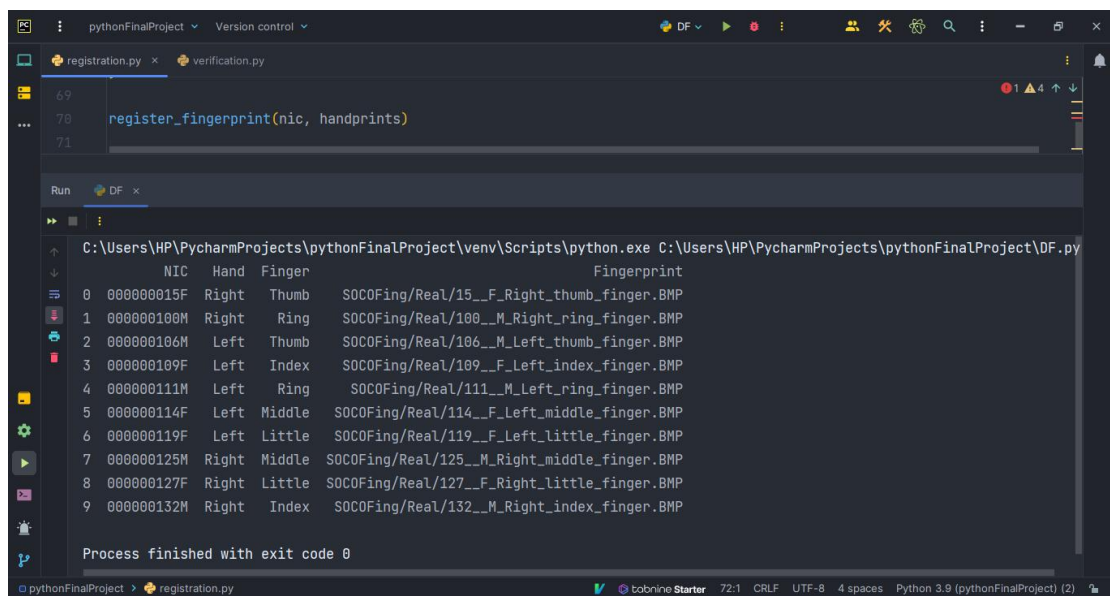
Assuming both the input NIC and fingerprint data pass the validations, the system proceeds to create a pandas DataFrame. This DataFrame serves as a structured table to store the fingerprint information, with four columns namely; 'NIC', 'Hand', 'Finger', and 'Fingerprint'. The system then enters a loop to iterate through each hand and respective finger provided as fingerprint data. Within the loop, it appends a new row to the DataFrame for each finger, alongside the voter's NIC number, hand, finger, and corresponding fingerprint data. This process ensures that all fingerprint data input for registration is stored in the DataFrame.

Additionally, the system includes a function called 'df\_exists' to check for the existence of a 'fingerprint\_database.csv' file using pandas' 'read\_csv' function. If the file is found, it returns True, indicating that the DataFrame should be appended without including the header. If the file is not found (raises a FileNotFoundError), it returns False, indicating that the DataFrame should include the header when saved.

Once the loop completes, the system saves the DataFrame to a CSV file named 'fingerprint\_database.csv'. The file is created if it doesn't exist, or appended to if it already exists. The mode parameter 'a' ensures that the data is appended to the file, while the index and header parameters are set accordingly to control the indexing and inclusion of column headers in the CSV file.



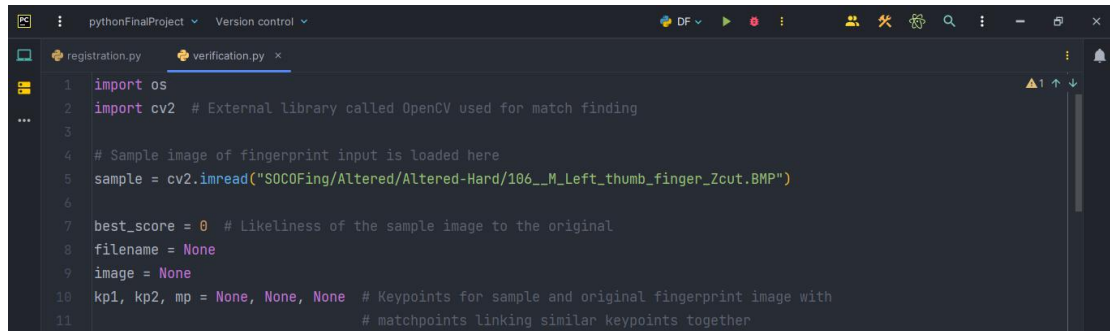
```
55 # Example usage
56 nic = '1234567890'
57 handprints = {
58     'Left': {'Thumb': 'left_thumb_fingerprint_data',
59              'Index': 'left_index_fingerprint_data',
60              'Middle': 'left_middle_fingerprint_data',
61              'Ring': 'left_ring_fingerprint_data',
62              'Pinky': 'left_pinky_fingerprint_data'},
63     'Right': {'Thumb': 'right_thumb_fingerprint_data',
64              'Index': 'right_index_fingerprint_data',
65              'Middle': 'right_middle_fingerprint_data',
66              'Ring': 'right_ring_fingerprint_data',
67              'Pinky': 'right_pinky_fingerprint_data'}
68 }
69
70 register_fingerprint(nic, handprints)
71
```



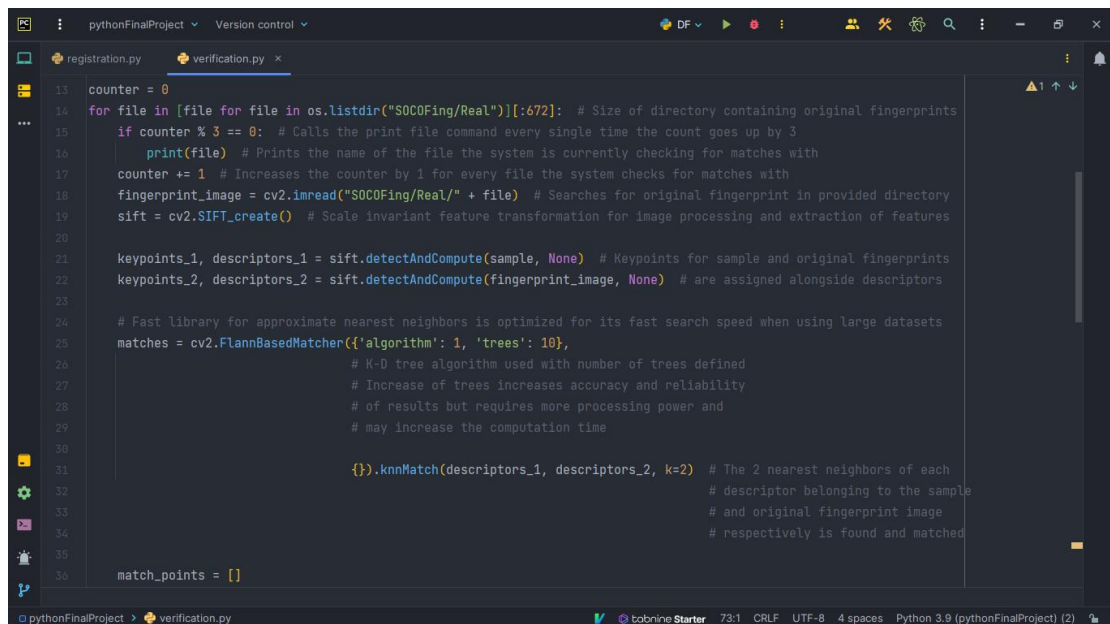
```
Run C:\Users\HP\PycharmProjects\pythonFinalProject\venv\Scripts\python.exe C:\Users\HP\PycharmProjects\pythonFinalProject\DF.py
NIC Hand Finger Fingerprint
0 000000015F Right Thumb SOCOFing/Real/15_F_Right_thumb_finger.BMP
1 000000100M Right Ring SOCOFing/Real/100_M_Right_ring_finger.BMP
2 000000106M Left Thumb SOCOFing/Real/106_M_Left_thumb_finger.BMP
3 000000109F Left Index SOCOFing/Real/109_F_Left_index_finger.BMP
4 000000111M Left Ring SOCOFing/Real/111_M_Left_ring_finger.BMP
5 000000114F Left Middle SOCOFing/Real/114_F_Left_middle_finger.BMP
6 000000119F Left Little SOCOFing/Real/119_F_Left_little_finger.BMP
7 000000125M Right Middle SOCOFing/Real/125_M_Right_middle_finger.BMP
8 000000127F Right Little SOCOFing/Real/127_F_Right_little_finger.BMP
9 000000132M Right Index SOCOFing/Real/132_M_Right_index_finger.BMP
Process finished with exit code 0
```

The provided example usage demonstrates how to utilize the system by registering fingerprints for a given NIC number and handprint data followed by an example of how data would be stored in the DataFrame. The 'register\_fingerprint' function is called with the NIC number ('1234567890') and a dictionary containing fingerprint data for both the left and right hands and their respective fingers. Each finger's fingerprint data is represented as a string in the example, but in practice, it would be the actual fingerprint data obtained from the scanner.

## Verification Process



In the context of verifying voters on the day the elections go live, the system is designed to perform fingerprint matching, optimizing the use of the OpenCV library and the Scale Invariant Feature Transformation (SIFT) algorithm. The system has been developed to begin by loading a sample fingerprint image and initializes variables to keep track of the best match score, filename, and image.



The system has then been programmed to iterate through a directory of original fingerprint images; while printing the name of the file currently being checked for every third image to indicate progression. It reads the original fingerprint image and creates a SIFT object for feature extraction. Using the SIFT algorithm, keypoints and descriptors are computed for both the sample and original fingerprint images. The algorithm then uses the Fast Library for Approximate Nearest Neighbors (FLANN) to find the two nearest neighbors for each descriptor in both images.

```
pythonFinalProject Version control
registration.py verification.py x
38 # Match filtration process through distance ratio test filters out less reliable or ambiguous matches
39 for p, q in matches: # Defines nearest neighbors as p and q
40     if p.distance < 0.1 * q.distance: # Distance ratio threshold for match validation
41         match_points.append(p) # Adds nearest neighbor p to the match_points list if it passes the test
42
43 # Smaller keypoint selection logic
44 keypoint = 0
45 if len(keypoints_1) < len(keypoints_2):
46     keypoints = len(keypoints_1)
47 else:
48     keypoints = len(keypoints_2)
49
50 # Results display logic
51 if len(match_points) / keypoints * 100 > best_score: # Match score calculation
52     best_score = len(match_points) / keypoints * 100 # and display
53     filename = file
54     image = fingerprint_image
55     kp1, kp2, mp = keypoints_1, keypoints_2, match_points
56     if best_score == 100:
57         break
```

```
pythonFinalProject Version control
registration.py verification.py x
59 # Statistical information regarding the best matching original fingerprint
60 if filename is not None:
61     print("Best Match: " + filename)
62     print("Match Score: " + str(best_score))
63
64 # Visual representation of sample fingerprint matches with original fingerprint
65 result = cv2.drawMatches(sample, kp1, image, kp2, mp, None)
66 result = cv2.resize(result, None, fx=3, fy=3)
67 cv2.imshow("Result", result)
68 cv2.waitKey(0)
69 cv2.destroyAllWindows()
70 else:
71     print("No match found.")
72
```

Next, a match filtration process is performed using a distance ratio test for each pair of nearest neighbors. If the distance ratio between them is below the given threshold, the match is considered reliable and added to the list of match points. The system also keeps track of the number of keypoints in both images and selects the smaller value with the match score being calculated by dividing the number of match points by the number of keypoints and multiplying by 100. If an original fingerprint image's match score is higher than the previous best score, it updates the best score, filename, image, and keypoints/match points variables. The system continues this process until it either finds a perfect match, (with a score of 100), or checks all the original fingerprint images. Upon completion, it displays the filename of the best match and the match score it achieved. It also generates a visual representation of the sample fingerprint's matches with the original fingerprint image using the drawMatches function in OpenCV. However, if no match is found, the system outputs a message indicating that no match was found.

## 5.5 PROTOTYPE TESTING AND EVALUATION

Having completed the development of the prototypes discussed earlier, the system was then thoroughly tested for functionality, performance, and usability.

The testing phase mainly involved unit tests to verify the individual components of the system. Some of the other tests to be conducted such as; integration tests for ensuring the seamless interaction between different modules, and system-level tests for validating the overall behavior and functionality of the developed prototype; proved to be harder to accommodate due to the system having been incomplete without the integration of the fingerprint/handprint scanner into the system.

However, several tests were carried out to make sure the system was fully functional up to the point of current development. To ensure this the system was subjected to different test cases, to assess its robustness and reliability. Test scenarios were designed to simulate real-world usage and evaluate the system's ability to handle different inputs and issues while producing accurate and expected outputs.

Performance testing was conducted to measure the system's response time, scalability, and resource utilization under varying workloads. This helped identify any performance bottlenecks and optimize the system for efficient operation. Usability testing played a crucial role in evaluating the prototypes from the end-users' perspective.

Feedback and observations from users were collected to assess the system's user-friendliness, intuitiveness, and effectiveness in achieving its intended goals. This feedback was invaluable in refining the user interface, improving user experience, and addressing any usability issues. The prototype testing and evaluation phase allowed for identifying and rectifying any bugs, glitches, or design flaws that may have been overlooked during the development stage. It provided valuable insights into the system's strengths, weaknesses, and areas for improvement.

Based on the test results and user feedback obtained, necessary refinements and enhancements were made to the prototypes to ensure their readiness for the next stages of development and deployment. Overall, the prototype testing and evaluation phase was critical in ensuring the reliability, performance, and usability of the systems. It served as a key milestone in validating the effectiveness of the prototype, gathering user feedback, and informing future development decisions.



### 5.5.1 WEBSITE (GUI) TEST LOGS

The unit initially tested was the website which was the GUI of the system and played a major role in directly influencing users' experiences of the newly idealized voting process. This component was mainly tested for functionality and listed below are the test logs of the process.

Test Scenario	Test Case ID	Expected Result	Actual Result	Status	Comments
User Registration	UR01	Users should be able to enter their required details to register for an account that will allow them to participate in the elections	Functions as Intended	Passed	Functionality Achieved
Handprint Registration	HR01	Users should be able to pre-register both of their handprints in order to complete the registration process for an account that will allow them to participate in the elections	Not fully Functional	Incomplete	Not fully achievable without scanner integration

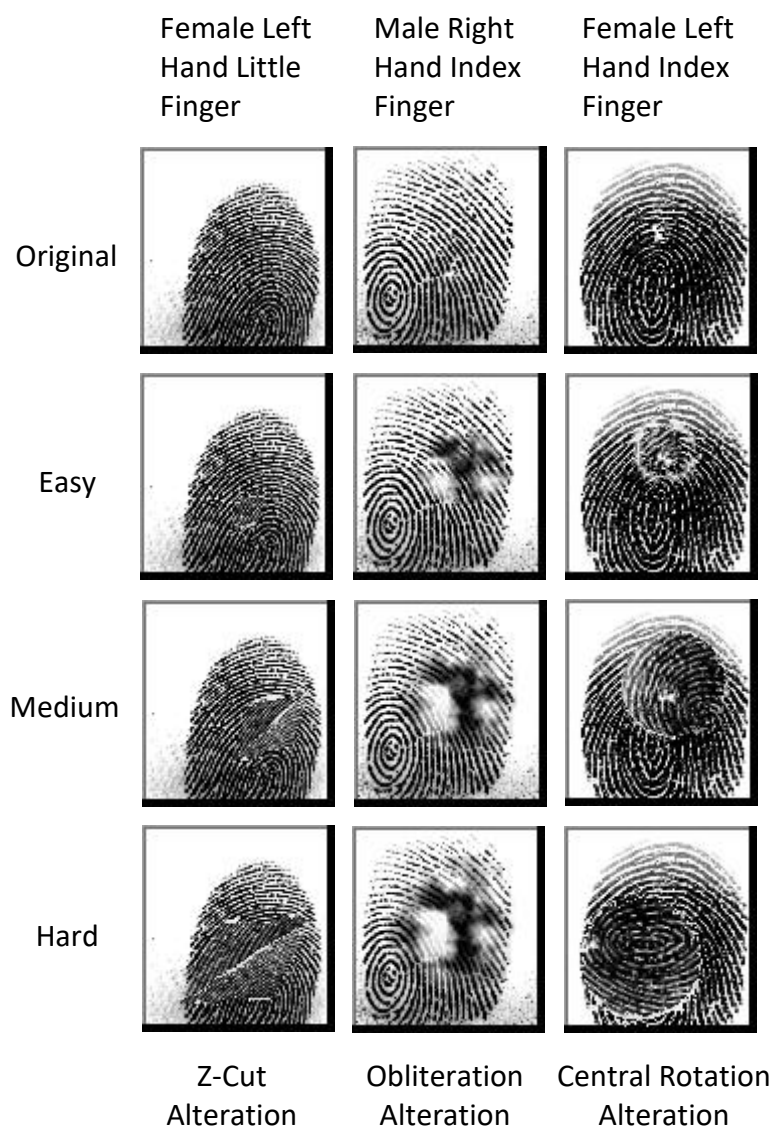
NIC Login	NL01	Users should be able to enter their required login details and be able to login to their existing accounts	Functions as Intended	Passed	Functionality Achieved
Handprint Login	HL01	Users should be able to login using any of their pre-registered fingerprints and be able to login to their existing accounts	Not fully Functional	Incomplete	Not fully achievable without scanner integration
Election CRUD Functionality	ECF01	Administrator accounts should be able to create, read, update and delete elections that have not gone live nor have any votes cast yet	Functions as Intended	Passed	Functionality Achieved

Candidate CRUD Functionality	CCF01	Administrator accounts should be able to create, read, update and delete candidates to elections that have not gone live nor have any votes cast yet	Functions as Intended	Passed	Functionality Achieved
Election Result Viewing	ERV01	Administrator accounts should be able to view the results of candidate vote totals in both ongoing elections and those that have ended	Functions as Intended	Passed	Functionality Achieved
Election Result Updating	ERU01	Administrator accounts should be able to view the results of candidate vote totals updating in ongoing elections as and when voters have cast their votes	Functions as Intended	Passed	Functionality Achieved

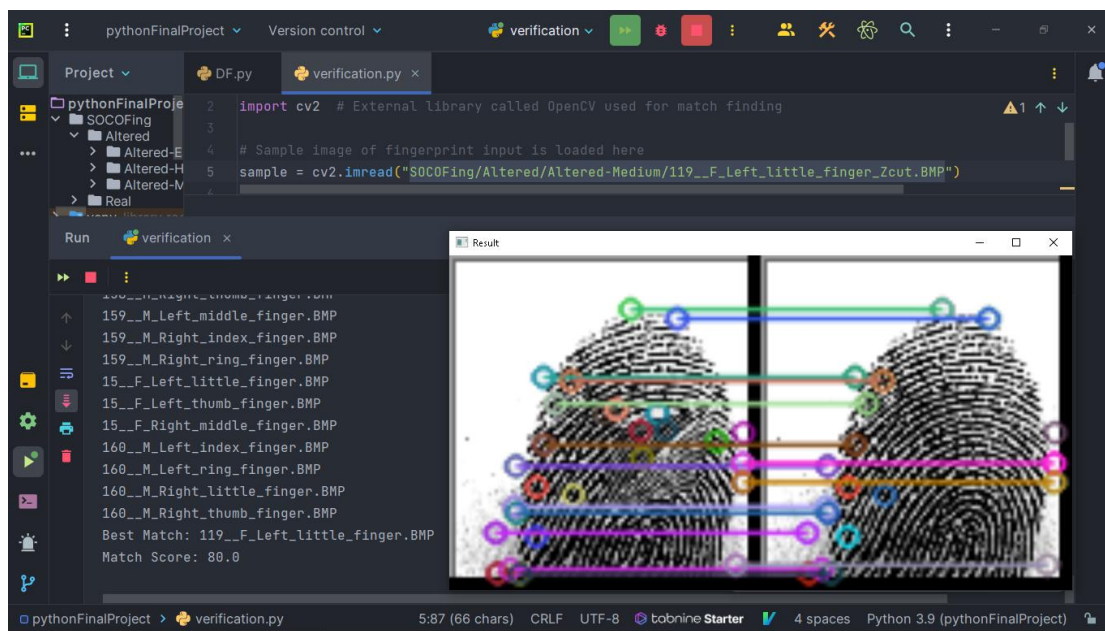
Voter Vote Casting	VVC01	Voter accounts should be able to cast their vote for their preferred candidate in elections that have gone live; and should be able to confirm their vote using their already registered fingerprints or handprints; and should only be able to vote once per election	Not fully Functional	Incomplete	Not fully achievable without scanner integration
Candidate Vote Count Updating	CVCU01	Voter accounts should be able to view the results of candidate vote totals updating in ongoing elections as and when voters have cast their votes	Functions as Intended	Passed	Functionality Achieved

## 5.5.2 MATCHING ALGORITHM TEST RESULTS

Due to the lengthy process associated with collating a dataset of fingerprints/handprints and the lack of resources required to do so, the matching algorithm unit was tested using a dataset of fingerprints previously published by Shehu et al. (2018). The authors' had developed a biometric fingerprint database designed for academic research purposes; made up of 6,000 fingerprint images from 600 African subjects. It is further elaborated that the Sokoto Coventry Fingerprint Dataset (SOCOFing), contains unique attributes such as labels for gender, hand and finger name for each original image as well as synthetically altered versions with three different levels of alteration for obliteration, central rotation, and z-cut type alterations as shown below.

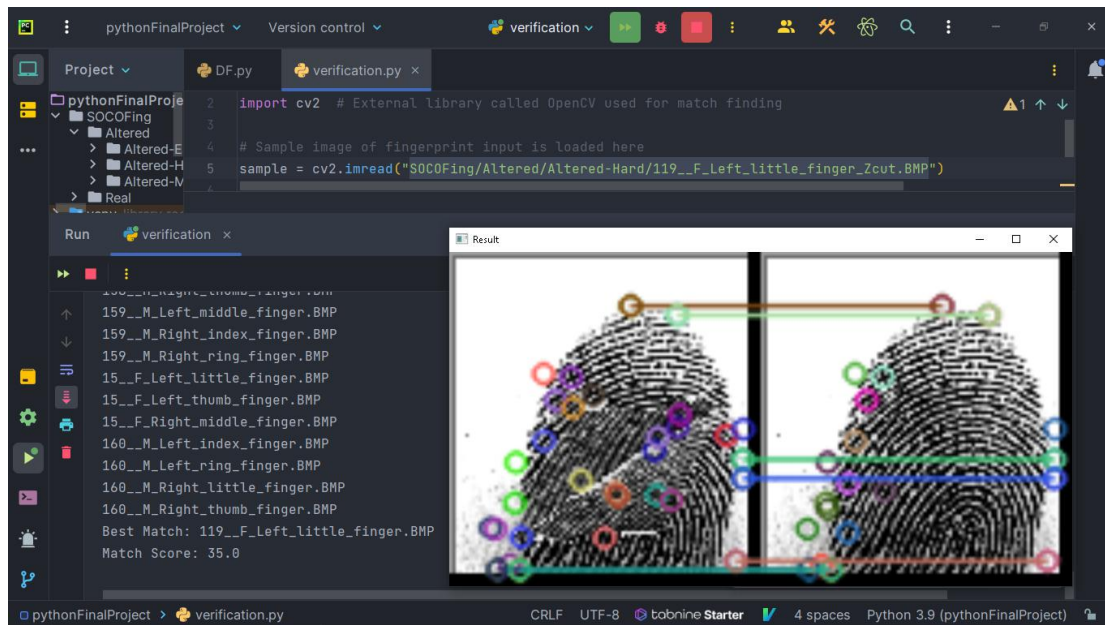


The SOCOFing dataset was utilized in test case simulations of the system's intended usage as a substitute for real-time fingerprint input by election participants. The altered fingerprint images were randomly selected, in terms of both difficulty and type of alteration, and then used as sample input images in which the system was expected to find the original print, both efficiently and accurately, amongst 6000 others. The usage of altered fingerprints as samples were purely for the testing of the system's ability to effectively find matches despite the inevitability of input inconsistency and several other contributing factors inclusive of, but not limited to environmental conditions; the condition of the fingerprint being scanned; as well as the positioning and pressure applied during the scan. Shown below are the results of some of the tests performed using the sample fingerprint images as seen before.

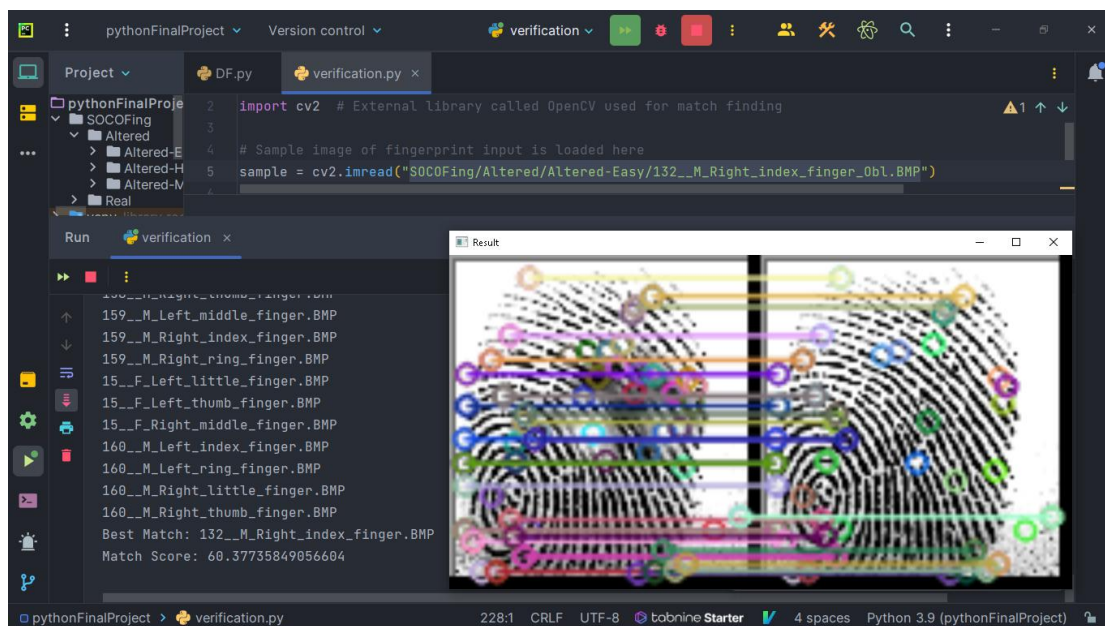


Female Left Hand Little Finger Z-Cut Alteration at Medium Difficulty

## Female Left Hand Little Finger Z-Cut Alteration at Hard Difficulty

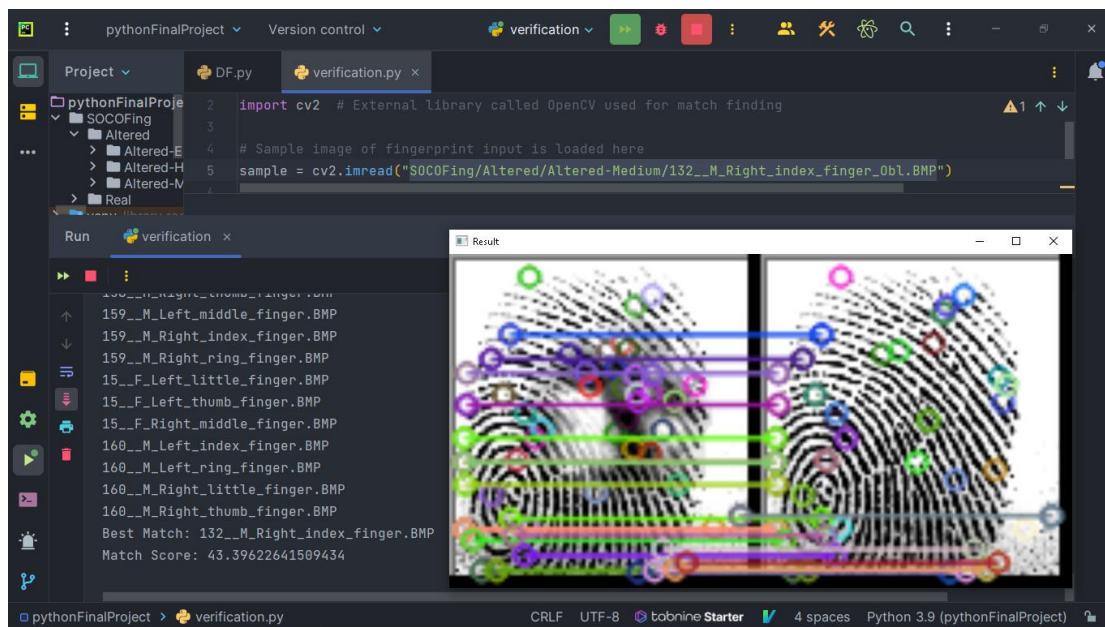


## Male Right Hand Index Finger Obliteration Alteration at Easy Difficulty

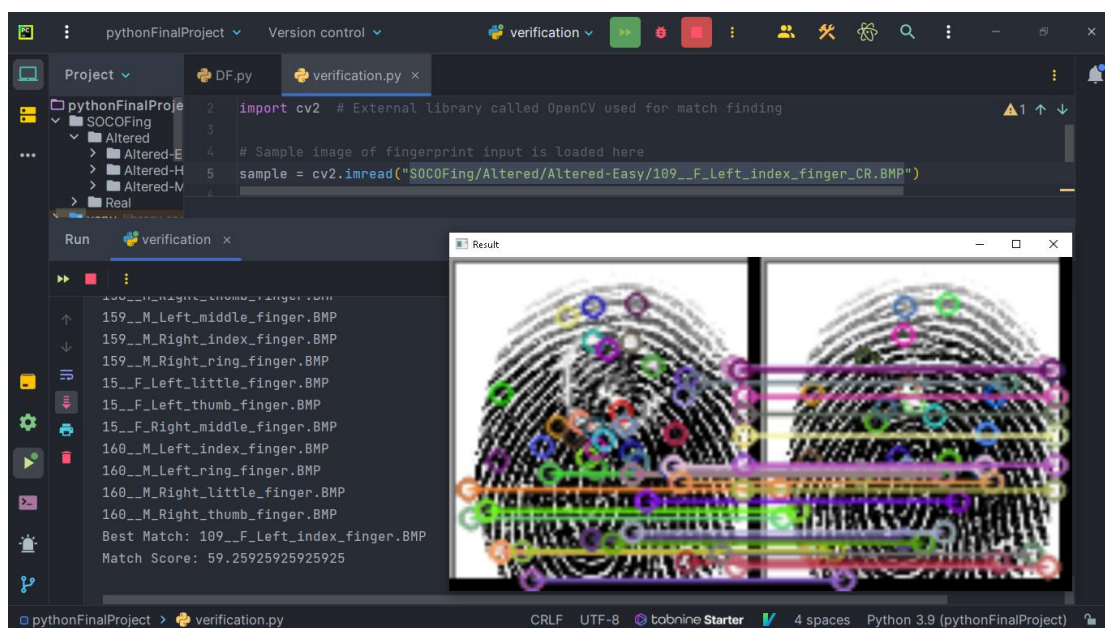




## Male Right Hand Index Finger Obliteration Alteration at Medium Difficulty

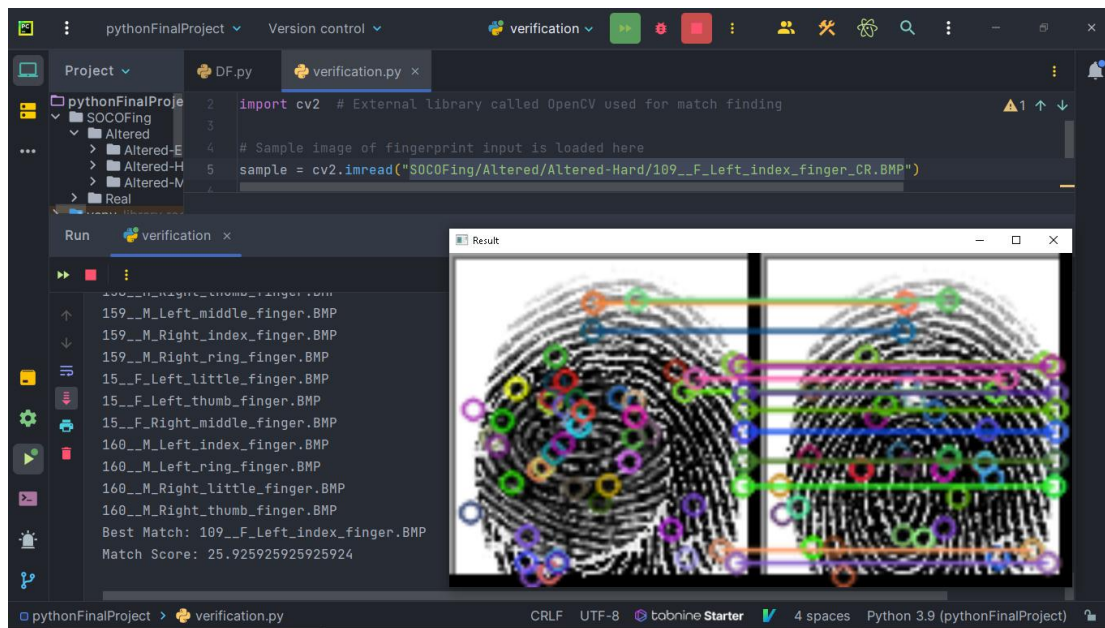


## Female Left Hand Index Finger Rotation Alteration at Easy Difficulty





## Female Left Hand Index Finger Rotation Alteration at Hard Difficulty



From the test results generated as shown in the aforementioned screenshots, an inversely proportionate correlation between the match scores and the alteration difficulties used can be seen. As the difficulty of type alteration used increases, the match score between the original and the sample images used decreases. However, it is important to note that despite the difficulty in regards to match finding as outlined by the decrease in match scores; the algorithm has been able to consistently match the altered sample used, to its original no matter how affected the fingerprint input at the time of scan may be, as indicated by the resulting best match sharing an identical name to the sample image used. Thus indicating that the system is able to retain its functional reliability and perform regardless of the quality of fingerprint input.

## 6 | CONCLUSION

In this project, the development of a secure and user-friendly fingerprint voting system that aimed to modernize and revolutionize the overall voting experience here in Sri Lanka was initiated; prioritizing the accuracy and confidentiality of the voting process more than most. Through the realization of these goals it can be said that significant strides towards advancing the concept of secure voting have been successfully made.

Despite facing several challenges in accommodating certain tests due to the absence of a fingerprint scanner and the limitations imposed by its absence, the tests carried out were made sure to be thorough enough to ensure the system's functionality up to the current development stage.

Findings derived from the tests run, revealed that the system is highly capable of effectively verifying voter identities through the matching algorithm developed for the fingerprint scanning process, therefore streamlining the voting process and enhancing security. The website developed as a user-friendly interface also received positive feedback during usability testing, in regards to its effectiveness in promoting ease of use for voters who took part in the test.

Upon reflection, the impact the project makes grows more prominent in terms of the potential it has in significantly increasing voter participation and bolstering the integrity of the voting process. By eliminating the need for traditional identification methods and replacing it with biometric verification methods, the system promptly addresses several concerns related to voter impersonation and fraud.

While the project has indeed reached its desired state of completion, it goes without saying that there are certain limitations that do require attention in future work, some of which include; the integration of the system with a live database for real-time verification, further scalability testing, and addressing potential privacy concerns such as spoofing; all of which are aspects that warrant further exploration in subsequent phases.

In conclusion, the fingerprint voting system developed so far showcases a promising advancement in the realm of secure voting solutions. By providing a seamless and reliable voting experience, it has the potential to strengthen democratic processes and restore public trust in Sri Lanka's electoral systems. It is strongly believed that the work done here lays a solid foundation for continued research and development in this domain, and therefore brings about great anticipation towards the positive impact that the developed system could potentially have on future elections.

## 7 | BIBLIOGRAPHY

- Rahman, M.S., Mohamad, O.B. and Abu Zarim, Z.B. (2014). Climate Change: A Review of Its Health Impact and Percieved Awareness by the Young Citizens. *Global Journal of Health Science*, 6(4).  
doi:<https://doi.org/10.5539/gjhs.v6n4p196>
- Gilson, L. L. & Goldberg, C. B. (2015). Editors' Comment: So, What Is a Conceptual Paper? *Group & Organization Management*, 40(2), 127–130.  
<https://doi.org/10.1177/1059601115576425>
- Afribery (2020). *Theoretical Framework vs Conceptual Framework (Differences and Similarities)*. [online] Afribery. Available at:  
<https://afribery.com/knowledge/theoretical-framework-vs-conceptual-framework/>
- Moramudali, U. (2017). *Sri Lanka's Debt and China's Money*. [online] thediplomat.com. Available at: <https://thediplomat.com/2017/08/sri-lankas-debt-and-chinas-money/>
- Perera, A. (2022). Why are Sri Lankans protesting in the streets? BBC News. [online] 14 Jul. Available at: <https://www.bbc.com/news/world-61028138>
- Hillman, J.E. (2018). Game of Loans: How China Bought Hambantota. [online] csis.org. Available at: <https://www.csis.org/analysis/game-loans-how-china-bought-hambantota>
- Farzan, Z. (2021). Sri Lanka's strategic locations falling into hands of foreign nations? [online] Sri Lanka News - Newsfirst. Available at: <https://www.newsfirst.lk/2021/09/09/sri-lankas-strategic-locations-falling-into-hands-of-foreign-nations/>
- Bandara, K. (2022). LG Polls will cost Rs. 10 billion: EC says - Breaking News | Daily Mirror. [online] www.dailymirror.lk. Available at: [https://www.dailymirror.lk/breaking\\_news/LG-Polls-will-cost-Rs-10-billion-EC-says/108-251197](https://www.dailymirror.lk/breaking_news/LG-Polls-will-cost-Rs-10-billion-EC-says/108-251197)

- Jayasinghe, C. (2020). Candidates spend Rs 2.2 bn over Sri Lanka's polls campaign period. [online] EconomyNext. Available at: <https://economynext.com/candidates-spend-rs-2-2-bn-over-sri-lankas-polls-campaign-period-72677/>
- Fernando, M. (2019). Gotabhaya alone expends over 59% of total election campaign expenditure. [online] Sunday Observer. Available at: <https://www.sundayobserver.lk/2019/11/10/news-features/gotabhaya-alone-expends-over-59-total-election-campaign-expenditure>
- Poem Analysis (n.d.). Slow and steady wins the race. [online] Poem Analysis. Available at: <https://poemanalysis.com/proverb/slow-and-steady-wins-the-race/>
- Newsfirst Sri Lanka (2021). The drawbacks in the election system of Sri Lanka | Role of Law (Episode 21). [online] www.youtube.com. Available at: <https://youtu.be/BpAZ3odXaCc>
- Abdelwhab, A. and Viriri, S. (2018). A Survey on Soft Biometrics for Human Identification. Machine Learning and Biometrics. doi:<https://doi.org/10.5772/intechopen.76021>
- Ellena, K. and Petrov, G. (2018). Cybersecurity in Elections Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies. [online] aceproject.org. Available at: [https://aceproject.org/ero-en/ifes-cybersecurity-in-elections/at\\_download/file](https://aceproject.org/ero-en/ifes-cybersecurity-in-elections/at_download/file)
- Krimmer, R., (orcid)0000-0002-0873-539X, <http://orcid.org/0000-0002-0873-539X>, Volkamer, M., (orcid)0000-0003-2674-4043, <http://orcid.org/0000-0003-2674-4043>, Cortier, V., Gore, R., Hapsara, M. and (orcid)0000-0002- (2018). Electronic Voting. [online] dl.mehralborz.ac.ir. Springer International Publishing : Available at: <https://dl.mehralborz.ac.ir/handle/Hannan/773>
- Mohammed, H.I. (2008). FingerPrint Base Electronic Voting System. [online] Available at: <http://dx.doi.org/10.13140/2.1.1108.4481>

- NeuralNine (2022). Fingerprint Matching in Python. [online] www.youtube.com. Available at: <https://youtu.be/llvfqfKkiio>
- Shehu, Y.I., Ruiz-Garcia, A., Palade, V. and James, A. (2018). Sokoto Coventry Fingerprint Dataset (SOCOFing). doi:<https://doi.org/10.48550/arxiv.1807.10609>