An Online Voting System using Face Recognition for Campus Election

Meor Muhammad Kamal Meor Muhammad Sulaiman[1], Mohd Fairuz Iskandar Othman[1], Wahidah Md Shah[1], Aslinda Hassan[1], Norhayati Harum[1], and Ibrahim Mohammed Alseadoon[2]
[1]Center for Advanced Computing Technology (C-ACT),
Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Univerisiti Teknikal Malaysia Melaka
Email: b031810170@student.utem.edu.my
[2]College of Computer Science and Engineering,
University of Ha'il, Ha'il, Saudi Arabia
Email: i.alsedon@uoh.edu.sa

Abstract— Online voting has been implemented in various countries for different purposes. It helps to improve accessibility and efficiency to the voter and organizer. Student council election in Universiti Teknikal Malaysia Melaka has been using an electronic voting machine that is placed at the polling site. Students need to come to the polling station to cast their votes thus causing an accessibility issue. This project was aimed to develop a remote voting system for easier access during voting day that allows voters to cast their vote remotely that is convenient and helps to improve accessibility to the student. Trust is highly related to the voting mechanism as it should be free and fair. To increase trust in online voting a better authentication should be implemented. The inherence-based factor would be able to verify a person's characteristics, and they should be present at the moment of the verification process. This study implements facial recognition as a form of authentication to authenticate legitimate voters. Students and organizers would benefit from this system as it is remotely reachable, trusted, convenient, and reduces the time taken for the voting process.

Index Terms—Voting, Face-recognition, E-Voting, I-Voting, authentication, AWS Rekognition.

I. Introduction

The use of an online system would make an application accessible, efficient, and convenient. Online voting systems has been used throughout the world, such as in the United States [1] and Canada [2]. Online voting system is a part of electronic voting (E-voting) which is divided into 4 different types of E-voting [3] such as Direct recording electronic (DRE) voting machines, Optical Mark Reader (OMR) system, Electronic ballot printers (EBPs) and Internet voting systems (I-Voting) where an online voting system is defined as an I-Voting where votes are cast via the Internet to a central server that manages the ballot and voter would be able to cast their vote from a public computer or kiosk at the polling station.

Universiti Teknikal Malaysia Melaka has been implementing electronic voting for their student council elections since 2006. Voting machines are placed at a specific location and would be used by students to cast their votes. This meant that each student needs to access the voting machine on election day. Permanent, fixed, and static placing of the voting machines causes some issue to voters such as accessibility and time contraints. Besides, election day is usually conducted on weekdays where students have lectures to attend, thus finding a suitable time to cast their vote was difficult. Therefore, a solution is needed to ensure that a more accessible and convenient voting mechanism is implemented. I-voting would be able to give a more suitable solution to the election organizers, students and also would be able to reduce the cost of running an election.

I-voting would have a positive impact and it is determined to be useful because of its level of trust, accessibility, and convenience [4]. I-voting would give a flexible way to casting votes where it allows the voter to cast their votes anywhere without going to the polling station [5]. Therefore, I-voting can provide easy access voting to students. Trust is the main aspect that is closely tied to a voting mechanism and highly impacting the usefulness of I-voting, one of which is authentication [6]. A failure of the voting system would affect the reliability of public confidence in an electoral system [4]. The authors in [7], found that there is a relationship between ease of use to trust and trust to the usefulness and intention of I-voting system adoption. Therefore, implementing a better authentication system would increase voter trust towards the I-voting system. Various studies have shown that inherence-based authentication would overcome the challenges and problems that comes with knowledge-based factor authentication such as password and tokens [8], Thus implementing inherence-based authentication such as biometric authentication would increase the system security. A study has shown that users are leaning towards biometric authentication rather than PIN/passwords because the technology is more secure even though 93.51% of the respondents used the PIN and password method [9]. Therefore, implementing a biometric authentication would increase the trust of users toward a system as it provides better security and increases the system's usefulness.

The main objective of this project is to develop a remote voting system for easier access during voting day that allows voters to cast their vote remotely. Second, to implement facial recognition for authentication purposes, to identify the legitimate voter. This system would be developed as a web-based system that authenticates voters during the login process before casting their votes. The voter would use a web browser to access the system remotely. Before accessing the system, facial recognition process would be performed by comparing the current facial image capture during the login process against the facial image stored in a central database. Upon successful authentication, voters would then be able to cast their votes using the system.

II. Previous work

To address the accessibility and voting efficiency the authors of [10], [11] developed an online voting system. The developed system allows students to register and cast their votes after a successful registration. However, the authors used knowledge-based factor authentication to verify the user. To ensure that legitimate voter is only allowed to access the voting system various approaches have been used.

Early work used fingerprint to identify voters [12] as it is unique and different for every individual. The author proposed a voting system that verifies voter using fingerprint as an authentication of a voter. However, special biometric devices are connected through a USB cable to scan the voter fingerprint thus this proposed system would need a biometric device to ensure that the system is able to authenticate voter fingerprint. The same approach is also implemented in [13] in which the voter is authenticated using biometric authentication but voters are verified with their fingerprint at a kiosk station and then a token was given that later would be used to redirect to the online system. This meant that the system implements a ticketing system to enable the online voting system.

The author in [14] developed a biometric authentication for the voting system. The biometric details are used during registration. However, this system is developed only for Android based devices and QR code were given to voter to access the Android based system. This system is unable to operate and work with a different environment such as a computer.

The authors of [15] proposed a solution for vote-rigging during an election, insecure or inaccessible polling stations, inadequate polling materials, and also inexperienced personnel issues. Their work allows online facial recognition verification process for a voter. Therefore, their paper expands the concept of an online system for a voting system such as [10] and [11] that would mitigate the accessibility issue and improve efficiency and incorporating facial recognition that is a part of biometric authentication [12] - [15] to increase voter trust toward the online voting system. However, based on the review literature there are gaps that has not been explored. Previous studies were focused toward implementing biometric authentication to authenticate voter. Most of the algorithm are run on local system or has not been discussed. Furthermore, compatibility aspect has not been addressed to help accessibility issue.

New technology such as cloud computing would offer better system development by running the algorithm remotely and effective solution for online facial recognition with a very few little studies and worthy to investigate. Therefore, this study little studies and worthy to investigate. Therefore, this study will fill the research gaps by implementing cloud service provided by Amazon Web Service (AWS) to perform facial recognition for online voting system.

III. Development and system design

The online voting system in this project was developed to ensure that voters are able to vote remotely and the system authenticates the user using facial recognition. In this project, the waterfall model is was used for system development: it involves requirement analysis, system design, system implementation, testing, and maintenance.

A. Requirement Analysis

In the requirement analysis, all the requirements were identified from the previous and related work in the realm of an online voting system which includes the hardware and software requirements to develop an online voting system. In this project, we implemented the cloud-based Software as a Service (SaaS) provided by AWS to recognize users during authentication. Previous research has used on-premise or local facial recognition algorithm. Amazon Rekognition is a cloud-based computer vision platform that can identify object, people, text, scenes, and activities provided by AWS that use deep neural network technology. The Amazon Rekognition allows the software application to perform the process on the cloud by providing image to Amazon Rekognition using Application Programming Interface (API) [16].

B. System design

System design is meant to correctly design a system by defining the elements that are needed such as modules, components, and data for a system with the respective requirement. Fig. 1 shows the system architecture for this project where voters accessing the system that is hosted on a server remotely from the client computer. Cloud service is then called using API for user authentication.

Fig. 2 shows the software components required for this project. Clients are accessing using a web browser while the system is hosted on a server using web server software. Also, all the data are stored in the database using MariaDB and the API calls from the server to the cloud service using PHP scripts.

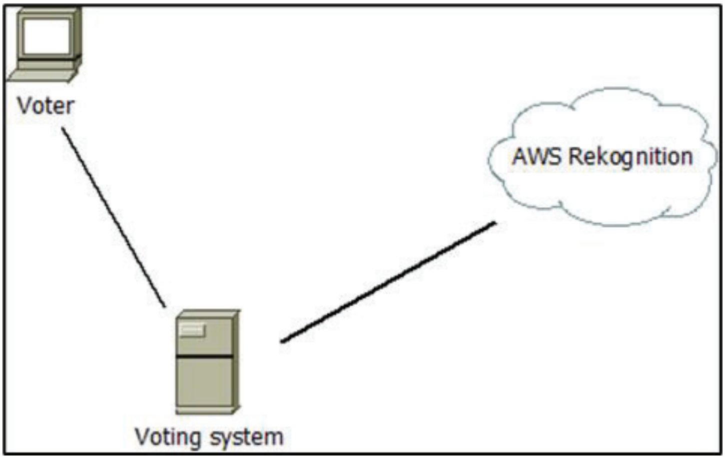


Fig. 1. System Architecture

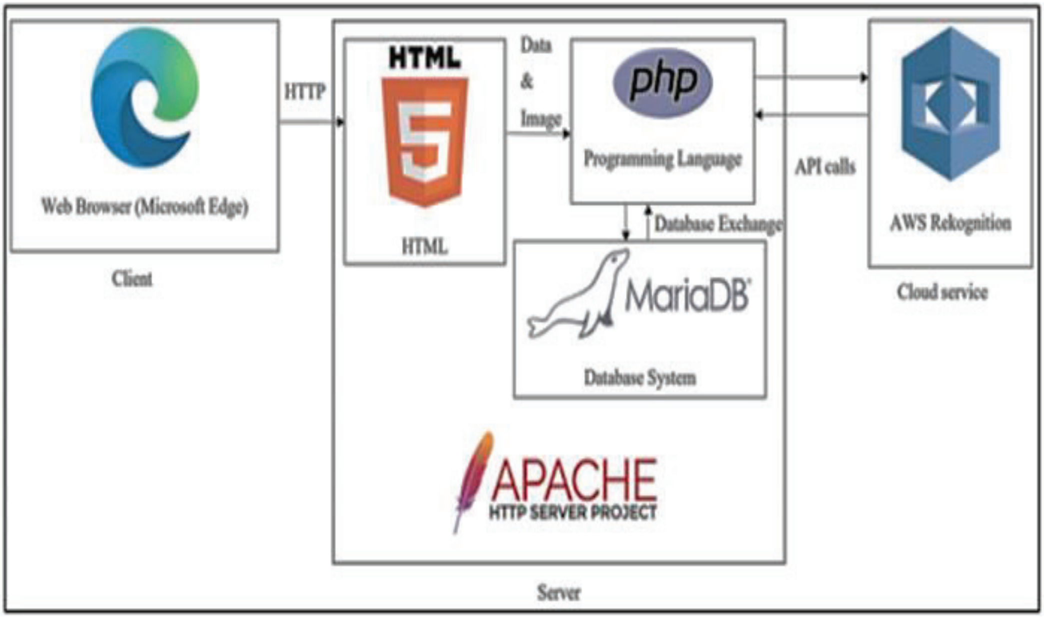


Fig. 2. Software Components

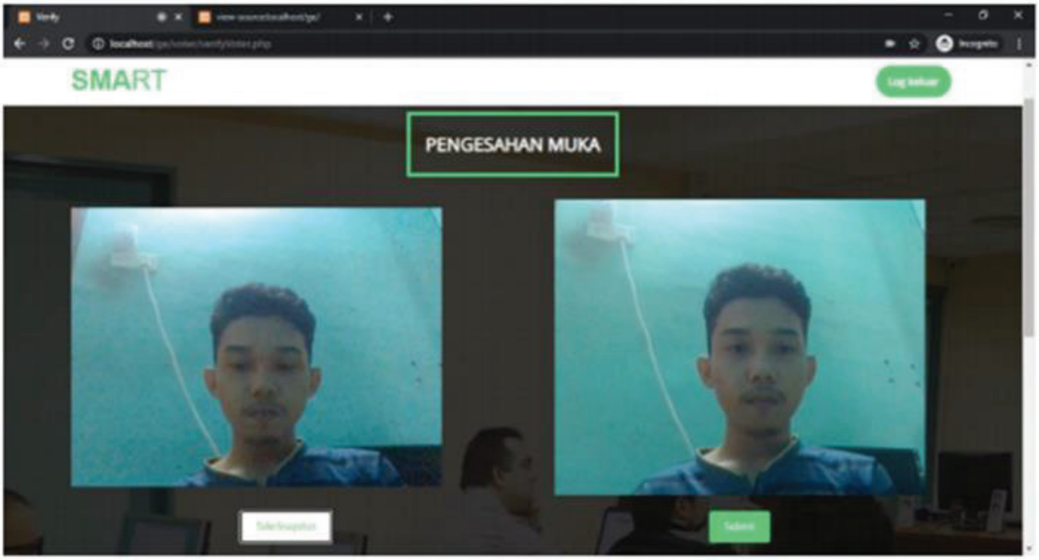
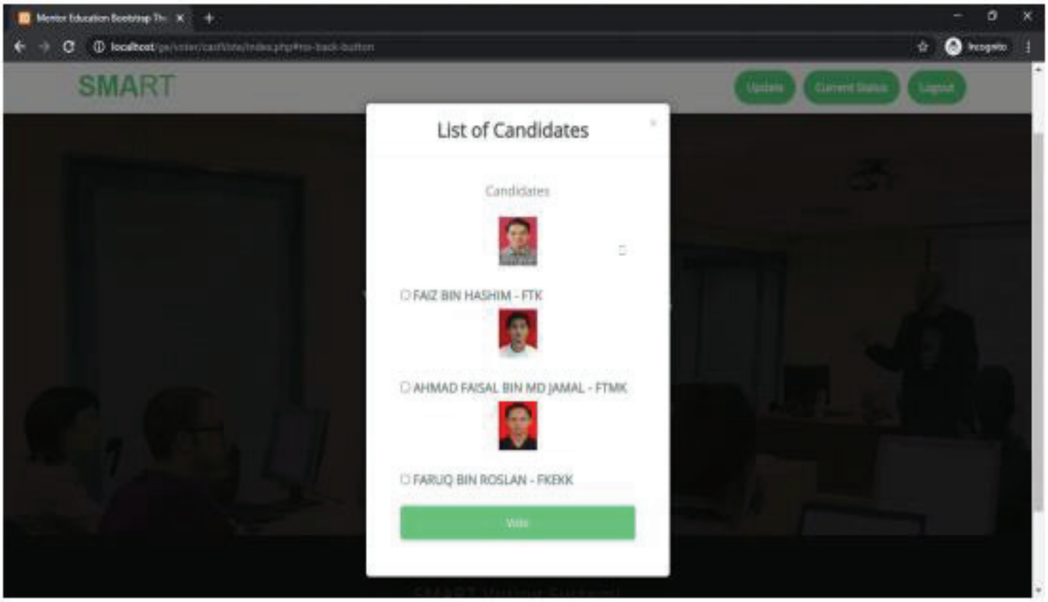


Fig. 3. Face recognition module



List of Candidates

Candidates

□ FAIZ BIN HASHIM - FTK

□ AHMAD FAISAL BIN MD JAMAL - FTMK

□ FARUQ BIN ROSLAN - FKEKK

Fig. 4. Voting module.

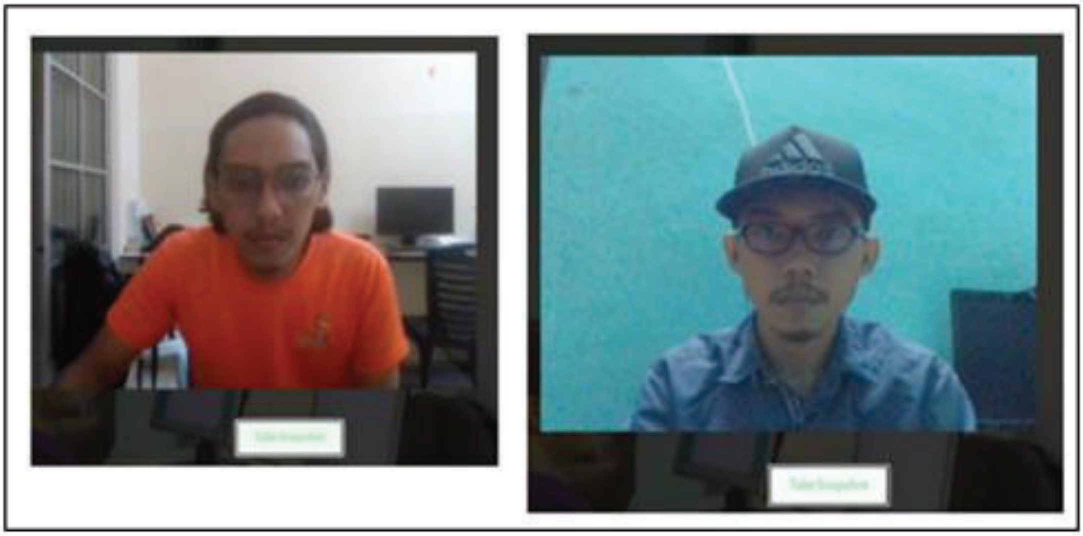


Fig. 5. Face occlusion testing.

C. Implementation

In the implementation phase, the software was developed based on the requirement to enable the voter to cast their vote remotely and authenticating them using facial recognition. Fig. 3 shows the developed interface for the system and Fig. 4 shows the voting module developed for the voter. The facial image will be captured and then analyzed by the cloud service with the pre-included voter image in the database.

D. Testing Results

Testing is a process of measuring, finding, and examining the quality of a product and fixing any defects during the testing process. All the testing implemented is done so that the correctness of the program, system logic, and function would have been determined. Functional testing would be used to ensure the system running correctly. This testing aims to ensure that the system is able to detect and recognize faces with an occlusion because there might be intentional or unintentional situations where voters wear a scarf or sunglasses to avoid being recognized or for medical reason and other sources of facial occlusion such as wearing a hat, having mustaches, and hairs[17], thus impacting the facial recognition algorithm[18].

Table 1 shows the details scenario and description of testing to ensure that the algorithm able to recognize voters with a facial occlusion. Table 2 shows the result of the testing based on the test codes in Table 1. Fig. 5 shows that participants were testing the authentication process with facial accessories and the system successfully detected both participants. We are sure that the algorithm implemented in this system had successfully recognizes user wearing facial accessories. Implementing AWS Rekognition helps to improve the performance of recognizing voter and as suggested by [19] that AWS Rekognition is accurate and works well with distant faces.

TABLE 1
TEST CASES

Test Codes	Descriptions
OVST1	Wearing spectacles
OVST2	Wearing headgear
OVST3	Wearing surgical mask

TABLE 2
TEST RESULT

Participants	OVST1	OVST2	OVST3
A	Pass	Pass	Failed
B	Pass	Pass	Failed
C	Pass	Pass	Failed
D	Pass	Pass	Failed
E	Pass	Pass	Failed

In addition, we also measure the processing time taken by the algorithm to recognize voters. Table 3 displayed the testing completion of each participant relative to the time taken to recognize voters during the recognition process.

TABLE 3
TEST COMPLETION TIME (IN SECONDS)

Participants	Completion time				
A	2.954	2.76	2.671	2.664	2.73
B	2.661	2.67	2.724	2.659	2.797
C	2.726	2.706	2.591	2.7	2.567
D	2.97	2.839	2.561	2.583	2.967
E	2.736	2.726	2.517	2.815	2.71

The light source would also affect the capability to recognize a person or individual. AWS Rekognition API also provides features to analyze and identifies facial image brightness. The value is between 0 to 100 which a higher value indicates a brighter face image. Table 4 shows the testing that has been done to identify the brightness level that AWS Rekognition is able to recognize.

A. Maintenance

The last and final stage is maintenance which requires maintenance of the system. Maintenance is only required when the developed system requires any future updates in terms of features and modules or if a failure is detected.

IV. Discussion

This project was developed to ensure voters convenience and trust of using an online voting system. This study shows that implementing the I-voting system offers voters with a highly convenient application which allows users to access remotely. This study can be a base application for future studies on the area of online voting and facial recognition. By using inherence-based authentication, it increases the trust between the user and the system as it would offer a secure mechanism to secure a system.

Moreover, this system would offer a new approach to authenticating an individual remotely. The common method of implementing biometric authentication is locally-based thus this project extends the use of cloud service that would allow biometric authentication to be performed remotely. However, the challenges faced during the implementation is to ensure that the facial occlusion does not present interruptions and poses a problem to the system. Therefore, selecting and testing the correct facial recognition algorithm must be done as shown in the testing phase that the algorithm implemented in this project has successfully recognized and then verify the voter in just under 3 seconds.

Furthermore, the deep learning technology developed by AWS was able to recognize voters with common facial accessories such as spectacles and headwear as described in Table 1 test case but it is also important to note that internet connection would influence the testing result. At the time of testing, the server was connected to the internet with a speed averaging around 110 megabits per second (Mbps). Therefore, slower internet speed would increase the time to complete the authentication process. Finally, this system is able to recognize voters in very low light conditions even though it uses a static image rather than infrared or other devices to capture a facial image. Table 4 shows that the brightness level above 10 would successfully recognize a face. Higher brightness level would be better for the algorithm to recognize facial images. For future research, we intend to add further security features such as adding secure web connection via https to ensure privacy of data transferred between host and server.

V. Conclusion

The online voting system was developed to ensure that voting would be done efficiently, and be accessible to the voter. This system has fulfilled the requirement for improving the current voting approach. Having an accessible application without facing any obstacles such as time and place. It also created a new way to manage and run an election. This system would benefit students and organizers as it provides an online voting with convenience, efficiency and high levels of trust.

Acknowledgment

The authors would like to thank Human Centered Computing – Information Systems Lab Research Group (HCC-ISL), Center for Advanced Computing Technology (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka.

References

[1] W. Kelleher, "Internet Voting in the USA: History and Prospects; or, How NIST has Misled Congress and the American People about Internet Voting Insecurity," *The Internet Voting Research and Education Fund,* 2013.

[2] N. Goodman. "Online Voting: A Path Forward for Federal Elections." https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html (accessed October 10, 2020).

[3] P. Wolf, R. Nackerdien, and D. Tuccinardi, *Introducing Electronic Voting: Essential Considerations*. International Institute for Democracy and Electoral Assistance, 2011.

[4] L. Carter and R. Campbell, "Internet Voting Usefulness: An Empirical Analysis of Trust, Convenience and Accessibility," *Journal of Organizational and End User Computing (JOEUC),* vol. 24, no. 3, pp. 1-17, 2012.

[5] K. Nwachukwu-Nwokeafor and I. Abraham, "Design of a Secured Online Voting System for electoral Process," *International Journal of Innovative Science, Engineering & Technology,* vol. 2, no. 12, pp. 456-471, 2015.

[6] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of e-voting: the past, present and future," *Annals of Telecommunications,* vol. 71, no. 7-8, pp. 279-286, 2016.

[7] M. Warkentin, S. Sharma, D. Gefen, G. M. Rose, and P. Pavlou, "Social identity and trust in internet-based voting adoption," *Government Information Quarterly,* vol. 35, no. 2, pp. 195-209, 2018.

[8] S. S. Harakannanavar, P. C. Renukamurthy, and K. B. Raja, "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends," *International Journal of Advanced Networking and Applications,* vol. 10, no. 4, pp. 3958-3968, 2019.

[9] N. S. Zabidi, N. M. Norowi, and R. W. O. Rahmat, "A Survey of User Preferences on Biometric Authentication for Smartphones," *International Journal of Engineering & Technology,* vol. 7, no. 4.15, pp. 491-495, 2018.

[10] C. Makungu, R. M. Munyao, and J. K. Mwai, "Student Online Voting System," *International Journal of Social Sciences and Information Technology,* vol. 4, no. 5, pp. 175-196, 2018.

[11] Y. Darmayunata, F. A. Syam, and A. Afriansyah, "Implementation And Development Of E-Voting System For Election Of Student Council Chairperson Of SMP Negeri 10 PEKANBARU," *Journal of Applied Engineering and Technological Science (JAETS),* vol. 1, no. 2, pp. 150-161, 2020.

[12] R. Bhuvanapriya, P. Sivapriya, and V. Kalaiselvi, "Smart Voting," in *International Conference on Computing and Communications Technologies (ICCCT)*, 2017: IEEE, pp. 143-147.

[13] L. K. Gupta, U. Tiwari, M. K. Chaudhary, and K. Kasaudhan, "Secure Voting Using Bio-metric Authentication," *International Journal of Computer Sciences and Engineering,* vol. 7, no. 2, pp. 731-735, 2019.

[14] M. Mahajan, Y. Pawar, M. Wagh, S. Alai, and P. Biswas, "M-Vote (Online Voting System)," *International Research Journal of Engineering and Technology,* vol. 5, no. 5, pp. 4099-4102, 2018.

[15] R. Damdoo and K. Kalyani, "Multilevel Voter Identity Protocol for Secure Online Voting," *International Journal of Advanced Trends in Computer Science and Engineering,* vol. 9, no. 3, pp. 3741-3745, 2020.

[16] *Amazon Rekognition Developer Guide*: Amazon Web Services, Inc, 2019, p. 537.

[17] R. Min, A. Hadid, and J.-L. Dugelay, "Improving the Recognition of Faces Occluded by Facial Accessories," in *Face and Gesture 2011*, 2011: IEEE, pp. 442-447.

[18] H. K. Ekenel and R. Stiefelhagen, "Why Is Facial Occlusion a Challenging Problem?," in *International Conference on Biometrics*, 2009: Springer, pp. 299-308.

[19] U. Popić, "Two Approaches for Face Recognition with IOT Technologies," Master of Science in Computer Science and Engineering, Department of Electronics, Information and Bioengineering, Polytechnic University of Milan, Milan, Italy, 2018.

Meor Muhammad Kamal Meor Muhammad Sulaiman, received his Diploma in 2017 from Politeknik Ungku Omar. He is currently an undergraduate student at Universiti Teknikal Malaysia Melaka. He holds various professional certifications such as Cisco Certified Network Professional (CCNP) and Red Hat Certified System Administrator (RHCSA8). His research interest includes Computer Networks and Computer Security.

Mohd Fairuz Iskandar Othman, Ph.D. Senior Lecturer, Department of Computer Systems and Communication, Faculty of Information and Communication Technology, UTeM. He received his Ph.D. in Information Technology from Queensland University of Technology and a Master's degree in Internetworking from the University of Technology, Sydney. His research interests include human behavioral issues in Information Security, IT Governance and Management, and other related topics in Computer Networks and Computer Security.

Wahidah Md Shah, Ph.D. Senior Lecturer, Department of Computer Systems and Communication, Faculty of Information and Communication Technology, UTeM. She holds a Bachelor of Information Technology from Universiti Utara Malaysia, Master of Computer Science from Universiti Teknologi Malaysia, and a Ph.D. in Computer Science from Lancaster University, UK. She is a member of the Information Security, Digital Forensic, and Computer Networking research group. Her research interests include system and networking, network security, and IoT related technology.

Aslinda Hassan, Ph.D. Senior Lecturer, Department of Computer Systems and Communication, Faculty of Information and Communication Technology, UTeM. She received her Ph.D. in Electrical Engineering from Memorial University of Newfoundland, M.Sc. degree in Computer Science, from Universiti Teknologi Malaysia, and B.Sc. degree in Business Administration with honors, from the University of Pittsburgh, Pittsburgh, PA, USA. Her research interests include in vehicular ad hoc network, vehicular communication, wireless ad-hoc network, and wireless sensor network.

Norharyati Harum, Ph.D. Senior Lecturer, Department of Computer Systems and Communication, Faculty of Information and Communication Technology, UTeM. She received her Bachelor in Engineering, MSc. In Engineering and Ph.D. in Engineering from Keio University, Japan. She has experience working in the R&D Department of Next Generation Mobile Communication at Panasonic Japan (2005-2009). Her research interests include the Internet of Things, Wireless Sensor Networks, Next Generation Mobile Communication, and Signal Processing. She is an accomplished inventor, holding patents to radio access technology, and copyrights of products using IoT devices.

Ibrahim Mohammed Alseadoon received his Masters from University of Wollongong (UOW), Wollongong, NSW, Australia in 2008 and PhD from Queensland University of Technology (QUT), Brisbane, QLD, Australia in 2014. He is currently an associate professor at University of Ha'il (UOH), Ha'il, KSA. He is an author of more than 6 articles in the field of Computer Security and Users' Behaviour. He served as general chair and program committee chair for several conferences. In addition, he served as the co-chair of the International Conference on Recent Advances in Computer Systems (RACS-2015) and The 2nd National Computing Colleges Conference (NC3 2017), And Chair for International Conference in Cybersecurity (ICCS) held at UOH