

Penggunaan *Face Recognition* & *Voice Recognition* sebagai Dua Langkah Verifikasi dan Peningkatan Keamanan pada *Smart Door*

Habibullah Zuber Matondang¹, Dodi Wisaksono Sudiharto², Aji Gautama P Satwiko³

^{1,2,3}Fakultas Informatika, Universitas Telkom, Bandung

¹habibzmaton@students.telkomuniversity.ac.id, ²dodiws@telkomuniversity.ac.id,

³ajigps@telkomuniversity.ac.id

Abstrak

Berbanding lurus dengan cepatnya perkembangan zaman, teknologi juga ikut serta mengambil peran dalam perkembangan tersebut terutama pada bidang keamanan. Teknologi biometrik belakangan ini menjadi sangat populer karena mekanisme identifikasi mengandalkan karakteristik fisik dari setiap individu sehingga diharapkan identik dengan sang pemilik identitasnya. Pada beberapa penelitian sebelumnya telah diciptakan pengamanan pintu rumah hanya dengan menerapkan satu langkah verifikasi saja, yaitu menggunakan suara. Namun hasilnya masih terdapat beberapa kesalahan deteksi terhadap pengguna yang berbeda. Tingkat kesalahan deteksi bahkan mencapai 44%. Hal ini tentunya dapat menjadi celah bagi orang asing yang ingin melakukan tindak kejahatan. Berbeda dari penelitian sebelumnya, penelitian ini memanfaatkan dua langkah verifikasi, yaitu menggunakan *voice recognition* dan *face recognition*. Verifikasi dilakukan melalui perangkat yang sudah dipasang di depan pintu. Lalu hasil verifikasi tersebut dikirim melalui komunikasi sinyal *bluetooth* ke modul *bluetooth* HC-05 yang terhubung dengan Arduino Uno. Lalu Arduino Uno mengirimkan perintah ke aktuator untuk membuka pintu. Presisi sistem dengan hanya menggunakan pengenalan suara, didapat hasil keberhasilan sistem sebesar 75%. Namun dengan ditambahkannya tahap berikutnya, yaitu pengenalan wajah, presisi sistem naik menjadi 100%, sehingga pengguna dengan kondisi "*false-negative*" pada pengenalan suara berubah menjadi "*false-positive*" pada tahap pengenalan wajah.

Kata Kunci: Biometrik, *two-steps verication*, *Face Recognition*, *Voice Recognition*, *Arduino*

Abstract

Directly proportional to the rapid development of times, technology also participates in taking part in these developments, especially in the security sector. Biometric technology has recently become very popular because the identification mechanism relies on the physical characteristics of each individual so that it is expected to be identical with the owner of his identity. In some previous studies, the security of house doors has been created by only applying one- step verification, which is using voice. But the result is that there are still some detection errors for different users. The detection error rate even reached 44%. This certainly can be a gap for foreigners who want to commit a crime. Different from previous studies, this study utilizes two-steps verification, namely using voice recognition and face recognition. Verification is done through a device that has been installed in front of the door. Then the verification results are sent via bluetooth signal communication to the HC-05 bluetooth module that is connected to Arduino Uno. Then Arduino Uno sends an order to the actuator to open the door. System precision using only voice recognition, obtained system success results of 75%. But with the addition of the next stage, namely face recognition, the precision of the system increased to 100%, so users with the "false-negative" condition on voice recognition changed to "false-positive" on stage of face recognition

Keywords: *Biometrics*, *Two-Step Verication*, *Face Recognition*, *Voice Recognition*, *Arduino*

1 Pendahuluan

1.1 Latar Belakang

Bersamaan dengan perkembangan zaman, teknologi juga terus berkembang menjadi sangat pesat setiap harinya, meliputi segala bidang. Perkembangan teknologi ini tentunya diharapkan dapat memenuhi kebutuhan manusia yang terus berkembang, terlebih pada kebutuhan keamanan sebagai bentuk pengamanan rumah. Pintu utama rumah merupakan komponen pertama dari kebutuhan keamanan pada rumah tersebut, sebagaimana pintu berfungsi sebagai akses masuk dan keluar dari sebuah rumah, maka dari itu tingkat keamanan dari pintu rumah harus benar-benar diperhatikan.

Beberapa penelitian sebelumnya yang terkait *smartdoor* yaitu dengan menggunakan *voice command* [1], kemudian penelitian selanjutnya yang memanfaatkan teknologi biometrik yang menerapkan *voice recognition* saja, masih memiliki kegagalan untuk memverifikasi *user* yang valid. Bahkan kegagalan bisa mencapai 44% pada gender pria pada perintah tertentu [2]. Angka kegagalan tersebut terbilang cukup tinggi. Salah satu solusi untuk

mengatasi masalah tersebut yaitu dengan melakukan mekanisme yang disebut dengan *two-step verification* [3].

Pada penelitian ini, ditawarkan sebuah sistem keamanan untuk pintu rumah dengan penambahan lapisan keamanan ekstra yang disebut dengan *two-step verification* [3]. Mekanisme ini diterapkan pada *smartdoor* sebagai solusi untuk mengatasi mekanisme *smartdoor* yang hanya menggunakan *single verification* dengan hanya menggunakan pengenalan suara pada penelitian sebelumnya. Sistem ini menggunakan pengenalan suara dan wajah untuk dapat mengakses pintu rumah, Sistem ini menggunakan proses pengenalan suara (*Voice Recognition*) dan pengenalan wajah (*Face Recognition*) terhadap pengguna yang ingin mengakses sistem untuk membuka pintu rumah.

1.2 Topik dan Batasannya

Pada penelitian [2] terdapat angka kesalahan yang cukup tinggi dengan hanya menggunakan *Single Verification* yang hanya menggunakan suara sebagai syarat akses. Maka dari itu, pada penelitian ini dicoba untuk mengatasi permasalahan dari penelitian sebelumnya, dengan memanfaatkan dua *trigger* pengenalan, yaitu pengenalan suara dan pengenalan wajah untuk dapat mengakses pintu rumah, yang secara umum disebut juga dengan *two-step verification*. *Two-step verification* atau sistem verifikasi dua langkah pada penelitian ini adalah dengan menambah lapisan keamanan ekstra yang diterapkan pada *smartdoor* dengan menggunakan mekanisme *face recognition* dan *voice recognition* sebagai dua langkah verifikasi untuk dapat membuka pintu [3].

Dalam menjalankan sistem keamanan untuk *smartdoor* ini diperlukan masukan berupa data suara untuk kemudian diverifikasi kecocokannya dengan data suara yang ada di dalam *server cloud*. Tidak hanya suara, sistem ini juga memerlukan masukan berupa data wajah berupa video singkat berdurasi dua detik untuk kemudian diverifikasi kecocokan dengan data wajah yang ada di dalam *server cloud*. Sistem ini memerlukan jaringan *internet* untuk dapat memproses pengenalan data suara dan data wajah dengan data yang ada pada *server cloud*. Pada penelitian ini pengguna dalam keadaan sehat dalam arti tidak terdapat perubahan suara atau wajah, sehingga masukan suara dan wajah yang digunakan sama seperti pada saat kondisi awal pengguna memasukkan data suara dan wajah sebagai data acuan pada *server cloud*.

1.3 Tujuan

Penelitian ini bertujuan untuk membuat sistem keamanan pada pintu rumah dengan menggunakan *Voice Recognition* dan *Face Recognition* yaitu pengenalan suara dan wajah di mana kemudian hasil dari proses pengenalan sebagai indikator untuk mengirimkan sinyal ke *Arduino* dan *solenoid* kunci pintu sebagai aktuator untuk membuka pintu rumah secara otomatis. Penelitian ini juga menampilkan analisis tingkat keberhasilan antara *two-step verification* menggunakan pengenalan suara dan wajah dibandingkan dengan *single verification* yang hanya menggunakan pengenalan suara.

1.4 Organisasi Tulisan

Setelah pendahuluan yang telah dijelaskan di atas. Bagian-bagian selanjutnya terdiri dari Studi Terkait yang berisi informasi beberapa penelitian sebelumnya yang mempunyai kaitan dengan penelitian ini, Sistem yang dibangun menjelaskan alur perancangan sistem, Evaluasi menjelaskan tentang hasil data pengujian beserta analisis, dan Kesimpulan dari seluruh penelitian.

2 Studi Terkait

Face Recognition adalah metode biometrik untuk mengidentifikasi individu dengan membandingkan gambar secara langsung (dalam bentuk video) atau gambar *digital* dengan rekaman data yang sudah disimpan sebelumnya. Terkait hal ini ada beberapa cara computer untuk mempelajari pengenalan wajah. Secara umum ada 4 langkah cara pengenalan wajah antara lain [4]:

- *Face Detection*
Face Detection adalah proses mencari letak bagian wajah dalam sebuah gambar. Langkah ini mengabaikan siapa orangnya, hanya mengenal wajah manusia saja.
- *Face Preprocessing*
Face Preprocessing adalah proses penyesuaian gambar wajah agar terlihat lebih jelas dan mirip dengan wajah yang lainnya.
- *Collect and Learn Face*
Collect and Learn Face adalah proses penyimpanan banyak wajah yang ada pada *preprocessing* (untuk setiap orang yang harus dikenali), dan belajar bagaimana cara mengenali wajah mereka.
- *Face Recognition*
Face Recognition adalah proses yang memeriksa mana wajah orang yang dikumpulkan sebelumnya dengan wajah yang ada di kamera.

Voice Recognition merupakan salah satu teknologi biometrik yang memanfaatkan suara, kata, dan intonasi dari pengguna. Melalui faktor-faktor tersebut masukan suara kemudian menghasilkan sebuah *waveform* atau sebuah *voice pattern* yang berbeda pada setiap suara seseorang sehingga setiap suara tersebut menghasilkan sebuah

keadaan dan karakteristik yang unik. Teknologi biometrik pada suara ini dapat digunakan sebagai sistem *verification* dengan mengacu pada *voice pattern* tersebut [5].

Penelitian [1] mengacu pada *home automation* dengan hanya mengandalkan perintah suara (*speech to text*) menggunakan *Google Speech Recognition*. Perintah suara di sini digunakan untuk membuka dan mengunci pintu dan jendela secara otomatis.

Pada penelitian [2] dan penelitian [5], merupakan sebuah sistem keamanan yang menggunakan teknologi biometrik dengan memanfaatkan karakteristik suara masing-masing individu menggunakan *voice recognition*. Dengan memanfaatkan keunikan karakter suara dari masing-masing individu maka dapat dibangun sebuah *security system* yang mengandalkan keunikan karakteristik suara.

Pada penelitian [6] dijelaskan sebuah *home security system* yang menggunakan *face recognition* yang berguna untuk mengidentifikasi pengunjung yang datang ke rumah dan juga sebagai kunci untuk mendapatkan akses masuk ke rumah. Sistem akan menangkap wajah pengunjung melalui kamera, lalu sistem melakukan identifikasi dan verifikasi wajah menggunakan *face recognition*. Apabila wajah berhasil teridentifikasi (dikenali), maka sistem akan memberikan akses masuk ke rumah.

Pada penelitian [7], menerapkan sistem *face recognition* dan *sound localization* yang diterapkan pada *smart door*. Sistem *smart door* yang dibangun disini menggunakan *face recognition* dan diintegrasikan dengan *sound localization*, dengan memanfaatkan sumber suara, kemudian kamera akan mencari objek dari sumber (pemilik) suara tersebut, lalu sistem akan menangkap wajah, dan kemudian mengidentifikasi wajah tersebut dengan yang ada dalam *database* sistem.

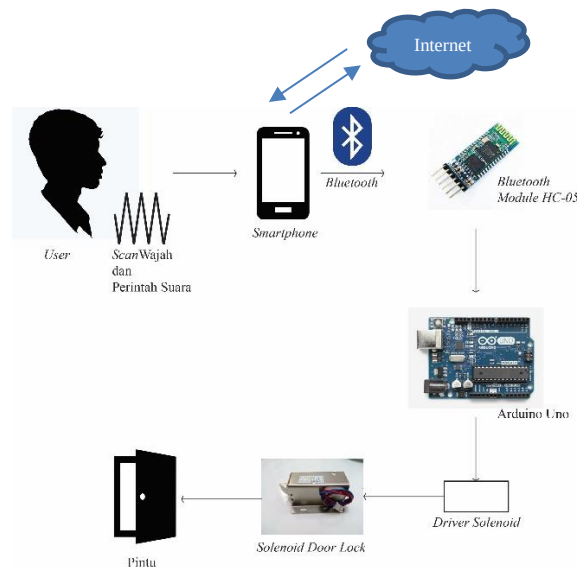
Pada penelitian ini sistem memanfaatkan teknologi biometrik yang dapat digunakan sebagai identifikasi akses melalui pintu rumah. Harapannya mekanisme ini dapat mengurangi tingkat pencurian akibat gagal sistem pengamanan. Teknologi biometrik yang diterapkan pada penelitian kali ini yaitu verifikasi suara (*voice recognition*) dan verifikasi wajah (*face recognition*). Teknologi biometrik yaitu *face recognition* dan *voice recognition* yang diterapkan pada sistem menggunakan API. API adalah singkatan dari *Application Programming Interface*, yang merupakan perantara perangkat lunak yang memungkinkan dua aplikasi untuk dapat berbicara satu sama lain [8]. Pada penelitian ini API yang digunakan pada sistem merupakan API yang disediakan oleh *VoiceIt* [9].

VoiceIt merupakan penyedia *platform* teknologi biomektriks berbasis *cloud-computing* yang dewasa ini menjadi sangat populer [9]. Teknologi biometrik yang disediakan mengandalkan keunikan karakteristik suara dan karakteristik wajah yang dimiliki oleh setiap individu. Pengenalan suara dan pengenalan wajah pengguna diproses langsung pada *cloud* yang sudah disediakan oleh penyedia yaitu *VoiceIt*. *VoiceIt* membantu membangun dan mewujudkan solusi keamanan dengan mengandalkan teknologi biometrik karena *VoiceIt* menyediakan API dalam banyak bahasa pemrograman yang tentunya dengan dokumentasi baik dapat mempermudah proses pengembangan sistem [9].

Pada penelitian ini, penentuan verifikasi *user* sistem menggunakan data nilai *confidence* sebagai info indikator pengenalan antara data uji dengan data acuan yang tersimpan pada *server cloud*. Nilai *confidence* merupakan nilai kepastian yang dihasilkan oleh data uji atau data sampel terhadap data acuan yang berada di dalam *server cloud* dengan membandingkan setiap satu karakteristik yang sama [10].

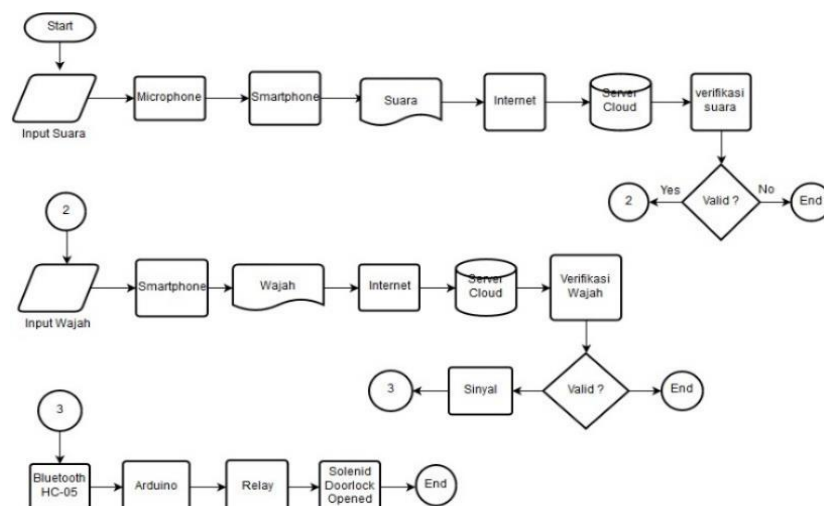
3 Sistem yang Dibangun

Penelitian ini dimaksudkan untuk membangun sebuah sistem keamanan pada pintu berbasis teknologi biometrik yaitu *voice recognition* dan *face recognition*. Secara umum sistem yang dibangun berupa aplikasi yang menerima masukan berupa rekaman suara dan rekaman video wajah pengguna, kemudian menghasilkan keluaran berupa hasil verifikasi/kecocokan data masukan dengan data di dalam *server cloud*. Sistem dibangun menggunakan bahasa pemrograman *Java-Android* dengan menggunakan aplikasi *Android Studio* yang dihubungkan dengan *server cloud voiceit* melalui jaringan internet, kemudian dihubungkan ke *Microcontroller* yaitu *Arduino Uno*. Di bawah ini merupakan gambaran umum dari sistem yang dibangun.



Gambar 1. Gambaran Umum Sistem

Pada Gambar 2 dapat dilihat bahwa sistem keamanan ini memiliki beberapa tahap proses mulai dari proses pengenalan sampai pada terbuka pintu secara otomatis. Tahap pertama dalam sistem keamanan pintu ini merupakan tahap verifikasi suara. Dalam tahap ini pengguna diminta memasukkan data suara ke sistem menggunakan *microphone* untuk diverifikasi kecocokan suara beserta kalimat yang digunakan dengan data acuan melalui internet pada *server cloud* dari *VoiceIt* yang telah disediakan. Jika suara pengguna valid terverifikasi maka akan masuk ke tahap selanjutnya. Tahap selanjutnya pada sistem keamanan pintu merupakan tahap verifikasi wajah. Dalam tahap ini pengguna memasukkan data wajah ke sistem melalui kamera yang ada pada *smartphone*. Data wajah tersebut kemudian diverifikasi kecocokannya dengan data acuan melalui internet pada *cloud server* *VoiceIt* yang telah disediakan. Jika wajah pengguna valid terverifikasi maka *smartphone* akan mengirimkan sinyal valid ke *Arduino Uno*. Sinyal valid yang diberikan dari *smartphone* kemudian dikirim melalui komunikasi *Bluetooth* menggunakan perangkat HC-05 ke *microcontroller* yaitu *Arduino Uno*. *Arduino Uno* sebagai motor mengirimkan perintah kepada *relay single channel 5V* untuk kemudian menggerakkan aktuator *solenoid* kunci pintu 12V untuk membuka pintu.



Gambar 2 Flowchart Sistem

3.1 Komponen Perangkat Keras dan Perangkat Lunak yang digunakan

Perangkat keras yang digunakan pada system ini yaitu,

- Smart-Phone sebagai *Interface* input wajah dan suara
- *Arduino Uno* sebagai perangkat control aktuator
- Aktuator berupa *Solenoid Door-Lock* 12V
- *Relay* 5V, sebagai saklar untuk aktuator.

Perangkat Lunak yang digunakan pada system ini yaitu,

- Sistem Operasi Android
- *Android Studio IDE*
- *Arduino IDE*
- *VoiceIt Android API*

4 Evaluasi

4.1 Skenario Pengujian

4.1.1 Kebutuhan Fungsionalitas

Skenario ini menguji fungsionalitas dari sistem apakah berjalan baik atau tidak. Selain itu juga bertujuan untuk memperoleh waktu respon sistem terhadap proses yang sedang terjadi. Berikut beberapa pengujian yang dilakukan:

- Pengujian terhadap sistem dapat melakukan *voice recognition* dan *face recognition*
- Pengujian terhadap sistem dapat mengirimkan data dari *smartphone* ke *Arduino Uno*.

4.1.2 Perangkat Keras

Skenario pengujian ini dilakukan terhadap perangkat keras yang digunakan untuk membangun sistem. Pengujian yang dilakukan yaitu pengujian terhadap kemampuan *microcontroller (Arduino Uno)* dalam memproses sinyal dari *smartphone* melalui HC-05 untuk diteruskan ke aktuator untuk membuka pintu secara otomatis.

4.2 Hasil Pengujian

Pengujian yang dilakukan berupa verifikasi suara serta wajah sebanyak 30 orang berbeda dengan rincian 12 orang berjenis kelamin laki-laki dan 18 orang berjenis kelamin perempuan. Setiap orang melakukan uji verifikasi suara dan wajah masing masing sebanyak tiga kali uji. Sistem diinisialisasi dengan 3 pengguna *verified* berjenis kelamin laki-laki, namun untuk pengujian hanya digunakan salah satu saja. Data pengguna yang diuji berupa data suara serta wajah sebagai masukan perangkat yang kemudian diverifikasi dengan data di dalam *server cloud*.

Pada penelitian ini, penentuan verifikasi pengguna pada sistem menggunakan data nilai *confidence* yang dikeluarkan oleh API sebagai info indikator pengenalan antara data uji dengan data acuan yang tersimpan pada *server cloud*. Nilai *confidence* merupakan nilai kepastian yang dihasilkan oleh data uji atau data sampel terhadap data acuan yang ada di dalam *server cloud* dengan membandingkan setiap satu karakteristik yang sama. Nilai *confidence* merepresentasikan tingkat keyakinan akurasi antara data uji (*sample*) dan data acuan dengan karakteristik pembanding yang sama [10].

Pada pengujian data suara dilakukan dengan jarak maksimal 30 cm dari perangkat dengan menekan *button "voice verification"* pada perangkat dan mengucapkan kalimat "*buka pintu*" yang tertera pada *interface* perangkat di depan pintu. Pada pengujian data wajah dilakukan dengan jarak maksimal 50 cm dari perangkat. Setelah terverifikasi sistem mengeluarkan info berupa nilai *confidence* setiap data *user*.

Table 1. *Hasil Rata-rata confidence*

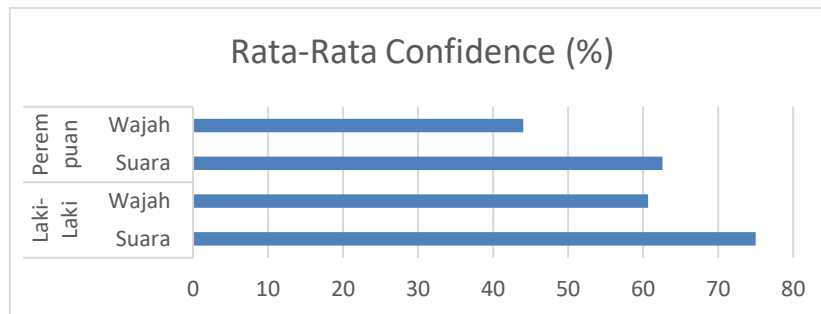
No	Jenis Kelamin	Jenis Verifikasi	Rata-Rata Confidence (%)	Rata-Rata Waktu Proses Verifikasi (s)
1	Laki-Laki	Suara	75	1,25
		Wajah	60,65	10,10
2	Perempuan	Suara	62,57	1,29
		Wajah	44,03	10,15

4.3 Analisis Hasil Pengujian

Pada proses pengujian, data yang diambil adalah data nilai *confidence* antara data pengguna yang menjadi sampel uji dengan data pengguna yang telah terdaftar pada *server cloud*. Tabel 1 menampilkan nilai rata-rata dari nilai *confidence* yang dihasilkan. Nilai *confidence* merepresentasikan akurasi kecocokan antara data uji pengguna yang tidak terdaftar (*unverified user*) dengan data pengguna yang telah terdaftar (*verified*) pada *server cloud*.

Dilihat dari perbedaan jenis kelamin, pada tabel 1 nilai *confidence* suara berjenis kelamin perempuan lebih kecil dibanding dengan berjenis laki-laki, ini menerangkan bahwa tingkat perbedaan yang cukup tinggi antara suara perempuan dengan suara laki-laki. Perbedaan suara ini tentunya berdasarkan beberapa faktor seperti frekuensi, *amplitudo*, *pitch*, *volume*, *timbre* dan *formant* suara. Dilihat dari *pitch*, suara laki-laki memiliki nilai *pitch* yang lebih rendah dari perempuan, sedangkan untuk nilai *formant*, laki-laki memiliki nilai yang lebih tinggi dari perempuan [11]. Sama halnya seperti suara, wajah antara laki-laki dan perempuan juga memiliki faktor pembeda yaitu bentuk ekor mata (pelipis) kanan dan kiri, kumis serta posisi dan bentuk bibir [11]. Hal ini

menunjukkan bahwa data suara dan wajah berjenis kelamin perempuan memiliki peluang *unverified* yang lebih tinggi dari data suara dan wajah berjenis kelamin laki-laki dikarenakan data acuan pada *server cloud* yang digunakan merupakan data suara dan wajah berjenis kelamin laki-laki.



Gambar 3. Grafik Perbedaan Confidence

Tabel 2 menampilkan hasil nilai *confidence* beserta status dari setiap data uji pengguna berjenis kelamin laki-laki yang tidak didaftarkan ke dalam *server cloud* sebelumnya. Hasil data uji menunjukkan terdapat 3 pengguna yang tidak terdaftar namun pengguna dinyatakan "*verified*" dan berhasil mengakses dan melewati tahap keamanan awal yaitu *voice verification* dengan nilai *confidence* yang tinggi. Kemudian pada tahap keamanan selanjutnya yaitu *face verification*, pengguna dinyatakan "*unverified*" dengan nilai *confidence* yang rendah sehingga pengguna tidak dapat mengakses pintu rumah. Hal ini menunjukkan sistem pengenalan wajah memiliki tingkat akurasi dan keberhasilan yang lebih baik dari pengenalan suara dan layak untuk dijadikan sebagai fitur keamanan lanjutan setelah pengenalan suara.

Tabel 2 adalah data uji dari nilai *confidence*. Bila nilainya lebih kecil dari 80 maka dianggap "*unverified*" karena nilai tersebut dijadikan *threshold* dari sistem. Untuk *single verification* pada suara wanita hasilnya adalah 100% *unverified*, begitu pun untuk *face confidence*-nya. Namun untuk laki-laki, hasilnya dapat dilihat pada tabel sbb:

Table 2. Hasil data uji

No	Nama	Jenis Kelamin	Percobaan (ke-)	Voice Confidence	Status	Face Confidence	Status
1	Reza	Laki-Laki	1	64,7	Unverified	57,76	Unverified
			2	69,5	Unverified	48,79	Unverified
			3	56,86	Unverified	50,45	Unverified
2	Maulana	Laki-Laki	1	64,5	Unverified	61,47	Unverified
			2	68,5	Unverified	64,15	Unverified
			3	66,5	Unverified	62,13	Unverified
3	Arif	Laki-Laki	1	78	Unverified	54,15	Unverified
			2	84	Verified	53,4	Unverified
			3	82	Verified	49,82	Unverified
4	Ari	Laki-Laki	1	84,5	Verified	62,78	Unverified
			2	85	Verified	62,1	Unverified
			3	83	Verified	60,32	Unverified
5	Fitrah	Laki-Laki	1	83	Verified	59,25	Unverified
			2	79	Unverified	56,73	Unverified
			3	84,5	Verified	58,86	Unverified
6	Cheki	Laki-Laki	1	71,23	Unverified	57,39	Unverified
			2	75,06	Unverified	55,05	Unverified
			3	73,90	Unverified	60,71	Unverified
7	Aan	Laki-Laki	1	78,27	Unverified	57,59	Unverified
			2	75,84	Unverified	56,19	Unverified
			3	77,68	Unverified	60,15	Unverified
8	Rahmat	Laki-Laki	1	83	Verified	64,61	Unverified
			2	82	Verified	58,95	Unverified
			3	79,9	Unverified	67,53	Unverified
9	Fiqi	Laki-Laki	1	73,83	Unverified	68,96	Unverified
			2	74,57	Unverified	66,75	Unverified
			3	77,97	Unverified	66,56	Unverified

No	Nama	Jenis Kelamin	Percobaan (ke-)	Voice Confidence	Status	Face Confidence	Status
10	Rizza	Laki-Laki	1	75,63	Unverified	65,1	Unverified
			2	74,95	Unverified	59,02	Unverified
			3	75,46	Unverified	65,39	Unverified
11	Hendri	Laki-Laki	1	78,62	Unverified	55,1	Unverified
			2	76,48	Unverified	61,84	Unverified
			3	74,84	Unverified	65,57	Unverified
12	Aswin	Laki-Laki	1	72,97	Unverified	64,25	Unverified
			2	75,64	Unverified	56,9	Unverified
			3	77,48	Unverified	68,11	Unverified
Precision					75%		100%

Pada Tabel 2 merupakan hasil data uji berjenis kelamin laki-laki yang tidak terdaftar pada *server cloud*. Percobaan dilakukan sebanyak tiga kali pada setiap orang. Pada sistem, pengguna yang berhasil melewati tahap verifikasi memiliki nilai *confidence* di atas 80% dan dengan status “*verified*”. Hasil Tabel 2 menunjukkan bahwa adanya beberapa pengguna tidak terdaftar namun berhasil melewati tahap pengenalan suara. Hal ini tentu berpengaruh pada tingkat keamanan dikarenakan ketidaktepatan yang diberikan sistem pada tahap pengenalan suara.

$$precision = \frac{a}{a+b} \times 100\% \quad (1)$$

Pendekatan (1) digunakan untuk menghitung presisi dari sistem yaitu tingkat ketepatan antara informasi yang diminta pengguna dengan informasi yang diberikan oleh sistem, di mana *a* sebagai *true-positive*, lalu *b* sebagai *false-negative*. Kondisi *false-negative* digambarkan terhadap pengguna yang tidak terdaftar pada *server cloud* namun berhasil melewati sistem pengenalan, sedangkan kondisi *true-positive* digambarkan terhadap pengguna yang tidak terdaftar pada *server cloud* dan gagal melewati sistem pengenalan. Pada Tabel 2 dapat dilihat nilai presisi yang dihasilkan oleh sistem pengenalan suara adalah 75%, sedangkan untuk nilai presisi yang dihasilkan sistem pengenalan wajah lebih tinggi mencapai 100%. Hasil presisi tersebut menjelaskan bahwa pada tahap pengenalan suara masih memiliki celah bagi pengguna yang tidak terdaftar berhasil masuk, namun dapat diatasi dengan tahap selanjutnya (*two-steps verification*) yaitu sistem pengenalan wajah yang memiliki nilai presisi yang lebih tinggi.

5 Kesimpulan dan Saran

5.1 Kesimpulan

Dilihat dari nilai *confidence* yang dihasilkan, pengguna berjenis kelamin laki-laki memiliki nilai *confidence* yang lebih tinggi dari pengguna berjenis kelamin perempuan. Hal ini dapat dijelaskan dalam *human behavior* bahwa sistem lebih mudah percaya kepada laki-laki sebagai seseorang yang berhak mengakses sistem ketimbang perempuan. Sebagai akibatnya kesalahan untuk membedakan antara individu yang tidak berhak melakukan akses dengan individu yang berhak melakukan akses untuk yang berjenis kelamin laki-laki lebih besar daripada yang berjenis kelamin perempuan.

Dalam penelitian ini, sistem diuji dengan 30 orang yang berbeda yang terdiri dari 12 laki-laki dan 18 perempuan dengan masing-masing tiga kali percobaan. Pada percobaan dapat dilihat bahwa nilai *confidence* pengenalan suara lebih tinggi dibanding dengan nilai *confidence* pengenalan wajah. Hal ini menerangkan bahwa suara pengguna yang tidak terdaftar pada *server cloud* dengan suara pengguna acuan yang ada pada *server cloud* terutama yang berjenis kelamin laki-laki memiliki nilai yang lebih tinggi untuk dianggap sebagai orang yang sama ketimbang yang berjenis kelamin perempuan. Hal ini juga dibuktikan dengan adanya beberapa pengguna dengan kondisi *false-negative* pada tahap sistem pengenalan suara pada yang berjenis kelamin laki-laki.

Pada tahap langkah pengamanan selanjutnya yaitu pengenalan wajah, pengguna tersebut tidak dapat mengakses dan dinyatakan sebagai pengguna “*unverified*”. Sehingga setidaknya untuk fungsi pengamanan, nilai *false-negative* dapat berubah menjadi *false-positive*.

5.2 Saran

Pada penelitian kedepannya, diharapkan dapat dilakukan pengukuran yang lebih komprehensif terkait *two-step verification*. Karena pada dasarnya pada pengukuran penelitian ini masih terpisah antara nilai *confidence* dari pengenalan suara dan nilai *confidence* dari pengenalan wajah.

Referensi

- [1] R. L. H. Pakpahan, D. W. Sudiharto and A. G. P. Satwiko, "The prototype of automated doors and windows by using voice commands," in International Seminar on Application for Technology and Communication, 2016.
- [2] A. Imario, D. W. Sudiharto, and E. Ariyanto, "The validated voice recognition measurement of several tribes in indonesia using Easy VR 3.0. Case Study: The Prototype of Automated Doors," in Int. Semin. Appl. Technol. Inf. Commun., 2017, 3–7.
- [3] Google, "Mengaktifkan Verifikasi 2 Langkah," https://support.google.com/accounts/answer/185839?hl=id&visit_id=1-636527603696737280-2617947003&rd=1.
- [4] R. S. D. Lélis Baggio, S. Emami, D. Millán Escrivá, K. Ievgen, N. Mahmood, J. Saragih, Mastering OpenCV with Practical Computer Vision Projects, Packt Publishing, 2012.
- [5] R. A. Rashid, N. H. Mahalin, M. A. Sarijari, and A. A. A. Aziz, "Security system using biometric technology: Design and implementation of voice recognition system (VRS)," in Int Conf. Comput. Commun. Eng. (ICCCE), 2008, pp. 898–902.
- [6] M. Sahani, C. Nanda, A. K. Sahu, and B. Pattnaik, "Home security system based on face recognition," in Int. Conf. Circuit, Power Comput. Technol. [ICCPCT], 2015.
- [7] T. Kim, H. Park, S. H. Hong, and Y. Chung, "Integrated system of face recognition and sound localization for a smart door phone," IEEE Trans. Consum. Electron., vol. 59, no. 3, pp. 598–603, 2013.
- [8] M. Stowe, Undisturbed REST: A Guide to Designing the Perfect API. MuleSoft, 2015.
- [9] "VoiceIt API," VoiceIt, 2007. [Online]. Available: <https://voiceit.io/>. [Diakses 26 July 2018].
- [10] S. Bengio, C. Marcel, S. Marcel and J. Mariethoz, "Confidence measures for multimodal identity verification," Elsevier, pp. 5-6, 2002.
- [11] S. B. Bhaskoro and A. R. W. D., "Aplikasi pengenalan gender menggunakan suara," in Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta, 2012.
- [12] R. K, K. B. Raja, V. K. R and L. M. Patnaik, "Feature extraction based face recognition, gender and age classification," International Journal on Computer Science and Engineering, vol. 02, no. 01S, pp. 7-9, 2010.