इंटरनेशनल जर्नल ऑफ सिक्योरिटी, प्राइवेसी एंड ट्रस्ट मैनेजमेंट (IJSPTM) खंड 9, संख्या 1/2, मई 2020

आवाज़ बायोमेट्रिक पहचान प्रमाणीकरण IoT उपकरणों के लिए मॉडल

सलाहाल्डीन दुरैबी1 , फ्रेडरिक टी. शेल्डन2 और वसीम अलहमदानी3

1कंप्यूटर विज्ञान विभाग इडाहो विश्वविद्यालय मॉस्को, आईडी, 83844, यूएसए
1कंप्यूटर विज्ञान विभाग जाज़ान विश्वविद्यालय जाज़ान, 45142, केएसए
2कंप्यूटर विज्ञान विभाग इडाहो विश्वविद्यालय, कोयूर डी'एलीन, आईडी 83814, यूएसए
3कम्प्यूटर और सूचना विज्ञान विभाग, कंबरलैंड्स विश्वविद्यालय,
विलियम्सबर्ग, केवाई, 40769, यूएसए

अमूर्त

व्यवहारिक बायोमेट्रिक प्रमाणीकरण को इंटरनेट ऑफ थिंग्स (IoT) पारिस्थितिकी तंत्र को सुरक्षित करने के लिए एक आशाजनक दृष्टिकोण माना जाता है। इस पत्र में, हमने IoT के उपयोगकर्ता प्रमाणीकरण में वॉयस रिकग्निशन सिस्टम को नियोजित करने की आवश्यकता और उपयुक्तता की जांच की। वॉयस रिकग्निशन सिस्टम को पूरा करने में उपयोग किए जाने वाले उपकरणों और तकनीकों की समीक्षा की गई है, और IoT वातावरण के लिए उनकी उपयुक्तता पर चर्चा की गई है। अंत में, IoT पारिस्थितिकी तंत्र उपयोगकर्ता प्रमाणीकरण के लिए एक वॉयस रिकग्निशन सिस्टम प्रस्तावित किया गया है। प्रस्तावित प्रणाली के दो चरण हैं। पहला नामांकन चरण है जिसमें एक पूर्व-प्रसंस्करण चरण शामिल है जहां नामांकन प्रक्रिया के लिए आवाज से शोर को हटा दिया जाता है, फीचर निष्कर्षण चरण जहां उपयोगकर्ता की आवाज से फीचर लक्षण निकाले जाते हैं, और मॉडल प्रशिक्षण चरण जहां वॉयस मॉडल को IoT उपयोगकर्ता के लिए प्रशिक्षित किया जाता है।

और दूसरा चरण यह सत्यापित करता है कि पहचान का दावा करने वाला व्यक्ति IoT डिवाइस का स्वामी है या नहीं। IoT प्रौद्योगिकियों की सीमित संसाधनों के आधार पर, पाठ-निर्भर आवाज़ पहचान प्रणालियों की उपयुक्तता को बढ़ावा दिया जाता है। इसी तरह, प्रस्तावित प्रणाली में MFCC सुविधाओं के उपयोग पर विचार किया जाता है।

कीवर्ड

इंटरनेट ऑफ थिंग्स, प्रमाणीकरण, प्रवेश नियंत्रण, बायोमेट्रिक, आवाज पहचान, सुरक्षा, साइबर सुरक्षा

1 परिचय

बायोमेट्रिक्स आधारित प्रमाणीकरण किसी व्यक्ति की शारीरिक और व्यवहारिक विशेषताओं का उपयोग करके उसकी पहचान का स्वतः सत्यापन करने के बारे में है। IoT पारिस्थितिकी तंत्र को सुरक्षित करने के लिए बायोमेट्रिक प्रमाणीकरण का उपयोग करना एक आशाजनक दृष्टिकोण है [1]। सामान्य तौर पर, बायोमेट्रिक प्रमाणीकरण प्रणाली में दो चरण शामिल होते हैं। ये उपयोगकर्ता का नामांकन और सत्यापन हैं। दोनों चरणों पर अनुभाग 2 में चर्चा की गई है।
वॉयस फीचर की पोर्टेबिलिटी, स्थिरता और गोपनीयता के कारण, वॉयस रिकग्निशन ऑथेंटिकेशन ने हाल के वर्षों में व्यापक ध्यान और अनुप्रयोग आकर्षित किया है [2]। वॉयस रिकग्निशन सिस्टम बहुमुखी, उपयोग में आसान और स्वभाव से गैर-घुसपैठिए हैं। इसे सटीक माना जाता है और इसके लिए विशेष उपकरणों की आवश्यकता नहीं होती है, विभिन्न सेवाओं के लिए दूरस्थ प्रमाणीकरण के लिए बस एक स्मार्टफोन ही पर्याप्त है। इसी तरह, अन्य बायोमेट्रिक प्रमाणीकरण मापदंडों में वॉयस उपयोगकर्ता प्रमाणीकरण के लिए आवश्यक और उपयोग करने के लिए सबसे सरल और आसान यूनिमॉडल है [3]।

परिणामस्वरूप, हाल के वर्षों में, वॉयस रिकग्निशन ने विभिन्न प्रौद्योगिकी अग्रणी कंपनियों को आकर्षित किया है। उदाहरण के लिए, Google ने उपयोगकर्ताओं को अपने स्मार्टफ़ोन को अनलॉक करने की अनुमति देने के लिए Android-आधारित ट्रस्टेड वॉयस प्रदान किया है। Saypay के mPayment उपभोक्ता लेनदेन करने के लिए वॉयस पासवर्ड का उपयोग करते हैं [2]। इसके अलावा, Google ने IoT में उपयोगकर्ताओं को प्रमाणित करने के लिए स्वचालित स्पीकर पहचान के रोजगार को बढ़ावा दिया है [4]। IoT पारिस्थितिकी तंत्र की प्रकृति के बारे में, विशेष रूप से इसके मोबाइल रिमोट कंट्रोल के बारे में, उपयोगकर्ता प्रमाणीकरण के लिए वॉयस रिकग्निशन का उपयोग हो सकता है

डीओआई: 10.5121/आईजेएसपीटीएम.2020.9201

एक जबरदस्त लाभ [5]। इसके अलावा, वॉयस बायोमेट्रिक के IoT पारिस्थितिकी तंत्र से संबंधित लाभ में छोटे भंडारण की आवश्यकता, संचरण में आसानी और गैर-घुसपैठ शामिल हैं [6]।

इस पेपर में, IoT इकोसिस्टम में इस्तेमाल की जाने वाली वॉयस रिकग्निशन ऑथेंटिकेशन सिस्टम का प्रस्ताव दिया गया है। IoT डिवाइस और रिमोट एक्सेस की संसाधन सीमितता को ध्यान में रखा गया है। उदाहरण के लिए, प्रस्तावित सिस्टम में फीचर्स निकालने के लिए MFCC और यूजर वेरिफिकेशन के लिए सपोर्ट वेक्टर मशीन (SVM) का इस्तेमाल किया जाता है जो रिमोट स्पीकर आइडेंटिफिकेशन के लिए मौलिक है [7]।

प्राप्त वॉयस डेटा से निकाली जा सकने वाली वॉयस विशेषताएँ उच्च-स्तरीय या निम्न-स्तरीय विशेषताएँ हो सकती हैं। स्वर तंत्र से संबंधित निम्न-स्तरीय विशेषताएँ वर्णक्रमीय मापों से प्राप्त होती हैं, जबकि उच्च-स्तरीय विशेषताएँ बोली, शब्द उपयोग, वार्तालाप पैटर्न आदि जैसे व्यवहार संकेतों से प्राप्त होती हैं। उच्च-स्तरीय विशेषताओं को निकालना मुश्किल होता है लेकिन वे शोर के प्रति कम संवेदनशील होती हैं [8, 9]। इस प्रकाश में, IoT उपयोगकर्ता प्रमाणीकरण के लिए निम्न-स्तरीय संकेतों का निष्कर्षण आवश्यक है।

पेपर का शेष भाग इस प्रकार है: खंड 2 पृष्ठभूमि है, खंड 3 संबंधित कार्य प्रस्तुत करता है, और खंड 4 अनुसंधान अंतराल पर चर्चा करता है, खंड 5 प्रस्तावित प्रणाली प्रस्तुत करता है, खंड 6 सीमाएं और धारणाएं प्रस्तुत करता है, और खंड 7 निष्कर्ष है।

2। पृष्ठभूमि

मशीन से मशीन (M2M), मशीन से व्यक्ति या व्यक्ति से व्यक्ति जैसे परस्पर जुड़े हुए वातावरण ही IoT पारिस्थितिकी तंत्र बनाते हैं। IoT पारिस्थितिकी तंत्र में स्मार्ट ऑब्जेक्ट आपस में संवाद कर सकते हैं, चीजें एक-दूसरे का पता लगा सकती हैं और सब कुछ एक-दूसरे के साथ और स्थानीय वातावरण के साथ बातचीत कर सकता है। इन अंतर्संबंधों को रिमोट सेंसिंग और ट्रैकिंग क्षमताओं के साथ सुगम बनाया गया है और प्रत्येक इकाई को इंटरनेट, वाई-फाई, ज़िगबी या ब्लूटूथ के माध्यम से डेटा ट्रांसफर प्रदान किया जाता है। विशेष रूप से, संगठनों को व्यवसाय, सामाजिक या अनुसंधान विश्लेषण के लिए ऐसे डेटा की आवश्यकता हो सकती है [10]। इस कारण से, बहुत सी जानकारी संग्रहीत, प्रबंधित और संसाधित की जाती है। इन निजी डेटा तक पहुँच के लिए सुरक्षित पहुँच नियंत्रण का अभ्यास करने की आवश्यकता है।

बताया गया है कि पासवर्ड जैसे पारंपरिक प्रमाणीकरण तंत्र का उपयोग IoT पारिस्थितिकी तंत्र के लिए अपर्याप्त है। इस प्रकार, बायोमेट्रिक तकनीक को IoT निजी डेटा की सुरक्षा के लिए एक बेहतर विकल्प माना जाता है [11]।

बायोमेट्रिक्स या तो शारीरिक या व्यवहारिक होते हैं। वॉयस रिकग्निशन ऑथेंटिकेशन मैकेनिज्म व्यवहारिक बायोमेट्रिक योजनाओं का हिस्सा है [12]। आवाज़ों के व्यक्तिगत विवरणों के आधार पर, शोधकर्ताओं ने कई प्रमाणीकरण योजनाएँ प्रस्तावित की हैं जो वॉयस रिकग्निशन का उपयोग करती हैं। वॉयस रिकग्निशन "आवाज़ के संकेतों के आधार पर स्वचालित रूप से पहचानने की प्रक्रिया है कि कौन बोल रहा है" [13]। हालाँकि, वॉयस रिकग्निशन योजनाएँ आमतौर पर मालिक की आवाज़ बदलने और रिकॉर्ड की गई मालिक की आवाज़ के इस्तेमाल के मुद्दों से ग्रस्त हैं। यानी, मालिक की आवाज़ पर्यावरणीय कारणों, जैसे थकान, सर्दी या फ्लू के कारण बदल सकती है।

इसी तरह, हमलावर वैध आवाज़ के मालिक की आवाज़ रिकॉर्ड कर सकते हैं और बाद में इसका इस्तेमाल अवैध प्रमाणीकरण के लिए कर सकते हैं [14]।

आवाज़ पहचान प्रक्रिया में दो मुख्य चरण होते हैं। यह आवाज़ नामांकन और आवाज़ सत्यापन है जैसा कि चित्र 1 में दर्शाया गया है। पहला चरण यह निर्धारित करने के लिए आवश्यक है कि आवाज़ डेटाबेस में एक नमूना है या नहीं, और दूसरा चरण पहचानता है कि यह डेटाबेस में कौन सा नमूना है। आवाज़ नामांकन प्रक्रिया में, कुछ शोधपत्र दावा करते हैं कि इस प्रक्रिया में डेटा संग्रह, फ़ीचर निष्कर्षण, फ़ीचर टेम्पलेट निर्माण और टेम्पलेट संग्रहण सहित चार चरण शामिल हैं। कुछ शोधकर्ता ऐसे भी हैं जिन्होंने एक और चरण जोड़ा है जो डेटा संग्रह के बाद और फ़ीचर निष्कर्षण चरणों से पहले आता है। वे इसे प्री-प्रोसेसिंग कहते हैं, और इसका उद्देश्य एकत्रित डेटा से शोर को हटाना है। इसी तरह, सत्यापन प्रक्रिया में डेटा संग्रह, फ़ीचर निष्कर्षण जैसे चरण शामिल हैं

निष्कर्षण, टेम्पलेट मिलान और मिलान निर्णय। इन पर निम्नलिखित उपखंडों में चर्चा की गई है:

2.1. डेटा संग्रह/अधिग्रहण

आवाज़ को इकट्ठा करने की प्रक्रिया और कुछ नहीं बल्कि वक्ता की आवाज़ का डिजिटलीकरण है। यह आमतौर पर एक माइक्रोफोन का उपयोग करके पूरा किया जाता है जो नमूना दर पर आवाज़ को कैप्चर करता है।
इसके बाद, इन आंकड़ों को बाद में प्रसंस्करण के लिए एक कंप्यूटिंग डिवाइस पर भेजा जाता है। कुछ शोधकर्ता इस प्रक्रिया को डेटासेट जनरेशन या डेटा सैंपल कलेक्शन [15] कहते हैं। आवाज़ इकट्ठा करने के दो मुख्य तरीके हैं, यानी फिक्स्ड टेक्स्ट और रैंडम नंबर स्ट्रिंग। हालाँकि, सिस्टम आमतौर पर बाद वाले का उपयोग करते हैं जहाँ संख्याओं की प्रत्येक स्ट्रिंग में 0 से 9 की सीमा के साथ 8 अरबी अंक होते हैं [16]। इस प्रक्रिया में एक प्री-प्रोसेसिंग चरण शामिल हो सकता है जहाँ मूल आवाज़ से शोर को हटा दिया जाता है [17]।

2.2. फ़ीचर निष्कर्षण

विशेषताएं एकत्रित किए गए ध्वनि डेटा से निकाली जाती हैं और पूर्ववर्ती प्रक्रिया में पूर्व-संसाधित की जाती हैं।
ये विशेषताएँ आंतरिक परिवर्तनशीलता के लिए मज़बूत होनी चाहिए जो तनाव या बीमारियों के कारण उपयोगकर्ता की आवाज़ में विकृति पैदा कर सकती हैं। सामान्य तौर पर, उपयोगकर्ता की आवाज़ से विशेषताएँ निकालने में कई तकनीकें शामिल होती हैं। इनमें रैखिक पूर्वानुमान सेप्स्ट्रल गुणांक (LPCC) और मेल-फ़्रीक्वेंसी सेप्स्ट्रल गुणांक (MFCC) [16, 17] शामिल हो सकते हैं, लेकिन इन्हीं तक सीमित नहीं हैं। दूसरे को कुछ शोधों में सीमित संसाधनों और अनियंत्रित परिचालन स्थितियों के मुद्दे को दूर करने के लिए नियोजित किया गया है जो IoT तकनीकों की प्रकृति के समान हैं [18]।

इस प्रक्रिया के बाद नामांकन और सत्यापन प्रक्रिया अलग-अलग मार्ग अपनाती है। उदाहरण के लिए, नामांकन प्रक्रिया के लिए, टेम्प्लेट निर्माण और टेम्प्लेट संग्रहण फ़ीचर निष्कर्षण के बाद आते हैं, जबकि सत्यापन प्रक्रिया में, टेम्प्लेट मिलान और निर्णय लेना फ़ीचर निष्कर्षण के बाद आते हैं।

2.3. टेम्पलेट निर्माण और संग्रहण

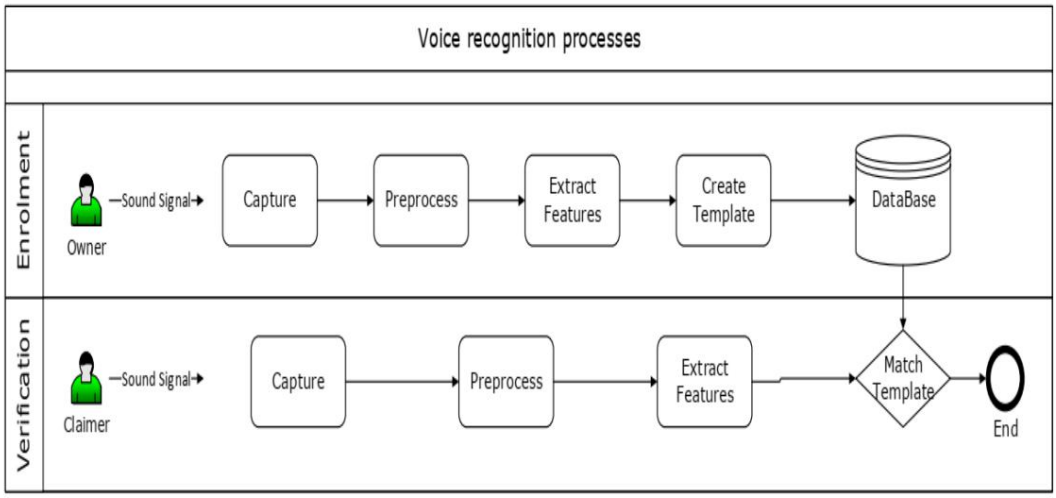
इस प्रक्रिया में सामान्य विशेषताओं से टेम्पलेट्स का निर्माण शामिल है जो इसके स्वामी से मेल खाते हैं। इसके बाद, टेम्पलेट्स को वॉयस रिकग्निशन डेटाबेस में संग्रहीत किया जाता है। VidTimit डेटाबेस और MEEI डेटाबेस जैसे कई डेटाबेस हैं।

2.4. टेम्पलेट मिलान और विश्लेषण

यह प्रक्रिया पहचान दावेदार की आवाज़ और पहले से संग्रहीत आवाज़ टेम्पलेट्स के बीच एक सटीक या लगभग सटीक मिलान खोजने की कोशिश करती है। इसे फूरियर ट्रांसफ़ॉर्म या लीनियर प्रेडिक्टिव कोडिंग (LPC) [19] का उपयोग करके पूरा किया जा सकता है। इसके बाद, टेम्प्लेट बनाए जाने के बाद, सिस्टम को टेम्प्लेट पर प्रशिक्षित किया जाता है। प्रशिक्षण विधियों में वेक्टर क्वांटिज़ेशन (VQ) शामिल है जो लिंडेबुज़ोग्रे (LBG) एल्गोरिथम पर आधारित है। इसके अलावा, हिडन मार्कोव मॉडल (HMM) और गॉसियन मिक्सचर मॉडल (GMM) का उपयोग फीचर प्रशिक्षण के लिए भी किया जाता है [17]।

2.5. मिलान निर्णय

इस प्रक्रिया का उद्देश्य यह निर्धारित करना है कि पहचान का दावा करने वाला व्यक्ति दो आवाज़ों की समानता के आधार पर दावा की गई पहचान से मेल खाता है या नहीं। इसके बाद, मिलान को या तो अस्वीकार कर दिया जाता है या स्वीकार कर लिया जाता है।
इस प्रक्रिया में दो तरह की त्रुटियाँ हो सकती हैं, झूठी-नकारात्मक या झूठी सकारात्मक। झूठी-नकारात्मक का मतलब है कि सिस्टम एक वास्तविक दावेदार की पहचान करने में विफल रहा है, जबकि झूठी सकारात्मक का मतलब गैर-अधिकृत उपयोगकर्ता को पहुँच प्रदान करना है [20]।



चित्र 1. आवाज पहचान प्रक्रियाएँ.

2.6. पाठ-निर्भर

दूसरी ओर, भाषण डेटा की पाठ्य सामग्री के आधार पर, आवाज पहचान प्रणालियों को दो श्रेणियों में वर्गीकृत किया जा सकता है; पाठ-निर्भर, पहचान दावेदार से वही शब्द बोलने की अपेक्षा की जाती है जो नामांकन के दौरान उच्चारित किए गए थे; इस पद्धति में, वक्ता को दो शर्तों को पूरा करना होता है, शब्द को जानना और आवाज का असली मालिक होना [2]। पाठ-स्वतंत्र, उपयोगकर्ता नामांकन और सत्यापन चरणों के दौरान स्वतंत्र रूप से बोल सकता है [21]। अधिकांश शोध दावा करते हैं कि पाठ-निर्भर पहचान प्रणालियों का प्रदर्शन बेहतर है और पाठ-स्वतंत्र प्रणालियों की तुलना में सरल हैं [22]। इस प्रकार, स्मार्ट उपकरणों की संसाधन सीमितता के संबंध में पाठ-निर्भर आवाज पहचान दृष्टिकोण IoT प्रमाणीकरण के लिए बेहतर होगा।

2.7. मूल्यांकन मेट्रिक्स

ध्वनि पहचान प्रणालियों की प्रभावशीलता को मापने के लिए कई मापदंडों का अध्ययन किया जाता है।
इन मापदंडों में गलत स्वीकृति दर (FAR) शामिल है जो सिस्टम द्वारा गलत तरीके से प्रामाणिक के रूप में लेबल किए जाने वाले हमलों की संख्या है। गलत अस्वीकृति दर (FRR) उन प्रामाणिक इंटरैक्शन की संख्या को संदर्भित करती है जिन्हें गलत तरीके से हमलों के रूप में खारिज कर दिया जाता है। सापेक्ष परिचालन विशेषताएँ (ROC) FAR और FRR के बीच एक समझौता दर्शाती हैं। यह सिस्टम को FAR और FRR दोनों को कम करने में मदद करता है [23]।

3. संबंधित कार्य

सामान्य तौर पर, IoT पारिस्थितिकी तंत्र में नियोजित बायोमेट्रिक आधारित प्रमाणीकरण प्रणाली दो प्रकार की होती हैं। उदाहरण के लिए मानव शरीर क्रिया विज्ञान, चेहरा, आंखें, फिंगरप्रिंट या इलेक्ट्रोकार्डियोग्राम। और व्यवहार संबंधी विशेषताएं जैसे हस्ताक्षर, आवाज, चाल या कीस्ट्रोक। उदाहरण के लिए, [24] में शोधकर्ताओं ने एक टकटकी सुविधा आधारित मॉडल पेश किया जो पुनरावृत्त और साइड चैनल हमलों के खिलाफ सुरक्षित है। इसी तरह, [25] में शोधकर्ताओं ने अपनी विधि के विकास के लिए इलेक्ट्रोकार्डियोग्राम का उपयोग किया जिसमें उन्होंने IoT उपकरणों के प्रमाणीकरण के लिए बायोमेट्रिक सुविधाओं की अच्छी उम्मीदवारी साबित की। इस योजना के कार्यान्वयन के परिणाम से पता चलता है कि इसमें सिग्नल अधिग्रहण के 4 सेकंड के लिए 1.41% एफएआर और 81.82% टीएआर है।

शोधकर्ताओं ने [26] में IoT उपकरणों के लिए हस्ताक्षर आधारित प्रमाणीकरण प्रणालियों की उपयुक्तता पर तर्क दिया है, जिसके तहत उन्होंने हस्ताक्षर आधारित योजना की तीन श्रेणियां प्रस्तुत की हैं, अर्थात् ऑफ़लाइन, ऑनलाइन और व्यवहार। IoT उपकरणों के लिए प्रस्तावित कुछ चाल पहचान आधारित प्रमाणीकरण प्रणालियाँ भी साहित्य में हैं [27]। [28] में एक टच स्क्रीन आधारित प्रमाणीकरण योजना प्रस्तावित की गई है।

[29] में, तीन चरणों नामांकन, क्लासिफायर और उपयोगकर्ता प्रमाणीकरण के साथ एक कीस्ट्रोक डायनेमिक्स आधारित प्रमाणीकरण योजना प्रस्तावित की गई है। इसी तरह, [30] में एक फिंगरप्रिंट आधारित प्रमाणीकरण प्रणाली प्रदान की गई है। [31] में, शोधकर्ताओं ने एक प्रमाणीकरण और प्राधिकरण योजना पेश की है जो चेहरे की पहचान का उपयोग करती है जिसका उपयोग IoT पारिस्थितिकी तंत्र के लिए किया जा सकता है। मोबाइल IoT उपकरणों को अनलॉक करने के लिए उपयोग की जाने वाली आइरिस आधारित प्रमाणीकरण प्रणाली [32] में प्रस्तावित है।

हमारी जानकारी के अनुसार, केवल दो शोधकर्ता हैं जिन्होंने IoT पारिस्थितिकी तंत्र के लिए प्रमाणीकरण तंत्र के रूप में वॉयस बायोमेट्रिक्स को अपनाया है। शिन और जून [33] ने स्वचालित घरेलू वातावरण को नियंत्रित करने और निगरानी करने के लिए अधिकृत उपयोगकर्ताओं को सत्यापित करने के लिए वॉयस रिकग्निशन तकनीक को लागू किया है। शोधकर्ता ने एक वॉयस रिकग्निशन सिस्टम प्रस्तावित किया है जो सर्वर और डिवाइस भागों में विभाजित है। सिस्टम के सर्वर भाग की भूमिका उपयोगकर्ता प्री-रजिस्ट्रेशन, उपयोगकर्ता पहचान और नियंत्रण कमांड विश्लेषण के लिए है। डिवाइस भाग की भूमिका डिवाइस कमांड रिसेप्शन और डिवाइस नियंत्रित फिर प्रतिक्रिया है। इस शोध में नियोजित मॉडल और तकनीकों के प्रकार पर चर्चा नहीं की गई है। इसी तरह, मॉडल के कार्यान्वयन की रिपोर्ट नहीं की गई है।

ऑस्कर एट अल. [1] ने चेहरे और आवाज़ के तौर-तरीकों के आधार पर IoT के लिए एक मल्टीमॉडल बायोमेट्रिक दृष्टिकोण प्रस्तावित किया है। शोधकर्ताओं ने IoT तकनीकों के सीमित संसाधनों को मापने के लिए अपने सिस्टम को डिज़ाइन किया है। सिस्टम के वॉयस रिकग्निशन भाग के लिए, शोधकर्ता फूरियर ट्रांसफ़ॉर्म के उपयोग से आवाज़ से MFCC सुविधाएँ निकालने में सक्षम थे। इसके प्रकाश में, फ़िल्टर बैंकों को असतत कोसाइन ट्रांसफ़ॉर्म के अनुप्रयोग के साथ विखंडित किया जाता है। यह सिस्टम वॉयस रिकग्निशन का पूरी तरह से उपयोग नहीं कर रहा है। हालाँकि, इसे एक केस स्टडी में लागू किया गया है, फिर भी इस मॉडल के अंतिम परिणाम की तुलना उस सिस्टम से नहीं की जा सकती है जो वॉयस रिकग्निशन का पूरी तरह से उपयोग करता है।

ऐसी बायोमेट्रिक आधारित योजनाओं के समग्र लाभ यह हैं कि इन्हें खोया नहीं जा सकता, इन्हें कॉपी करना बहुत मुश्किल है, इन्हें वितरित करना कठिन है, और इनका आसानी से अनुमान नहीं लगाया जा सकता। इसके विपरीत, पारंपरिक पासवर्ड-आधारित प्रमाणीकरण विधियाँ कई कमियों से ग्रस्त हैं और इनका आसानी से अनुमान लगाया जा सकता है, हैक किया जा सकता है और क्रैक किया जा सकता है। समीक्षा की गई बायोमेट्रिक प्रणालियों का प्रदर्शन तालिका 1 में दिखाया गया है।

तालिका 1. सिस्टम प्रदर्शन का सारांश

सूत्रों का कहना है	शीर्षक	तरीका	एफआरआर %	एफएआर %	ईआरआर %
[1]	उन्नत IoT सुरक्षा के लिए मल्टीमॉडल बायोमेट्रिक्स	आवाज़ और चेहरा	81.62 एन/ए		8.04
[24]	मोबाइल उपकरणों पर नज़र और स्पर्श का उपयोग करके मल्टीमॉडल प्रमाणीकरण	निगाहें	एन/ए	एन/ए	0.32
[25]	मोबाइल उपकरणों के लिए ईसीजी प्रमाणीकरण	कीस्ट्रोक	81.82	1.4	एन/ए
[26]	इशारों और हस्ताक्षरों का उपयोग करके टच स्क्रीन उपकरणों पर व्यवहार आधारित मानव प्रमाणीकरण	हस्ताक्षर	90	0	0.5
[27]	एन्क्रिप्टेड बायोमेट्रिक टेम्प्लेट का उपयोग करके एज-केंद्रित मल्टीमॉडल प्रमाणीकरण प्रणाली	चेहरा	एन/ए	एन/ए 1.72%	
[28]	टचलाइसटिक्स: निरंतर प्रमाणीकरण के लिए व्यवहारिक बायोमेट्रिक के रूप में टचस्क्रीन इनपुट की प्रयोज्यता पर	स्पर्श गतिशीलता N/A		एन/ए	2-3%
[29]	टच स्क्रीन डिवाइस के लिए कीस्ट्रोक डायनेमिक्स प्रमाणीकरण प्रणाली में दो नवीन बायोमेट्रिक विशेषताएं कीस्ट्रोक		8.40% 8.32% 8%		
[30]	मोबाइल डिवाइस का उपयोग करके अधिक कुशल कुंजी-हैश आधारित फिंगरप्रिंट रिमोट प्रमाणीकरण योजना	अंगुली की छाप	एन/ए	एन/ए	एन/ए
[31]	निरंतर प्रमाणीकरण के लिए आंशिक चेहरा पहचान	चेहरा	एन/ए	1%	एन/ए
[32]	फ़िरमे: मोबाइल जुड़ाव के लिए चेहरा और आईरिस पहचान	चेहरा और आईरिस	0.25	0.8	0.40%
[33]	स्मीकर: पहचान के माध्यम से होम IoT डिवाइस प्रमाणन	आवाज़	एन/ए	एन/ए	एन/ए

4. अनुसंधान अंतराल

एक्सेस कंट्रोल और यूजर ऑथेंटिकेशन के लिए IoT इकोसिस्टम में वॉयस रिकग्निशन सिस्टम की तैनाती से संबंधित क्षेत्रों पर केवल कुछ ही शोध किए गए हैं। एक कार्यशील वॉयस रिकग्निशन सिस्टम का निर्माण या इसे IoT इकोसिस्टम में एकीकृत करने के बारे में साहित्य में बहुत कम जानकारी है।
हालाँकि, सामान्यतः ध्वनि पहचान के क्षेत्र में कुछ पर्याप्त परियोजनाएं की गई हैं।
कुछ को मोबाइल और क्लाउड कंप्यूटिंग प्रतिमानों के लिए अपनाया जाता है। IoT उपकरणों के सीमित कम्प्यूटेशनल, स्टोरेज और पावर संसाधनों की चुनौतियाँ परिष्कृत प्रमाणीकरण प्रणालियों के विकास को खतरे में डाल रही हैं। इसलिए, एक नया बायोमेट्रिक दृष्टिकोण प्रस्तावित किया जाना चाहिए [11, 34]।

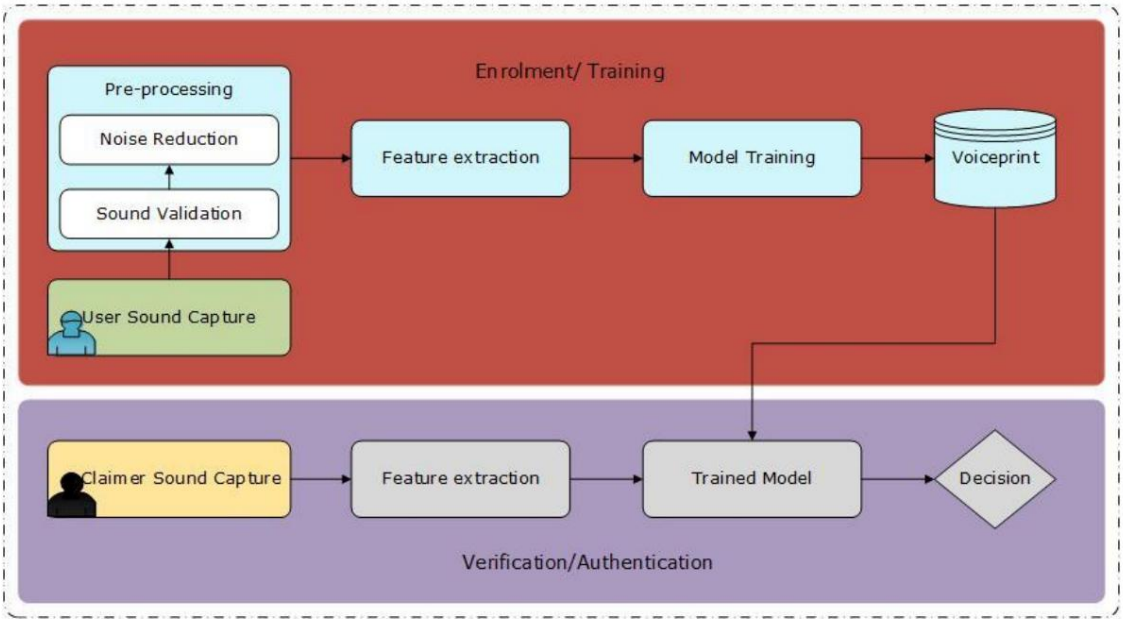
5. हमारा काम

हम एक स्वचालित वॉयस बायोमेट्रिक प्रमाणीकरण प्रणाली की कल्पना करते हैं जो रिमोट से IoT उपकरणों के प्रबंधन और निगरानी के लिए उपयुक्त होगी। जैसा कि पहले चर्चा की गई थी, हमारे मॉडल में एक प्रशिक्षण या नामांकन चरण और एक सत्यापन या प्रमाणीकरण चरण होगा (चित्र 2)। निम्नलिखित अनुभाग मॉडल के विभिन्न घटकों पर व्यापक रूप से चर्चा करता है।

5.1. नामांकन चरण

ध्वनि कैप्चर

यह चरण प्रशिक्षण के लिए IoT डिवाइस के मालिक की आवाज़ या ध्वनि को कैप्चर करता है। यह स्मार्टफ़ोन द्वारा किए जाने की उम्मीद है जहाँ मालिक IoT डिवाइस के नियंत्रण ऐप का उपयोग करता है। इस चरण का आउटपुट उपयुक्त फ़ाइल फ़ॉर्मेट के साथ परिवर्तित फ़ाइलें हैं।



चित्र 2. IoT वॉयस प्रमाणीकरण मॉडल.

पूर्व प्रसंस्करण

इस चरण में, एकत्रित ध्वनि डेटा को दोषों के लिए मान्य किया जाता है। यह विभिन्न पैमानों पर विभिन्न आवृत्तियों पर डेटा को विघटित करके पूरा किया जाता है। और परिणामी वेवलेट को किसी भी क्लिपिंग के अस्तित्व के लिए जाँचा जाता है। इसके बाद, पहचाने गए शोर वेवलेट को हटा दिया जाता है और शोर मुक्त डेटा प्राप्त किया जाता है। एकत्रित ध्वनि डेटा से शोर को हटाने के दो तरीके हैं।

यह थ्रेशोल्ड आधारित डी-नॉइज़िंग विधि [35, 36, 37] और रिकर्सिव कम से कम वर्ग अनुकूली फ़िल्टरिंग विधि [38, 39] के उपयोग के साथ है। हालाँकि, स्मार्ट डिवाइस की उपयुक्तता के लिए हमारे काम में पहला तरीका अपनाया गया है।

सुविधा निकालना

इस चरण में सिस्टम के लिए महत्वपूर्ण माने जाने वाले वॉयस फीचर निकाले जाते हैं। ऐसे फीचर वेक्टर का निष्कर्षण और चयन वॉयस रिकग्निशन सिस्टम की गुणवत्ता में वृद्धि करता है।

मालिक की आवाज़ से निकाले गए फ़ीचर लक्षण दूसरों से अलग होने की उम्मीद है, शोर और विकृति के लिए मज़बूत होना चाहिए, आसानी से निकाले जाने योग्य होना चाहिए, प्लेबैक हमलों के लिए मुश्किल होना चाहिए, और मालिक के पर्यावरण या स्वास्थ्य के परिवर्तन के साथ नहीं बदलना चाहिए। इस प्रकार, इस मॉडल में उपयोग की जाने वाली सबसे उपयुक्त विशेषताएँ MFCC विशेषताएँ हैं। MFCC गुणांक को इसकी कंप्यूटिंग सरलता के लिए चुना गया है जो IoT पारिस्थितिकी तंत्र की संसाधन विवश विशेषताओं के लिए उपयुक्त है। और यह मानव कानों की मानव श्रवण प्रकृति की नकल कर रहा है। इसी तरह, MFCC प्रत्येक फ्रेम के लिए एक हैमिंग विंडो लागू करके ध्वनि संकेत को फ्रेम में विभाजित करता है [40]।

मौजूदा वॉयस रिकग्निशन सिस्टम में दो प्रसिद्ध सिग्नल विश्लेषण उपकरण उपयोग किए जाते हैं। डिस्क्रीट कोसाइन ट्रांसफॉर्मेशन और हिडन मार्कोव मॉडल टूलकिट (HTK)। इसलिए, इस प्रस्तावित सिस्टम में ये उपकरण प्रत्येक फ्रेम की सेप्स्ट्रल विशेषताओं को प्राप्त करने के विवरण का ध्यान रखेंगे।

मॉडल प्रशिक्षण

MFCC सुविधाओं के निष्कर्षण के बाद, IoT स्वामी के लिए वॉयस मॉडल को प्रशिक्षित किया जाता है। इस सिस्टम के लिए HMM मॉडल को अपनाया जाता है। इसका कारण यह है कि HMM को फ़ोन के लिए बहुत प्रभावी माना जाता है क्योंकि सिस्टम ऐप का उपयोग स्मार्टफ़ोन पर किया जाना है। अंत में, वॉयसप्रिंट को डेटाबेस में संग्रहीत किया जाता है।

5.2. सत्यापन/मान्यता चरण

एक बार जब उपयोगकर्ता नामांकन चरण पूरा हो जाता है, तो सिस्टम से अब यह सत्यापित करने की अपेक्षा की जाती है कि पहचान का दावा करने वाला व्यक्ति IoT डिवाइस का मालिक है या नहीं। वॉयस डेटा संग्रह और फीचर निष्कर्षण के समान चरण स्मार्टफोन के माध्यम से दावेदार की आवाज़ के लिए किए जाते हैं। इसके बाद, निकाले गए MFCC फीचर्स को सत्यापन के लिए प्रशिक्षित मॉडल के विरुद्ध परीक्षण किया जाता है। नामांकन डेटा से सत्यापन डेटा को स्वचालित रूप से निर्धारित करने के लिए एक अच्छा सामान्यीकरण प्रदान करने के लिए क्लासिफायर को प्रशिक्षित करने के लिए इस चरण में सपोर्ट वेक्टर मशीन (SVM) का उपयोग किया जाता है। और अंत में, अस्वीकृति या स्वीकृति के लिए निर्णय लिया जाता है। यदि दावेदार की वॉयस फीचर्स प्रशिक्षित मॉडल के विरुद्ध परीक्षण पास करने में विफल रहती हैं, तो प्रमाणीकरण को अस्वीकार कर दिया जाता है।

6. सीमाएं और मान्यताएं

इस कार्य की मुख्य सीमाओं में से एक यह है कि मॉडल वैचारिक है और अभी तक अपने इच्छित वातावरण में लागू नहीं किया गया है। सिस्टम में उपयोग के लिए प्रस्तावित या प्रचारित अधिकांश उपकरण और एल्गोरिदम का तकनीकी रूप से मूल्यांकन भी नहीं किया गया है। लेखकों ने संसाधन विवश प्रकृति पर ध्यान केंद्रित किया

IoT तकनीक के बारे में विस्तार से बताया और उस पहलू के लिए अलग-अलग उपकरण प्रस्तावित किए। उपकरणों की मजबूती और लचीलेपन का वैज्ञानिक रूप से भी गहन अध्ययन नहीं किया गया है। फिर भी, इन सभी सीमाओं को हमारे आगामी शोध योगदानों में संभाला जाएगा।

7। निष्कर्ष

अनधिकृत उपयोगकर्ताओं को IoT पारिस्थितिकी तंत्र तक पहुँचने से रोकने के लिए, व्यवहारिक बायोमेट्रिक्स प्रमाणीकरण प्रणाली पर सबसे अधिक विचार किया जाता है। ऐसा माना जाता है कि आवाज़ पहचान के माध्यम से, IoT उपयोगकर्ता प्रमाणीकरण अधिक सुरक्षित, सटीक और मज़बूत होगा। इसलिए, इस पेपर में हमने IoT पारिस्थितिकी तंत्र के लिए एक टेक्स्ट-निर्भर आवाज़ पहचान प्रणाली प्रस्तावित की है। इस प्रणाली में दो चरण होते हैं: नामांकन चरण जहाँ उपयोगकर्ता को आवाज़ दर्ज करनी होती है, और प्रमाणीकरण चरण का सत्यापन जहाँ पहचान का दावा करने वाले से आवाज़ बोलने की अपेक्षा की जाती है और बाद में नामांकित व्यक्ति के साथ तुलना की जाती है। भविष्य में, हम उसी क्षेत्र के लिए प्रस्तावित अन्य बायोमेट्रिक योजनाओं की तुलना में इसकी सुरक्षा और प्रदर्शन के लिए प्रणाली को विकसित और परीक्षण करने की योजना बना रहे हैं।

इसके अलावा, इस पेपर में समीक्षा की गई विभिन्न तकनीकों को मिलाकर, हम वॉयस फीचर एक्सट्रैक्शन और पहचान के लिए प्रयोज्यता को अनुकूलित करेंगे। हम बेहतर कम्प्यूटेशनल आवश्यकताओं के लिए क्लाउड में उनका उपयोग करने पर भी विचार करेंगे।

प्रतिक्रिया दें संदर्भ

[1] ओलाज़ाबल, ओ., एट अल. उन्नत IoT सुरक्षा के लिए मल्टीमॉडल बायोमेट्रिक्स। 2019 IEEE 9वीं वार्षिक कंप्यूटिंग और संचार कार्यशाला और सम्मेलन (CCWC) में। 2019. IEEE.

[2] रेन, वाई., एट अल., आवाज प्रमाणीकरण के लिए लाउडस्पीकर द्वारा विरूपण के आधार पर रिप्ले हमले का पता लगाना। मल्टीमीडिया टूल्स और एप्लीकेशन, 2019. 78(7): पृष्ठ. 8383-8396.

[3] नैनन, एस. और वी. कुलकर्णी। वीक्यू और जीएमएम का उपयोग करके टेक्स्ट स्वतंत्र स्वचालित स्पीकर पहचान का प्रदर्शन मूल्यांकन। प्रतिस्पर्धी रणनीतियों के लिए सूचना और संचार प्रौद्योगिकी पर दूसरे अंतर्राष्ट्रीय सम्मेलन की कार्यवाही में। 2016. एसीएम।

[4] मैकलारेन, एम., इंटरनेट ऑफ थिंग्स में उपयोगकर्ताओं को प्रमाणित करने के लिए स्वचालित स्पीकर पहचान। 26 अगस्त 2016.

[5] गुप्ता, एस. और एस. चटर्जी, स्पेक्ट्रम विश्लेषण और छवि अधिग्रहण का उपयोग करते हुए पाठ पर निर्भर आवाज़ आधारित बायोमेट्रिक प्रमाणीकरण प्रणाली, एडवांस इन कंप्यूटर साइंस, इंजीनियरिंग एंड एप्लीकेशन, 2012, स्प्रिंगर। पृ. 61-70.

[6] कोलकाता, सी., वॉयस बायोमेट्रिक और स्पीकर रिकॉग्निशन के बारे में। 2014.

[7] ठाकुर, ए.एस. और एन. सहायम, यूक्लिडियन दूरी का उपयोग करके भाषण पहचान। इंटरनेशनल जर्नल ऑफ इमर्जिंग टेक्नोलॉजी एंड एडवांस्ड इंजीनियरिंग, 2013. 3(3): पृष्ठ 587-590।

[8] पेट्रोव्स्का-डेलाक्रेटाज़, डी., ए. एल हन्नानी, और जी. चॉलेट, टेक्स्ट-स्वतंत्र स्पीकर सत्यापन: अत्याधुनिक स्थिति और चुनौतियाँ, नॉनलाइनियर स्पीच प्रोसेसिंग में प्रगति। 2007, स्प्रिंगर। पृ. 135-169।

[9] रोसेनबर्ग, एई, एफ. बिम्बोट, और एस. पार्थसारथी, स्पीकर पहचान का अवलोकन, स्प्रिंगर में स्पीच प्रोसेसिंग की पुस्तिका। 2008, स्प्रिंगर। पृ. 725-742.

[10] यासीन, ए., एट अल., फ़ॉग और क्लाउड कंप्यूटिंग के साथ स्मार्ट घरों के लिए IoT बड़ा डेटा एनालिटिक्स। भविष्य जनरेशन कंप्यूटर सिस्टम, 2019. 91: पृष्ठ. 563-573.

[11] फेराग, एम.ए., एल. मैग्लारस, और ए. डेरहाब, बायोफीचर का उपयोग करके मोबाइल IoT उपकरणों के लिए प्रमाणीकरण और प्राधिकरण: हालिया प्रगति और भविष्य के रुझान। सुरक्षा और संचार नेटवर्क, 2019. 2019.

[12] हामिदी, एच., इंटरनेट ऑफ थिंग्स और बायोमेट्रिक तकनीक पर आधारित प्रमाणीकरण का उपयोग करके स्मार्ट स्वास्थ्य विकसित करने का एक दृष्टिकोण। भविष्य की पीढ़ी के कंप्यूटर सिस्टम, 2019. 91: पृष्ठ 434-449।

[13] रेनॉल्ड्स, डीए, टीएफ क्वाटिएरी, और आरबी डन, अनुकूलित गौसियन मिश्रण का उपयोग करके स्पीकर सत्यापन मॉडल. डिजिटल सिग्नल प्रोसेसिंग, 2000. 10(1-3): पृ. 19-41.

[14] सु, एक्स., एट अल., IoT स्मार्ट डिवाइस नियंत्रक के लिए सुरक्षा में सुधार करने के लिए अध्ययन: कमियां और प्रतिवाद। सुरक्षा और संचार नेटवर्क, 2018. 2018.

[15] ली, डी., जे. वांग, और वाई. यांग. पीवीडी: इंट्रा-स्पीकर पहचान अनुसंधान रुचि के लिए एक नया पैथोलॉजिकल वॉयस डेटासेट. 2016 में चीनी बोली जाने वाली भाषा प्रसंस्करण (आईएससीएसएलपी) पर 10वीं अंतर्राष्ट्रीय संगोष्ठी. 2016. आईईईई.

[16] झांग, एक्स., एट अल. सिंगल बायोमेट्रिक रिकॉग्निशन रिसर्च: एक सारांश. सूचना प्रौद्योगिकी पर 6वें अंतर्राष्ट्रीय सम्मेलन की कार्यवाही में: IoT और स्मार्ट सिटी. 2018. एसीएम.

[17] ब्रुनेट, के., एट अल. मोबाइल उपयोगकर्ता प्रमाणीकरण के लिए स्पीकर पहचान: एक एंड्रॉइड समाधान। 2013.

[18] गोफ़मैन, एम., एट अल. मोबाइल डिवाइस पर विभेदक सहसंबंध विश्लेषण के माध्यम से मल्टीमॉडल बायोमेट्रिक्स। सुरक्षा और प्रबंधन पर अंतर्राष्ट्रीय सम्मेलन (एसएएम) की कार्यवाही में। 2018. कंप्यूटर विज्ञान में विश्व कांग्रेस की संचालन समिति, कंप्यूटर।

[19] गबादामोसी, एल., टेम्प्लेट मैचिंग का उपयोग करते हुए वॉयस रिकॉग्निशन सिस्टम। इंटरनेशनल जर्नल ऑफ रिसर्च इन कंप्यूटर साइंस, 2013. 3(5): पृष्ठ 13.

[20] थुलियर, एफ., बी. बूचार्ड, और बी.-ए. मेनेलास, एक टेक्स्ट-स्वतंत्र स्पीकर प्रमाणीकरण प्रणाली मोबाइल डिवाइस के लिए क्रिप्टोग्राफी, 2017. 1(3): पृष्ठ 16.

[21] अनवर, एम.यू., मोबाइल उपकरणों पर उन्नत भाषण प्रमाणीकरण प्रणाली का डिज़ाइन। 2018.

[22] खित्रोव, ए. और के. सिमोनचिक, पाठ-निर्भर स्पीकर पहचान के लिए प्रणाली और उसकी विधि। 2019, गूगल पेटेंट।

[23] ओक, आर., व्यवहारिक बायोमेट्रिक तकनीकों का उपयोग करके प्रमाणीकरण पर एक साहित्य सर्वेक्षण, इंटेलिजेंट कंप्यूटिंग और सूचना और संचार में। 2018, स्प्रिंगर। पृ. 173-181।

[24] खमीस, एम., एट अल. गेजटचपास: मोबाइल डिवाइस पर टकटकी और स्पर्श का उपयोग करके मल्टीमॉडल प्रमाणीकरण। 2016 सीएचआई सम्मेलन की कार्यवाही में कंप्यूटिंग सिस्टम में मानव कारकों पर विस्तारित सार। 2016।

[25] आर्टेगा-फाल्कोनी, जेएस, एच. अल ओस्मान, और ए. एल सद्दीक, मोबाइल उपकरणों के लिए ईसीजी प्रमाणीकरण। आईईईई ट्रांजेक्शन ऑन इंस्ट्रूमेंटेशन एंड मेजरमेंट, 2015. 65(3): पृष्ठ 591-600।

[26] शहजाद, एम., ए.एक्स. लियू, और ए. सैमुअल, इशारों और हस्ताक्षरों का उपयोग करके टच स्क्रीन डिवाइस पर व्यवहार आधारित मानव प्रमाणीकरण। IEEE ट्रांजेक्शन ऑन मोबाइल कंप्यूटिंग, 2016. 16(10): पृष्ठ 2726-2741।

[27] अली, जेड., एट अल., एन्क्रिप्टेड बायोमेट्रिक टेम्प्लेट का उपयोग करके एज-केंद्रित मल्टीमॉडल प्रमाणीकरण प्रणाली। फ्यूचर जनरेशन कंप्यूटर सिस्टम, 2018. 85: पृष्ठ 76-87.

[28] फ्रैंक, एम., एट अल., टचैलिटिक्स: निरंतर प्रमाणीकरण के लिए व्यवहारिक बायोमेट्रिक के रूप में टचस्क्रीन इनपुट की प्रयोज्यता पर। IEEE ट्रांजेक्शन ऑन इन्फॉर्मेशन फोरेंसिक्स एंड सिक्योरिटी, 2012. 8(1): पृष्ठ 136-148।

[29] तासिया, सी.जे., एट अल., टच स्क्रीन डिवाइस के लिए कीस्ट्रोक डायनेमिक्स प्रमाणीकरण प्रणालियों में दो नवीन बायोमेट्रिक विशेषताएँ। सुरक्षा और संचार नेटवर्क, 2014. 7(4): पृष्ठ 750-758।

[30] खान, एम.के., एस. कुमारी, और एम.के. गुप्ता, मोबाइल डिवाइस का उपयोग करके अधिक कुशल की-हैश आधारित फिंगरप्रिंट रिमोट प्रमाणीकरण योजना। कंप्यूटिंग, 2014. 96(9): पृष्ठ 793-816।

[31] महबूब, यू., एट अल. निरंतर प्रमाणीकरण के लिए आंशिक चेहरा पहचान. 2016 IEEE इंटरनेशनल में
इमेज प्रोसेसिंग पर सम्मेलन (आईसीआईपी)। 2016. आईईईई।

[32] डी मार्सिको, एम., एट अल., फ़िरमे: मोबाइल जुड़ाव के लिए चेहरा और आईरिस पहचान। इमेज और विज़न कंप्यूटिंग, 2014. 32(12): पृष्ठ 1161-1172।

[33] शिन, डी.जी. और एम.एस. जून. होम स्पीकर पहचान के माध्यम से IoT डिवाइस प्रमाणन। 2015 में 17वां
उन्नत संचार प्रौद्योगिकी पर अंतर्राष्ट्रीय सम्मेलन (ICACT). 2015. IEEE.

[34] अटवाडी, वाई. और एम. हम्मौदेह. इंटरनेट ऑफ थिंग्स के लिए प्रमाणीकरण तकनीकों पर एक सर्वेक्षण. भविष्य के नेटवर्क और वितरित प्रणालियों पर अंतर्राष्ट्रीय सम्मेलन की कार्यवाही में. 2017.
एसीएम.

[35] साहू, टीआर और एस. पात्रा, टेक्स्ट इंडिपेंडेंट स्पीकर आइडेंटिफिकेशन के लिए स्पीच सिग्नल का साइलेंस रिमूवल और एंडपॉइंट डिटेक्शन। इंटरनेशनल जर्नल ऑफ इमेज, ग्राफिक्स एंड सिग्नल प्रोसेसिंग, 2014. 6(6)।

[36] झांग, एक्स., एट अल. एंड्रॉइड स्मार्ट फोन पर आधारित वॉयस बायोमेट्रिक आइडेंटिटी ऑथेंटिकेशन सिस्टम। 2018 IEEE 4th इंटरनेशनल कॉन्फ्रेंस ऑन कंप्यूटर एंड कम्युनिकेशंस (ICCC) में। 2018. IEEE.

[37] मूसा, एएन, एनबी इथनिन, और ओए मियाकिल। सेवा उपभोक्ताओं के रूप में बुनियादी ढांचे के लिए वैचारिक फोरेंसिक तत्परता ढांचा। 2014 IEEE सम्मेलन में सिस्टम, प्रक्रिया और नियंत्रण (ICSPC 2014)। 2014. IEEE।

[38] ढकाल, पी., एट अल., वॉयस-बेस्ड यूजर इंटरफेस के लिए एक नियर रियल-टाइम ऑटोमैटिक स्पीकर रिकग्निशन आर्किटेक्चर। मशीन लर्निंग और नॉलेज एक्सट्रैक्शन, 2019. 1(1): पृष्ठ 504-520।

[39] मौसा, एएन, एट अल. एक उपभोक्ता-उन्मुख क्लाउड फोरेंसिक प्रक्रिया मॉडल। 2019 IEEE 10वें कंट्रोल एंड सिस्टम ग्रेजुएट रिसर्च कोलोक्वियम (ICSGRC) में। 2019. IEEE.

[40] मूसा, ए.एन., एन. इथनिन, और ए. ज़ैनल, सीएफएएएस: द्विपक्षीय रूप से सहमत साक्ष्य संग्रह। जर्नल ऑफ़
क्लाउड कंप्यूटिंग, 2018. 7(1): पृ. 1.