BULUT SİSTEMLERİ İÇİN BİYOMETRİK TABANLI GÜVENLİK SİSTEMLERİ

Sercan AYGÜN[1], Muammer AKÇAY[2], Ece Olcay GÜNEŞ[3]
[1]Yıldız Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul
[2]Dumlupınar Üniversitesi, Bilgisayar Mühendisliği Bölümü, Kütahya
[2]İstanbul Teknik Üniversitesi, Elektronik ve Haberleşme Mühendisliği Bölümü, İstanbul
sercan@ce.yildiz.edu.tr, muammer.akcay@dpu.edu.tr, gunesec@itu.edu.tr

ÖZET

Günümüz bilgisayarları çoğunlukla bilgileri birincil olarak sabit diskte saklarken, aslında bulut sistemler depolama açısından daha verimli ve erişilebilirdir. Bulut sistemler kişisel bilgilerin saklanması için geleceğin önemli depolama birimleri olarak görülmektedir. Ancak, kişisel bilgilerin saklanmasında güvenliğin sağlanması önemli bir problemdir. Bu çalışmada, SystemC'de yapılan tasarım ve Arduino geliştirme kartıyla alınan biyometrik parmak izi verisi yardımı ile Diffie-Hellman anahtar değişimi kriptografi algoritmasının buluta erişimde güvenlik derecesini arttırması hedeflenmiştir. Şifreleme için gerekli çarpma işleminin daha etkili yapılması için bilgisayar ortamındaki SystemC ile kriptoloji algoritması gerçeklenmiştir. Bulut sistem kullanıcısının biyometrik verilerini alan Arduino UNO mikro denetleyicisi, hemen ardından Diffie-Hellman işlemleri için bilgisayar (SystemC) ile haberleşir. Biyometrik veriler anahtar değişimi algoritmasının hesaplarında kullanılmak üzere gizli, kişiye özel bir tanımlama numarası (ID-identification number) ile eşleştirilir. Böylelikle, kişiye ait olan eşsiz biyolojik veriler yardımı ile güvenliği arttırılmış bir yapı hedeflenmiştir. Gömülü sistemlerin, yazılım ve donanım mühendisliğini içine alan en geniş çalışma alanı olduğu düşünüldüğünde, önerilen tasarımın disiplinler arası bir çalışma ürünü olarak ileride de geliştirmeye açık olduğu düşünülmektedir. Güvenlik uygulamasına yönelik olan bu çalışma, biyometrinin de katkısı ile işler bir çözüm sunmaktadır.

Anahtar Kelimeler: Arduino; biyometrik güvenlik; bulut sistemler; Diffie-Hellman anahtar değişimi; Kriptografi; SystemC

BIOMETRY BASED SECURITY SYSTEMS PROPOSED FOR CLOUD SYSTEMS

ABSTRACT

Today's personal computers primarily store all the data in the hard disk drives, while cloud systems are more efficient and accessible in terms of storage. Moreover, cloud systems are considered as the significant storage units of our personal data for the future. However, it is an important problem to provide security for the storage of personal information. In this study, it is aimed to increase the security level of accesses into cloud systems via Diffie-Hellman key exchange cryptography algorithm, whereby design in SystemC and the usage of Arduino development board to take the fingerprint data. To increase the efficiency of the multiplication process needed for encryption, cryptography algorithm is realized by using the SystemC on the PC side. The Arduino UNO microcontroller, which captures the biometric data of the cloud user, immediately communicates with PC (SystemC) to have the Diffie-Hellman process started. Each biometric data is mapped into a confidential and private ID to be used in the calculations of key exchange process. Thus, a new structure that has increased security via the unique biological data of the person, is aimed. When it is considered that the embedded system is the largest intersection of hardware and software engineering, proposed design as an interdisciplinary work is considered to be worthy of future research for further development. By the addition of the biometrics, this study as for the applied security, serves an efficient solution.

Keywords: Arduino; biometric security; cloud systems; Cryptography; Diffie-Hellman key exchange; SystemC

1. GİRİŞ (INTRODUCTION)

Bulut bilişimde kullanıcılar kendi verilerinin nasıl saklandığıyla ilgili kesin ve detaylı bilgi sahibi olmadıkları için servis sağlayıcılara güvenmek durumundadırlar [1]. Bu durumu sistem düzeyinde tasarımlarla hazırlanan donanım destekli şifreleme algoritmalarıyla bir miktar daha güvenli hale getirmek oldukça kritiktir. Ancak biyometrik bilgilerin güvenlik sağlamak amacıyla kullanılması sırasında bir sorun ortaya çıkmaktadır: Biyometrik bilgilerin güvenliği ne derece gizli tutulacaktır? Her biyometrik verinin kişiye özel olan eşsiz bir anahtar olduğu düşünülürse, kişiye özel alanlara giriş çıkış sırasında güvenlik arttıran bir unsur olarak kullanılabilmesi mümkündür. Biyometrik veriler değiştirilmesi mümkün olmayan doğuştan biyolojik olarak gelen değerli özelliklerdir. Bu sebeple bu özel verilerin güvenliğini de göz önüne alarak bir sistem tasarımı yapılmıştır.

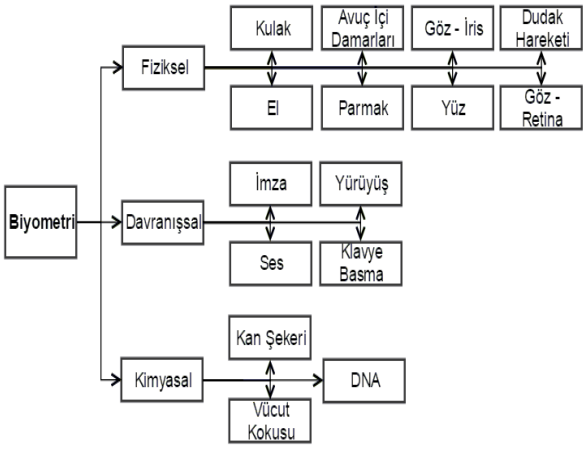
Geçtiğimiz günlerde, bazı ünlü kişilerin bulutta saklanan kişisel verilerinin kötü niyetli üçüncü şahısların eline geçtiği iddiası medyada yer bulmuştur. Bu durum, bulut bilişime erişimin daha kontrollü yapılması gerektiğini ortaya koymaktadır. Buradan yola çıkarak bu çalışmada, kişiye özel hesaplara erişim sırasında, kişiye ait çalınamaz, değiştirilemez özelliklerin kullanılması ile yetkilendirme yapılması amaçlanmaktadır. Kişilerin kendi özel biyometrik verilerini, üçüncü şahısların eline geçmesi endişesi ve hatta bulut servisi sağlayıcılara olan güvensizliklerinden dolayı, doğrudan bulut tarafında değil de kendi taraflarında kontrol etmeleri daha güven vericidir. Bu sebeple bu çalışmada, kişisel şifrenin yanında hesapları izinsiz girişten korumak adına, parmak izi verisi kontrolü ve alınan biyometrik veriye bağlı gizli anahtar üretimi işlemleri de yer almaktadır. Gizli anahtar bulut ile haberleşme aşamasında kullanılacak önemli bir parametredir.

Makalenin geri kalan kısmı şu şekilde düzenlenmiştir. II. Bölümde web uygulamalarının kullanım alanları ve güvenlik durumları hakkında bilgi verilmiştir. III. Bölümde OWASP (Open Web Application Security Project) tarafından 2013 yılında yayınlanan listedeki ilk on web açıklığı; uygulama, sunucu ve iletişim altyapısı güvenliğini tehdit eden unsurlar şeklinde üç başlık altında ele alınmıştır. IV. Bölümde ise bu açıklıklara yönelik yapılan saldırı yöntemlerine karşı kullanılan güvenlik çözümleri ve hangi tür saldırılara ne tür önlemler alınabileceği incelenerek güvenlik çözümlerinin karşılaştırılması yapılmıştır. V. Bölümde ise sonuç ve öneriler üzerinde durulmuştur.

A. Biyometri (Biometrics)

Biyometri köken olarak antik Yunanca "bios" yani *yaşam* ve "metron" *hesaplama* kelimelerinin birleşiminden oluşmaktadır [2]. Doğuştan gelen kişiye özel bu eşsiz özellikler artık günümüzde pek çok mühendislik uygulamasında güvenlik, sınıflandırma, doğrulama, tanımlama gibi amaçlarla ve adli vakalarda kullanılmaktadır.

Biyometrik metotların çeşitlerine bakıldığında, bunları 3 ana sınıfta toplamak mümkündür: fiziksel, davranışsal ve kimyasal [3]. Uygulamaya yönelik biyometrik özelliklerin kullanılması durumunda, Şekil 1'deki şemadan faydalanarak tasarımı gerçekleştirmek, ortaya konan tasarımın uygulanabilirliği açısından önemlidir.



Şekil 1. Biyometrik metotların çeşitlerinin sınıflandırılması [3]

B. Bulut Sistemler (Cloud Systems)

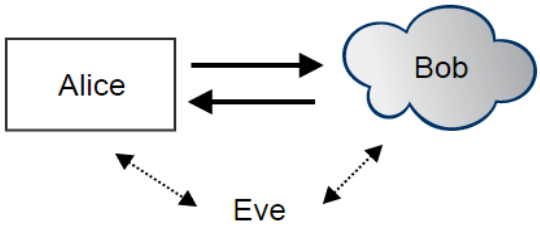
Gizli, açık veya hibrit modelleri olan bulut bilişimin üç tip servisi bulunmaktadır. Bunlardan ilki, Yazılım Olarak Servis (*Software as a Service (SaaS)*), kullanıcılara servis sağlayıcının bulut altyapısındaki uygulamalarını kullanmasını sağlar. Bu serviste platform ve altyapı katmanları ile ilgili bir yönetim söz konusu değildir. Sunulan ikinci servis, Platform Olarak Servis (*Platform as a Service (PaaS)*) olup, uygulamaların bulut tarafına programlama dilleri yardımıyla konulmasını sağlar. Son servis, Altyapı Olarak Servis (*Infrastructure as a Service (IaaS)*)'dir. Burada kullanıcılar diğer servislerle birlikte en geniş kontrol alanına sahiptirler [2].

C. Arduino Geliştirme Kartı (Arduino Development Board)

Son yıllarda gittikçe yaygınlaşan, programlama özellikleri bakımından kolaylıklar sağlayan Arduino geliştirme kartları, bu çalışmada mikro-denetleyici olarak kullanılmaktadır. Örnek çalışmada, UNO isimli modeli kullanılan bu kart ile parmak izi sensöründen alınan verilerin sensör içindeki tanımlama ve karşılaştırma işlemleri, ardından da ait oldukları kullanıcıya bağlı eşsiz numaranın şifreleme yapısına gönderilmesi gerçekleştirilmiştir. Bilgisayar ve bulut ile de haberleşme imkanı sağlayan Arduino geliştirme kartları C++ tabanlı programlama ortamı sunmaktadır. Sisteme ilişkin kodlar, bu kartın geliştirme aracı sayesinde (Arduino IDE 1.0.5), nesneye yönelik olarak (*Object Oriented Programming*) gerçekleştirilmiştir.

D. Diffie-Hellman Anahtar Değişimi (Diffie-Hellman Key Exchange)

Şekil 2'de Alice isimli kullanıcının biyometrik verisini, giriş yapmak istediği bulut alanına, diğer bir deyişle Bob'a gönderdiğini varsayarsak, verilerin iletimi sırasında, Eve isimli bir siber korsanın olması ve verileri çalmak istemesi mümkün olabilir [4]. Bu durum, aradaki adam saldırısı (*man-in-the-middle attack*) olarak da nitelendirilir [5]. Bu gibi saldırılardan kişisel verileri korumak için verilerin şifrelenerek yollanması başvurulan yollardan birisidir.



Şekil 2. Verilerin iletimi sırasındaki olası tehlike senaryosu

Diffie ve Hellman tarafından 1976 yılında ortaya konan anahtar değişimi algoritması ile verileri gönderen kişilere ait gizli sayılar saklı kalarak kişilerin birbirlerini tanıması ve haberleşmesi daha güvenli hale gelmiştir. Buna göre, iki kişi yani Alice ve Bob, kendi aralarında haberleşirken birbirleri ile haberleştiklerini garantilemek için kullanacakları ortak/aynı α ve p sayılarına ek olarak yalnızca kendilerine özel olan a ve b ile sembolize edilen gizli sayılara da sahiptirler. Bu a ve b sayılarını yalnızca kendileri bilecek şekilde saklamaları ve veri alışverişinden önce, gönderdikleri kişi de dahil olmak üzere kimsenin elde etmesi mümkün olmayan bir gizleme ile korumaya almaları gerekmektedir. Burada matematiksel olarak modüler aritmetik ve üs alma işlemlerinden faydalanan Diffie-Hellman, tarafların kullandığı ortak ve açık olarak paylaşılan α taban ve p mod değeri olmak üzere α'nın üssü olarak işleme giren gizli a ve b değerlerini kullanmışlardır [6]. Açıklanan matematiksel yaklaşım aşağıdaki (1) denkleminde ifade edilmektedir.

$$(\alpha^b \bmod p)^a \bmod p = (\alpha^a \bmod p)^b \bmod p \qquad (1)$$

Örnek Durum:

$\alpha = 5, p = 7, a = 2, b = 3$ olmak üzere;

$5^3 \bmod 7 = 125 \bmod 7 = 6 = (\alpha^b \bmod p) = B$ ve

$5^2 \bmod 7 = 25 \bmod 7 = 4 = (\alpha^a \bmod p) = A$

(1) numaralı denkleme göre,

$(\alpha^b \bmod p)^a \bmod p = (\alpha^a \bmod p)^b \bmod p$

$= (B)^a \bmod p = X = (A)^b \bmod p = Y$ olacak şekilde,

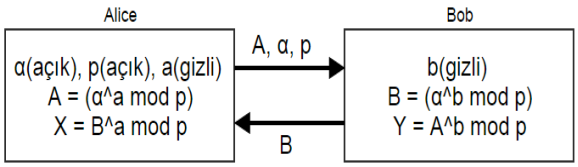
$= (6)^2 \bmod 7 = (4)^3 \bmod 7$

$= 36 \bmod 7 = 64 \bmod 7$

$= 1 = 1$

yani, $X = Y$ olarak bulunmaktadır.

Görüldüğü üzere, (1) numaralı denklemdeki eşitlik verilen sayısal örnekle de desteklenmiştir. Burada Bob'un gizli b değerinin ($\alpha^b \bmod p$) şeklinde, Alice'e ait gizli a değerinin ise ($\alpha^a \bmod p$) şeklinde işleme dahil edildiği söylenebilir. Böylece bu değerlerin gizlenerek paylaşıldığı, ayrıca açık olarak paylaşılan α ve p değerleri ile de, yeniden gönderildiği tarafta üstel ve modüler işleme sokularak, birbirlerinin aynısı X ve Y değerlerine ulaşıldığı görülmektedir. Haberleşmeden önce böyle bir yaklaşım ile bulut kullanıcısı ve bulut tarafı desteklenen donanım ile haberleşip, biyometrik parmak izi verisi ile de arttırılmış güvenlikle birbirlerini tanıyabilirler. Şekil 3'te kullanılan değişkenlere ve paylaşılan değerlere ait bilgiler verilmektedir.



Şekil 3. Diffie-Hellman anahtar değişimi [7]

Burada a ve b sayıları, verilen örnekteki gibi düşük bitli sayılar değildir. Örneğin, önerilen sistem için daha güvenli olması açısından 512 bit değerindeki sayılar kullanılmıştır, çünkü SystemC ortamı *sc_biguint<512>* değişken tanımlaması ile bu imkanı sunmaktadır. Büyük bitli sayılarla çalışmak, özellikle kullanılan algoritma gereği üs alma sırasında çarpma işlemlerinin her bir zaman döngüsü açısından fazla olması anlamına gelmektedir. Bundan sonraki çalışmalar için çarpma işlemini daha etkin bir yöntem ile gerçekleştirerek iyileştirme öngörülmektedir. Bu nedenle, SystemC ortamı tercih edilmiştir.

II. ÖNERİLEN SİSTEM (PROPOSED SYSTEM)

Literatürde, bu çalışmada da kullanılan ZFM-20 parmak izi sensörü ile mikroişlemci tabanlı erişim kontrolü sistemleri görülmektedir [8,9]. Çalışmalardan birinde, şifreleme ile ilgili değil, yalnızca sensörden yapılan eşleşmeye göre erişim kontrolü sağlayan sistem tasarımı gerçeklenmiştir [8]. Bir başka çalışmada ise laboratuvar erişim kontrolü sistemi ethernet tabanlı olarak gerçeklenmiştir [9]. Bu kaynak, sensörün çalışma prensibini de detaylı olarak anlatmaktadır. Biyometrik verilerin güvenli kullanımı açısından özetleme (*hash)* fonksiyonlarına benzer matematiksel yaklaşımlar kullanılabilir.

Biyometrik verilerin özetleme fonksiyonları ile işlenmesi fikri Tulyakov ve arkadaşlarının çalışmasında ayrıntılı olarak anlatılmıştır [10]. Buna göre, (2) numaralı denklemde gösterilen simetrik özetleme fonksiyonundan yola çıkarak (3) numara ile gösterilen verinin girdi olarak fonksiyona gönderilmesi ile özetleme sonucu elde edilmektedir. Ayrıca (4)

denklemindeki veriler de (2)'deki fonksiyonda kullanılırsa sonuç yine aynı çıkacaktır. Simetrik olan özetleme fonksiyonundan yola çıkarak önerdikleri sistemde Tulyakov, biyometrik verilerin ufak değişimlere olan direncinden ve kullanılabilirliğinden bahsetmektedir. Çünkü standart özetleme fonksiyonları girdi değişimine karşı çok hassastır ve biyometrik parmak izi verileri resim olarak alındığı sırada %100 aynı gri seviye değerlerine, ışık şiddetine ve parmak yönüne sahip olamayabilir. Bu çalışmada, gelecek araştırmalarda esneklik sağlaması açısından parmak izinden anahtar üretimi sırasında benzer bir fonksiyon kullanılmıştır. Ancak, biyometrik veriden anahtar elde edilmesi sırasında üstel fonksiyonun çalışma zamanının fazla olmasından dolayı giriş verisinin tüm değerleri toplandıktan sonra üs alma işlemi denklem (5)'de olduğu gibi uygulanmıştır.

$$H^m(X) = x_1{}^m + x_2{}^m + ... + x_n{}^m \quad (2)$$

$$X = x_1 x_2 x_3 ... x_n \quad (3)$$

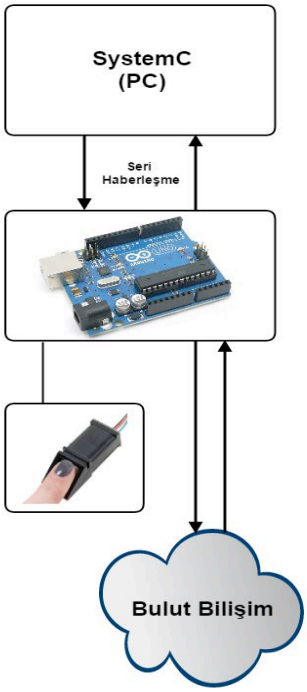
$$X = x_2 x_3 x_n ... x_1 \quad (4)$$

$$H'^m(X) = (x_1 + x_2 + ... + x_n)^m \quad (5)$$

Bu makale aynı zamanda yazılımı ve donanımı bir araya getirerek sistem seviyesinde tasarım yapmayı amaçlamaktadır. Tasarımda, basit kriptografi algoritmalarına donanım yardımıyla çözüm getiren SystemC tabanlı bir yapı kullanılmıştır. Sensörlerden alınan verilere bağlı ID değerlerini şifrelenmek üzere kullanılacak olan yapıya gönderen Arduino UNO geliştirme kartının ve verilerin iletiminden önce yetkilendirme için kendi anahtarını (ortak α ve p değerlerine bağlı olarak) üreten bulut yapısının bir araya gelerek eşzamanlı olarak çalışması hedeflenmektedir. Böylece kullanıcı güvenliği arttırılacaktır. Şekil 4'te önerilen sistemin genel yapısı görülmektedir.

Sistemin çalışma prensibi kısaca şu şekildedir: Giriş yapacak kişi, kullanıcı adını ve şifresini (*PIN*, *password*) standart sistemlerde olduğu gibi sisteme girer ve önceden bu bilgilerle yeni kayıt sırasında eşlenmiş parmak izi verisi karşılaştırması için sensöre parmağını gösterir. Eşleşme sensörün kendisinde gerçekleşir. Şifre kullanımı, uç durumları önlemek adına geleneksel çoğu giriş sisteminde olduğu gibi, tasarlanan bu sistemde de bulunmaktadır.

Örneğin; tek yumurta ikizlerine ait biyometrik benzerlikten ortaya çıkabilecek güvenlik sorunlarını ve parmak sağlığı açısından problemi olan kullanıcıların (örneğin fiziksel açıdan engelli vatandaşların yalnızca şifre kullanması, parmak izi verisi noksanlığı) sıkıntılarını en aza indirmek için şifre kullanımı sürdürülmektedir. Okutulan parmak izinin doğruluğu sensörde bulunan flaş bellekteki kayda göre yapılmaktadır. İlk kayıt sırasında alınan veriler *template* – şablon olarak saklanmaktadır. Sensör, kullanıcı tarafında bulunduğu için, buluta doğrudan parmak izi verisi iletimi söz konusu değildir. Parmak izi – şifre eşleşmesi ardından, Arduino kontrol kartı bilgisayar ortamında var olan SystemC tabanlı yapı ile haberleşerek alınan biyometrik veriye bağlı üretilen 512 bitlik anahtar için Diffie-Hellman işlemleri gereği hesaplanan değişkenleri alır ve bulut ortamı ile haberleşmek için, buluttan gelecek olan Diffie-Hellman değişkenini talep eder. Gerekli karşılaştırmaları yapan Arduino kontrol kartı, kişiye ait olan eşsiz parmak izi verisine bağlı olarak üretilen anahtar sayesinde buluttan gelecek verilerin doğrulamasını yapabilmektedir. Biyometrik veriden dinamik olarak anahtar üretmek için ise sensörden okunan parmak izi verisine ait ilgili bayt değerleri ardışık olarak toplanmış olup, PIN (4 bayt) de üstel olarak (5) numaralı denklemdeki gibi işleme katılmış ve denklem (6) elde edilmiştir. Eğer gerekli ise, 0 değerleri ile 512 bitlik bir değere tamamlanmıştır. Elde edilen değer 512'den büyük ise, yalnızca 512 bit kullanılmıştır.

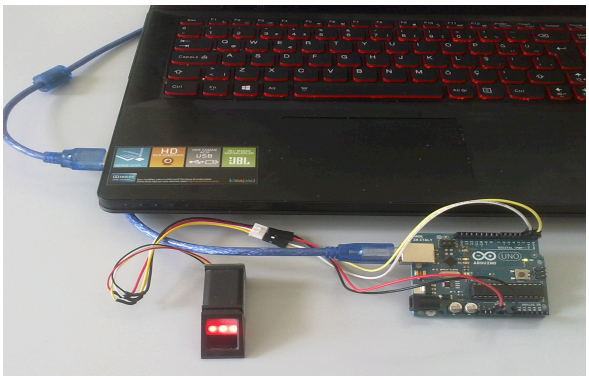


Şekil 4. Önerilen sistemin genel yapısı

$$Y = (ParmakİziBayt1 + ParmakİziBayt2 + ... + ParmakİziBayt256)^{PIN} \quad (6)$$

Bu ID veya anahtar, kişinin bulata veri aktarma ve buluttan gelecek veri kontrolünde Diffie-Hellman anahtar değişimi için kullanılacak olup, böylece sanal sistemlerdeki rastlantısal olarak sayı üretme işlemi de kişinin dinamik değerlerine bağlanacaktır.

Burada Alice isimli tarafın önerilen sistem, Bob isimli tarafın ise bulut bilişim olduğu düşünülebilir. Şekil 5'de, sensör, Arduino ve bilgisayar ile kurulan sistem gösterilmektedir.



Şekil 5. Kurulan sisteme ait bilgisayar, mikro kontrolcü ve sensör bağlantıları

Sistemde kullanılan parmak izi sensörü, içindeki özel DSP çip yardımıyla görüntüyü alma, saklama, karşılaştırma gibi performans ve görüntü işleme teknikleri gerektiren işlemleri etkin biçimde gerçekleştirmektedir. Sensör, fabrikasyon olarak 57600 *Baud Rate* -birim zamanda iletilen karakter-değerinde haberleşecek şekilde üretilmiştir. Bu oran iletişim protokolleriyle hazırlanan veri paketleri ile 9600 seviyesine çekilmiştir. Sensör çalışırken parmaktan 256x288 piksellik Şekil 6'daki formatta ham görüntüyü alır. Ardından görüntüden bir şablon elde eder ve veri tabanında saklar.

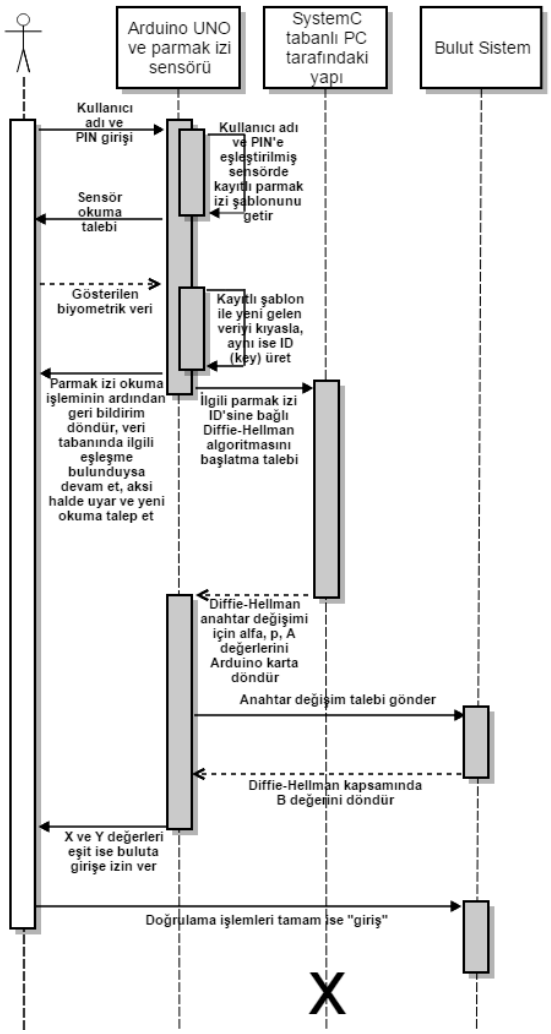
Sensöre ait Yanlış Kabul Oranı *(False Acceptance Rate-FAR) <%0.001* ve Yanlış Red Oranı *(False Reject Rate-FRR) <%1.0* olarak görülmektedir [11]. Sistemin tek yumurta ikizleri açısından güvenilirliğinin değerlendirmesinin yapılması açısından [12] çalışmasına bakılabilir. Bahsi geçen çalışmada yalnızca ikizlerin bulunduğu bir araştırmaya ait FAR ve FRR oranları sunulmaktadır. Aynı sistemde ikiz olan ve olmayanların dahil edildiği bir analiz de sunulmuştur. İlgili makaledeki değerlere göre bu çalışmada kullanılan sensörün FAR ve FRR oranları kabul edilebilirdir. Yine de ikizler gibi güvenlik açığı doğurabilecek örnekler için, tasarlanan sistemde PIN koruması da bulunmaktadır.

$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	. . . .	$a_{1,286}$	$a_{1,287}$	$a_{1,288}$
$a_{2,1}$	.						$a_{2,288}$
$a_{3,1}$		.					$a_{3,288}$
.			.	.			.
.							.
.				.			.
.					.		.
$a_{256,1}$	$a_{256,2}$	$a_{256,3}$	$a_{256,4}$	. . . .	$a_{256,286}$	$a_{256,287}$	$a_{256,288}$

Şekil 6. 256x288 piksellik ham parmak izi görüntüsünün temsili yapısı

Ayrıca önerilen sistemin tüm işlemleri Intel Core i7-4700MQ 2,4 GHz işlemcili, 16GB RAM'e sahip, x64-bit Windows 8 işletim sistemi olan bir dizüstü bilgisayarda gerçekleştirilmiştir. SystemC için geliştirme ortamı ise Visual Studio 2008 (C++) olarak sağlanmıştır. SystemC kütüphaneleri ilgili ortama aktarılarak yazılım gerçeklenmiştir.

Tasarımın ilk evrelerinde sistemin genel çalışma yapısı çalışma diyagramı olarak hazırlanmış ve Şekil 7'deki son haline ulaşılmıştır. Bu diyagram, (*sequence diagram*) belli kurallara uygun olarak ve bazı örnekler incelenerek çizilmiştir [13].



Şekil 7. Sistemin çalIşma diyagramI (değişken isimleri Şekil 3'e göre verilmiştir.)

III. SONUÇ (CONCLUSION)

Bu çalışma sonunda, donanımsal olarak doğru ve eşzamanlı çalışan bir sistem elde edilmiştir. Bilgisayar üzerinden seri haberleşme protokolü vasıtasıyla haberleşen yapı, Diffie-Hellman anahtar değişimi için gerekli değişkenleri SystemC ile yazılan yapıdan alıp

bulut bilişim ile güvenli anahtar değişimi yapmaya hazır hale getirilmiştir. Böylelikle kişilerin bulut hesaplarına arttırılmış güvenlikle erişmeleri mümkün olmaktadır.

Kullanılan parmak izi tarayıcısına ait güvenilirlik oranları, sensörün özelliği gereği belli bir kesinliğe bağlı olarak elde edilmektedir. Bu, sistemde kayıtlı olan parmak izi verisi ile doğrulama sırasında okutulan parmağın durumuna bağlı olarak değişmektedir. Tablo 1'de, beş farklı kişiye ait önceden kayıtlı parmak izi şablonuna, sensör yardımıyla ulaşılıp, erişim anındaki doğrulama sırasında elde edilen kesinlik yüzdeleri sunulmuştur. Veri tabanında toplam beş kişi olacak şekilde, yine aynı kullanıcılar önceden tanımlanmıştır. Burada verilen oranlar, sensörün kesinliğine bağlı olarak sensörden dönen "*confidence number*" yani güvenilirlik sayısına göre yüzdesel sunulmuştur. İlgili güvenilirlik aralığı 0-255'dir [11]. Verilen oranlar, kişinin önceden okuttuğu parmak izi verisine ve geçiş anında okuttuğu verinin kalitesine göre önemli ölçüde değişiklik göstermektedir.

Ayrıca sensörün veri okuma, karşılaştırma ve sonuç döndürme işlemlerinin toplam zamanı, Tablo 1'deki güvenilirlik ölçümü yapıldığı sırada kaydedilip Tablo 2'de sunulmuştur.

TABLO I. PARMAK İZİ SENSÖRÜ KESİNLİK ORANLARI

Veri alınan kişi	Okunan veriye bağlı kesinlik oranı (%)
A	%81
B	%69
C	%72
D	%60
E	%78

Kullanılan sensörün üretici firma tarafından sunulan Windows işletim sistemi için hazırlanmış bir kullanıcı ara yüzü de bulunmaktadır. Bu program, USB üzerinden bilgisayara doğrudan bağlı olan sensörü denetleyici olmadan kontrol eder. Tablo 2'de verilen okuma sürelerinden çok daha hızlı (~[40,100] ms) işlem süreleri elde edildiği görülmüştür.

TABLO II. PARMAK İZİ SENSÖRÜ ÇALIŞMA ZAMANLARI

Veri alınan kişi	Tablo 1 için sensörün veri okuma, karşılaştırma ve sonuç döndürme işlemlerinde geçen toplam süre (milisaniye - ms)
A	1170ms
B	1207ms
C	1163ms
D	1126ms
E	1141ms

Önerilen sistem ile uygulamaya yönelik bir güvenlik sistemi sunulmuştur. Parmak izi verisinden kullanılabilir bir anahtar elde edilmesi ve donanımsal bir modül tasarımının da gerçeklenmesi ile diğer çalışmalara göre farklı bir yaklaşım, uygulama tabanlı olarak tasarlanmış ve test edilmiştir. [10] kaynağında da bahsedildiği üzere parmak izi verisinin özetleme (*hash*) fonksiyonuna benzer bir fonksiyon ile işlenmesi eşsiz bir numara üretmek için kullanılmıştır. Elde edilen eşsiz *ID* tasarlanan sisteme entegre edilmiş ve bu yönü ile uygulanabilirlik açısından önemli bir adım atılmıştır.

Gelecekte öngörülen çalışmalardan öncelikli olanı sistem için Windows tabanlı bir ara yüzün hazırlanmasıdır. Bu, çalışmanın gerçek hayatta mühendislik uygulaması olarak kullanılabilirliğini arttıracaktır. Ayrıca, SystemC tarafında gerçeklenen Diffie-Hellman anahtar değişimi algoritmasından farklı başka algoritmalar da gerçeklenebilir. Parmak izi sensörü dışında, teknolojinin gelişimi ile birlikte yeni sensörlerin ortaya çıkmasıyla ve yeni yöntemlerin geliştirilmesiyle başka biyometrik verilerin alınmasını sağlayan sensörler de sisteme eklenebilir.

Burada bahsedilen bulut yapısı açık kaynak kodlu herhangi bir sağlayıcı olabilir. Hatta üzerinde bulut sistemi gerçekleştirilmiş Raspberry Pi veya Beagle Board/Bone gibi geliştirmeye açık bir kart ile haberleşmek de Arduino kartı ile mümkündür. Buradaki bilgisayar-mikro denetleyici arasındaki kablolu haberleşme yerine, XBee gibi bir kablosuz haberleşme modülü kullanarak yeni ve daha pratik bir çözüm getirilebilir.

IV. TEŞEKKÜR (ACKNOWLEDGMENTS)

Bu çalışma, yazarlardan Sercan Aygün'ün Anadolu Üniversitesi ve İstanbul Teknik Üniversitesi'ndeki yüksek lisans çalışmaları sürecinde elde edilen bilgilerin harmanlanması ile ortaya konmuştur. Bu kapsamda, tez çalışması için maddi desteği sağlayan İstanbul Teknik Üniversitesi Rektörlüğü, BAP birimine ve ayrıca kriptoloji konusundaki bilgilendirmelerinden dolayı Doç. Dr. Berna Örs Yalçın'a teşekkürlerimizi sunarız.

V. KAYNAKLAR (REFERENCES)

[1] D.G. Martinez, E.A. Rua, and D.A.R. Silva, "Secure Crypto-Biometric System for Cloud Computing," Securing Services on the Cloud (IWSSC), 2011 1st International Workshop, Milan, İtalya, 6-8 Eylül 2011, pp. 38-45.

[2] K.M.S. Soyjaudah, G. Ramsawock, and M.Y. Khodabacchus, "Cloud Computing Authentication Using Cancellable Biometrics," AFRICON, 2013, Pointe-Aux-Piments, Mauritius, 9-12 Eylül, pp. 1-4.

[3] H. Banirostam, E. Shamsinezhad, and T. Banirostam, "Functional Control of Users by Biometric Behavior Features in Cloud Computing," 4th International Conference on

Intelligent Systems, Modelling and Simulation, 29-31 Ocak 2013, pp. 94 – 98.

[4] A. Sibille, "Analysis of Alice-Bob-Eve Scenarios for Secret Key Generation from Random Channels," General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI, 16-23 Ağustos 2014, pp. 1 – 4.

[5] M. Eriksson, "An Example of a Man-in-the-Middle Attack Against Server Authenticated SSL-Sessions", Simovits Consulting Wenner-Gren Center 113 46 Stockholm, İsveç, n.d.

[6] W. Diffie, and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, Kasım 1976.

[7] "Diffie-Hellman anahtar değişimi," Wikipedia, Özgür Ansiklopedi, [Çevrimiçi], Erişim: http://tr.wikipedia.org/wiki/Diffie-Hellman_anahtar_değişimi, [25 Şubat 2015].

[8] D. Sunehra, "Fingerprint Based Biometric ATM Authentication System," vol. 3, no. 11, pp. 22–28, 2014.

[9] F. Hai-Jian, C. Cheng-Wei, and Z. Chang-Wei, "Research on Application of Ethernet-Based Fingerprint Identification System in College Laboratory Management," Proc. - 2011 4th Int. Symp. Knowl. Acquis. Model. KAM 2011, pp. 274–276, 2011.

[10] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric Hash Functions for Secure Fingerprint Biometric Systems," Pattern Recognit. Lett., vol. 28, no. 16, pp. 2427–2436, 2007.

[11] Adafruit (2014, Mart). "Adafruit Optical Fingerprint Sensor", Ladyada, [Çevrimiçi], Erişim: https://learn.adafruit.com/downloads/pdf/adafruit-optical-fingerprint-sensor.pdf [25 Şubat 2015].

[12] A.K. Jain, S. Prabhakar, and S. Pankanti, "Can Identical Twins Be Discriminated Based on Fingerprints?," Pattern Recognition, 35, 2653-2663, 2002.

[13] R. Panchumarthy, R. Subramanian, and S. Sarkar, "Biometric Evaluation on the Cloud: A Case Study with HumanID Gait Challenge," 2013 Biometric Consortium Conference, 17-19 Eylül 2013, Tampa, Florida, USA.