Güvenli Pasif RFID Protokolünün Gerçeklenmesi

Implementation of Passif Secure RFID Protocol

Mehmet Yavuz Yağcı
Bilgisayar Mühendisliği
İstanbul Üniversitesi-Cerrahpaşa
İstanbul, Türkiye
myy@istanbul.edu.tr

Muhammed Ali Aydın
Bilgisayar Mühendisliği
İstanbul Üniversitesi-Cerrahpaşa
İstanbul, Türkiye
aydinali@istanbul.edu.tr

***Öz*— Tanımlama ve yetkilendirme gibi alanlarda RFID(Radyo Frekanslı Tanımlama) sistemlerine başvurulmaktadır. Fakat RFID sistemlerinde birçok güvenlik problemleri bulunmaktadır. RFID sistemleri aktif etiketler ve pasif etiketler olarak ikiye ayrılmaktadır. Aktif RFID etiketlerinin hesaplama gücü bulunmasından dolayı üzerlerinde birçok çalışma yapılmış ve çözümler üretilmiştir. Pasif etiketlerin hesaplama gücü bulunmamasından dolayı bu etiketler üzerine güçlü algoritmalara dayanan çözümler üretilememektedir. Pasif etiketler üzerindeki güvenlik problemlerinden biri olan kart kopyalama herkesin ulaşabileceği cihazlar ile yapılabilir hale gelmiştir. Kopya kartın tespit edilememesi istenmeyen kişilerin istenmeyen bölgelere sürekli erişimine olanak sağlar. Önerilen çözümde pasif RFID etiketlerinin kopyalandığı zaman kopya kartın tahmin edilmesiyle beraber geçersiz kılınması üzerinde çalışılmıştır. Etiket her başarılı okumada merkezi bilgisayardan gelen ve rastgele üretilen yeni özüt değerini tutmaktadır. Oluşturulan özüt değeri rastgele metinlerin özütlerinden oluştuğu için belirli bir düzen teşkil etmemektedir. Her okumada değiştirilen özüt değeri sayesinde ilk okutulan kart geçerli kart olarak kabul edilecek ve aynı kart numarasına sahip başka bir kart okutulduğunda kopya kart olarak etiketlenecektir.**

Anahtar Sözcükler*— *RFID, Kimlik Doğrulama, Yetkilendirme, RFID Kart Kopyalama

Abstract— RFID(Radio Frequency Identification) systems are being used in areas such as identification and authorization. However, RFID systems have many security problems. RFID systems are divided into active tag and passive tag. Due to the computational power of active RFID tags, many studies have been made on them and solutions have been produced. Since passive tags have no computational power, solutions based on strong algorithms can not be produced on these tags. One of the security problems with passive tags, card copying has become possible with devices that anyone can access. The inability to identify the copy card allows continuous access to unwanted areas by unwanted persons. The suggested solution is to override passive RFID tags when they are copied, along with estimating the copy card. The tag holds the value of the new hash, which is randomly generated from the central computer in every successful reading. The generated hash value does not constitute a specific order because it is composed of hash of random texts. With the modified hash value in each reading, the first card read will be treated as the current card, and if another card with the same card number is read, it will be labeled as the copy card.

Keywords*— *RFID, Authentication, Authorization, RFID Card Copy

I. GİRİŞ

Teknolojideki gelişmeler ile beraber kablosuz haberleşme sistemleri günlük hayatımızın bir parçası haline gelmiştir. Günümüzde en çok kullanılan kablosuz haberleşme türlerinden bazıları WiFi(Wireless Fidelity – Kablosuz Alan), Bluetooth, NFC(Near Field Communication – Yakın Alan İletişimi), RFID(Radio Frequency Identification – Radyo Frekanslı Tanımlama) ve ZigBee 'dir. Kullanılan bu kablosuz haberleşme sistemlerinin gelişimi ile beraber güvenlik konusu önem kazanmaktadır.

RFID teknolojisi radyo frekansı ile haberleşen bileşenlerden oluştuğu ve tanımlama işlemlerinde kullanıldığı için Radyo Frekansı ile Tanımlama olarak adlandırılır. RFID teknolojisinde 3 ana bileşen vardır. Bunlar okuyucu, etiket ve antendir. Okuyucular, genellikle bir mikroişlemci tarafından hesaplama gücüne sahip olan ve etiket üzerindeki bilgileri sahip olduğu anten sayesinde radyo dalgalarını kullanarak etiket üzerinde okuma ve yazma yapabilen bileşendir. Etiketler ise aktif ve pasif olmak üzere ikiye ayrılır. Aktif etiketlerin kendi güç kaynakları mevcuttur. Bu nedenden dolayı okuyucu ile kendileri iletişime geçebilir ve okuyucudan gönderilen veriyi işleyebilir. Pasif etiketlerin ise kendilerine ait güç kaynakları yoktur. Bu nedenden dolayı okuyucuyla iletişime geçmek için okuyucudan gelen radyo dalgalarını elektrik enerjisine çevirir. Elde edilen güç ile içerisinde bulunan veriyi okuyucuya gönderir. Basit yapısından dolayı pasif etiketlerin maliyetleri çok düşüktür. Tablo I'den görüldüğü üzere gündelik yaşamımızda kullanım alanı oldukça geniş olduğu gibi gelecekte de kullanım oranında büyük bir artış beklenmektedir.

TABLO I. RFID KULLANIM ISTATISTIGI

Milyar	Yıl		
	2005	2010	2020
Aktif	0.05	0.06	0.8
Pasif	0.66	2.3	124
Toplam	0.71	2.4	125

Pasif RFID kartları bazı güvenlik sorunları ile karşı karşıya kalmaktadır. Kart kopyalanması, yanıtlama saldırısı, izleme ve konumlandırma saldırısı pasif RFID'ler de sıklıkla karşılaşılan güvenlik sorunlarıdır[2]. Kart kopyalama ve kart şifrelerinin kırılması için hazır donanımlar bulunmakta ve rahatlıkla ulaşılabilir web sitelerinde satılmaktadır[3]. Birçok RFID güvenlik protokolü verinin şifrelenmesi, özütlenmesi gibi hesaplama gücü gerektiren kriptolojik fonksiyonlar içermektedir. Düşük hesaplama güçlü pasif RFID kartlar kriptolojik fonksiyonları çalıştırabilecek işlem gücüne sahip değildir[4].

978-1-5386-7893-0/18/$31.00 ©2018 IEEE

Bu çalışmada pasif RFID etiketlerinin maruz kaldığı kart kopyalama atakları ele alınmıştır. Bina girişleri ve bölge yetkilendirmeleri RFID kart sistemleri ile yapılmaktadır. Yetki sahibi bir kart kopyalandığında, tüm erişim yetkileri kopya kart üzerinde de tanımlı hale gelmiştir. Gerçek kart ve kopya kart içerikleri aynı olduğundan dolayı birbirlerinden ayırt edilememekte ve kart kopyalama atağı tespit edilememektedir.

II. ÖNCEKİ ÇALIŞMALAR

RFID kimlik doğrulama ile ilgili birçok çalışma yapılmıştır. Bu çalışmaların birçoğu hesaplama gücü olan etiketlere yönelik olmuştur.

A. Güvenli bir RFID protokolünün gerçekleşmesi

Araştırmacıların önerdiği protokol[5]; doğrulama işlemi üzerine çalışmaktadır. Doğrulama işleminin yapılması sırasında rastgele sayı üretimi ve simetrik şifreleme yöntemleri kullanılmaktadır. Gerçeklenmesi sırasında Digi firmasının Xbee[6] modülü ve Texas Instrument firmasının Msp430[7] kiti kullanılmıştır. MSP430 ile oluşturulan etiket benzetimi etikete bir hesaplama gücü tanımladığı için pasif RFID etiketlerine uygulanabilir bir çözüm olmaktan çıkmıştır. Okuyucu kısmında ise ARM tabanlı bir işlemci kullanılmıştır.

B. Çipsiz hafif güvenlik protokolü

Araştırmacıların önerdiği protokol[8]; rastgele sayı üretimi ve XOR yöntemlerine dayanmaktadır. Protokol işleyişinde Open loop resonator ile rastgele sayı üretimi ile başlayan süreç üretilen değerin dijital olarak kodlanması ve FPGA(Alanda Programlanabilir Kapı Dizileri) üzerinde işlemlere tabi tutulması gibi aşamalar içermektedir.

C. Verimli özüt dizisi uygulaması

Araştırmacıların önerdiği protokol[9]; Lamport şeması temel alınarak yapılmıştır. İlk başta kullanıcıdan bir şifre değeri girmesi beklenmektedir. Girilen şifrenin özütü alınarak pasif RFID etiketine yazılmakta ve her okuma sonrasında aynı şifre değerinin farklı sayıda iç içe özütü alınarak karta yazılmaktadır. Arduino'nun kısıtlı hesaplama gücünden dolayı iç içe maksimum 25 özüt hesaplayabilmektedir. Her 25 girişte kullanıcının şifreyi değiştirmesi istenmiştir. Fakat kullanıcı şifreyi sistem üzerinde bulunan ve karakter sayısı az olan bir tuş takımından girmektedir. Ayrıca kurulan sistem en fazla 5 kullanıcı için çalışmakta ve tek bir okuyucu üzerinden yerel hafızalı olarak işlemektedir. Bu nedenden dolayı sisteme okuyucu eklenmesi ve raporlama gibi ihtiyaçlara cevap veremeyecek durumdadır.

III. ÖNERİLEN ÇÖZÜM

Bu çalışmada gerçekleştirilmek istenen uygulama için okuyucu tarafında ATmega328P mikro kontrolcüye sahip Arduino Uno ve Mifare kart desteğine sahip SPI protokolü ile haberleşen RFID okuyucu kullanılmıştır. Sisteme kullanıcı kısıtı koymamak ve birden fazla okuyucu desteği sağlamak adına dağıtık bir sitem kurulmuştur. Kurulan sistemde kullanıcı geçmişinin ve kayıtların tutulması için merkezi bir bilgisayar ile haberleşen okuyucu ağı kullanılmıştır.

A. Kullanılan Ekipmanlar

1) Arduino Uno

Arduino Uno ATmega328P mikro kontrolcüye sahip bir mikro denetleyicidir[10]. Ayrıca Arduino Uno üzerine uygulanabilen modüllerle beraber kablolu kablosuz birçok haberleşme desteklenmektedir. Önerilen sistemde birden çok okuyucu olması, okuyucu ve merkezi sistem arası haberleşme ihtiyacını ortaya çıkarmaktadır. Bu ihtiyaca kolay çözümler geliştirebilmek için Arduino Uno seçilmiştir.

Arduino Uno RFID etiketindeki verileri okumak, okunan verilerin uygun formatta merkezi bilgisayara gönderilmesi ve merkezi bilgisayardan alınan verinin etikete yazılması aşamalarında kullanılmaktadır. Etiket üzerinde hangi bloklarda işlem yapılacağı Arduino Uno üzerinde koşan programda belirlenmiştir.

2) Rc522 Kart okuyucu

Rc522, 13,56Mhz frekansında çalışan kartlar üzerinde okuma yazma yeteneği olan bir karttır.

Arduino Uno ile SPI ara yüzünden haberleşen Rc522; etiketlerin okunması ve yazılmasında kullanılmaktadır. Seri haberleşme ara yüzü sayesinde kolay uyum sağlayabilmektedir.

B. Kullanılan Özüt Algoritmaları

1) MD5(Message Digest – Mesaj Özeti)

MD5 yaygın olarak kullanılan özüt algoritmasıdır[12]. Girişten gelen verinin boyutundan bağımsız olarak 128 bit çıkış üretmektedir. Girişten gelen veriyi 512 bitlik bloklara ayırır. Verinin boyutuna bakılmaksızın ekleme işlemi uygulanır. Lojik işlemler içeren 16 adımdan oluşmaktadır. Çıkış uzunluğunun etiket üzerinde 2 sektörde tutulmasından dolayı tercih edilmektedir.

2) SHA-256(Secure Hash Algorithm – Güvenli Özetleme Algoritması)

SHA-256 yüksek güçte ve kısa uzunlukta olmasından dolayı özüt algoritmaları içerisinde tercih edilmektedir[13]. Girişten gelen maksimum $2^{(64-1)}$ bit uzunluğundaki mesajdan 256 bit çıkış üretmektedir. Girişten gelen veriyi 512 bit uzunluğunun katı olacak şekilde yapılandırır. Dairesel kaydırma, mesaj genişletme ve lojik işlemleri içermektedir.

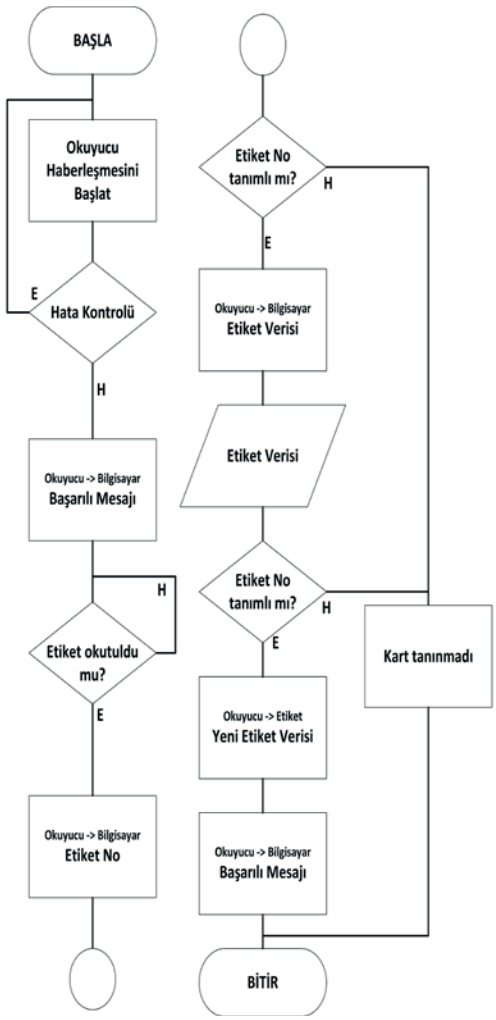
C. Önerilen Algoritma

Okuyucu ilk çalıştırıldığında iç haberleşmesi denetlenir. Herhangi bir hata ile karşılaşılmaması durumunda merkezi bilgisayara başarılı mesajı iletilir. Başarılı mesajının iletilmediği durumlar okuyucu arızalarının tespiti için kullanılmaktadır.

Okuyucu kart okutulduğunda merkezi bilgisayara her etikette benzersiz bulunan etiket numarası gönderilmektedir. Etiketin numarasını alan bilgisayar tarafından kayıt kontrolü yapılır. Etiket numarası sisteme kayıtlı değilse kart tanınmadı uyarısı verilir. Kart numarası sistemde kayıtlı ise okuyucudan etiketin ilgili sektörlerindeki veri alınır. Alınan veri sistemde kayıtlı olan etiket numarası, etiket verisi ve tarih ilişkilendirilmesi ile uyuyorsa etikete yeni veri hazırlanır. Yeni veri hazırlama kısmında alfabedeki harf ve rakamlar kullanılarak rastgele metin üretilmektedir. Üretilen metinin özüt değeri alınmasıyla yeni etiket verisi elde edilmiş olur. Özüt değerinin oluşturulması için Yeni etiket verisi okuyucuya gönderilmesiyle, okuyucu etikete yeni veriyi yazar. Yazma sırasında ortaya çıkabilecek hatalar bilgisayara

raporlanır. Hata ile karşılaşılması durumunda etiket verisi yeniden üretilerek yazılmaktadır. Hata oluşmadan yazma işlemi tamamlandıktan sonra bilgisayara gönderilen başarılı mesajı ile etiket numarası, etiket verisi ve tarih ilişkilendirmesi güncellenir.

Sisteme yeni kart tanımlanması için kartın numarasını bir seferlik olarak sisteme tanıtmak ve herhangi bir okuyucuya okutmak yeterli olacaktır. Şekil 1'de okuyucu üzerinde çalışan algoritma, Şekil 3'de merkezi bilgisayar üzerinde çalışan algoritma verilmiştir.



Şekil 1. Okuyucu Üzerinde Çalışan Algoritma

O- Rc522 kart okuyucu haberleşmesini başlat

O- Merkezi bilgisayar haberleşmesini başlat.

O- Okuyucunun sorunsuz başladığına ilişkin mesajı merkezi bilgisayara gönder.

O- Etiket okutulduğu zaman etiketin numarasını merkezi bilgisayara gönder.

O-Merkezi bilgisayardan gelen cevap olumlu ise etiket içerisindeki özüt verisini oku ve merkezi bilgisayara gönder.

M.B.- Okuyucudan gelen numara ve özüt bilgilerinin eşleşip eşleşmediğini kontrol et, eşleşiyorsa rastgele metin üret ve özütünü al. Elde edilen yeni özüt değerini etikete gönder.

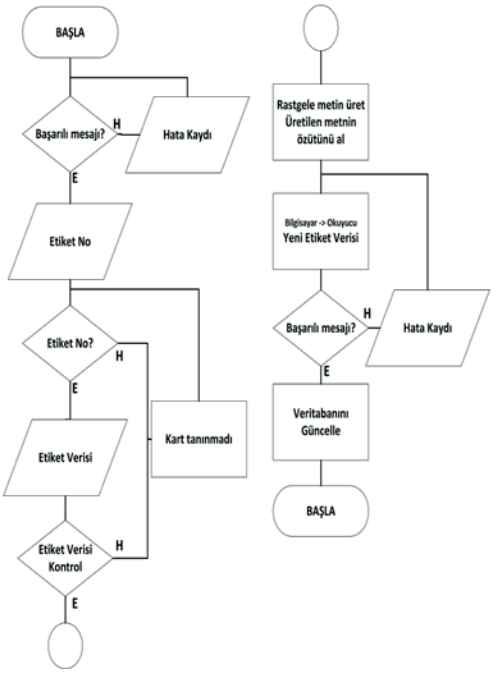
O- Merkezi bilgisayardan gelen özüt değerini al, etikete yaz.

O- Etikete yazma başarılı ise merkezi bilgisayara ilgili mesajı gönder.

M.B.- Okuyucudan başarılı yazma mesajı geldiyse özüt değerini güncelle.

O- Okuyucu
M.B.- Merkezi bilgisayar

Şekil 2. Yalancı Kod



Şekil 3. Merkezi Bilgisayar Üzerinde Çalışan Algoritma

IV. TESTLER VE KARŞILAŞTIRMA

Verimli özüt dizisi uygulaması [9]'nda önerilen prototip kullanıcıdan 0-9 ve A-D arası girişleri almak için tuş takımı, Arduino ve kart okuyucu kullanmaktadır. Etiket verisi ise iç içe özüt mekanizması kullanılarak Arduino üzerinde hesaplanmakta ve depolanmaktadır.

Önerilen çalışmada kurulan prototipte kart okuyucu ve Arduino bulunmaktadır. Hesaplama gücü gereken tüm işlemler ve etiket kayıtları merkezi bilgisayar tarafından yapılmaktadır. Ayrıca okuyucunun merkezi bilgisayara uzaklığına bağlı olarak çeşitli haberleşme modülleri kullanılabilmektedir.

Yapılan testlerde 5 adet Mifare kart kullanılmıştır. Testler güvenlik, kayıt tutma, süre ölçümü gibi bölümler halinde yapılmıştır. Performans testinde alınan süre ölçümleri ve önceki çalışmalarda verilen süre ölçümleri aşağıdaki tabloda verilmiştir.

TABLO II. PERFORMANS TEST SONUÇLARI

Fonksiyonlar	Çalışmalar		
	Verimli özüt dizisi uygulaması [9]	Önerilen Çalışma	
Kullanılan Algoritma	SHA-256	MD5	SHA-256
Etiket No Okuma Süresi (µs)	64980	840	840
Etiket Okuma Süresi(µs)	145548	25884	51940
Yeni Özüt oluşturma süresi(µs)*	72404	35064	35330
Etiket Yazma Süresi(µs)	102964	71872	115500
Toplam Süre(µs)	313492	133064	195616

[a.] Bu çalışmada Yeni Özüt Oluşturma Süresine Merkezi Bilgisayar Haberleşme Süresi dâhildir.

Tablo II'de bulunan veriler incelendiğinde sistemin referans alınan sistemden[9] daha hızlı çalıştığı görülmektedir. Etiket numarası okunurken kartın tip, hafıza vb. gibi bilgilerin alınması yerine sadece kart numarası alınması, performansta büyük bir artış sağlamıştır. Özüt algoritmasının ve rastgele sayı üretiminin bilgisayar üzerinde çalışmasından dolayı performans farklılığı ortaya çıkmaktadır.

Etiket üzerinde 16 sektör bulunmakta ve her sektör 64 bit veri depolamaktadır. MD5 algoritmasının kullanımı sırasında etiket içerisinde 2 sektör kullanılmakta, SHA-256 algoritmasının kullanımında ise 4 sektör kullanılmaktadır. Kullanılan sektör sayısının iki katına çıkmasıyla orantılı olarak okuma ve yazma süreleri de artmaktadır.

V. SONUÇLAR

Bu çalışmada pasif RFID etiketlerine kopyalama ve benzeri ataklara karşı direnç kazandırmak için dağıtık okuyucu destekli uygulama yapılmıştır. Uygulamada Arduino Uno, RC522 kart okuyucu ve merkezi bilgisayar kullanılmıştır. Gerçek pasif etiketler ile çalışılarak sistem gerçeğe yakın tasarlanmıştır. Her başarılı okumadan sonra merkezi bilgisayar tarafından rastgele metinler üzerinden üretilen özüt değeri etikete yazılmaktadır. Etiketin içerdiği özüt değerinin her başarılı okumada değişmesinden dolayı kart kopyalama ataklarına karşı savunma mekanizmalı yeni bir uygulama geliştirilmiştir. Referans alınan çalışmada bulunan kullanıcı limiti sorunu kayıtların ve kontrolün bilgisayar ortamına aktarılmasıyla, iç içe özüt alımından ortaya çıkan okuma-yazma limiti ise rastgele özüt kullanımıyla giderilmiştir. Ayrıca merkezi bilgisayar kullanımı ile etiket hareketlerinin raporlanması, sisteme yeni okuyucu eklenmesi gibi işlemler yapılabilir hale gelmiştir.

Önerilen çalışma çok yüksek kullanıcı sayılarında yeterli derecede kararlı ve hızlı olamayacaktır. Elde edilen tecrübe ve birikimle, önerilen sisteme kenar bilişim teknikleri uygulanarak daha geniş kapsamlı ve hızlı çalışmalar yapılabilir.

KAYNAKÇA

[1] P. Harrop, "the Global Market for RFID 2010-2020," vol. 7215, p. 217, 2011.

[2] Z. Shi, S. Ren, F. Wu, and C. Wang, "The Vulnerability Analysis of Some Typical Hash-Based RFID Authentication Protocols," J. Comput. Commun., vol. 04, no. 08, pp. 1–9, 2016.

[3] "Proxmark3." [Online]. Available: https://www.amazon.com/Rysc-Corp-Proxmark3-Kit/dp/B072KNWWN3. [Accessed: 24-May-2018].

[4] M. Feldhofer, "An authentication protocol in a security layer for RFID smart tags," Proc. 12th IEEE Mediterr. Electrotech. Conf. (IEEE Cat. No.04CH37521), pp. 759–762, 2004.

[5] S. G. Baskir and B. Ors, "Implementation of a secure RFID protocol," in 2013 21st Signal Processing and Communications Applications Conference (SIU), 2013, pp. 1–4.

[6] Digi International, "XBee ® /XBee-PRO ® RF Modules," Prod. Man. v1.xEx-802.15.4 Protoc., pp. 1–69, 2009.

[7] Texas Instruments, "MSP430G2x53 MSP430G2x13," Options, no. April 2011, 2012.

[8] V. Sharma, A. Vithalkar, and M. Hashmi, "Lightweight security protocol for chipless RFID in Internet of Things (IoT) applications," in 2018 10th International Conference on Communication Systems & Networks (COMSNETS), 2018, pp. 468–471.

[9] A. Pratama, T. Hidyatullah, and D. S. C. Putranto, "Efficient implementation of hash sequence authentication based on RFID," in 2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering, 2017, pp. 468–473.

[10] Atmel, "ATmega328 / P," AVR Microcontrollers. p. 442, 2016.

[11] Mifare®, "MFRC522 Datasheet," no. 3.9, p. 95, 2016.

[12] N. Jayapandian, R. Menagadevi, S. Abinaya, and O. Sri Sampoorani, "To enhance consumer privacy and security for online shopping using MD5 algorithm," in Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017, 2018, vol. 2018–Janua, pp. 1–4.

[13] M. Padhi and R. Chaudhari, "An optimized pipelined architecture of SHA-256 hash function," in 2017 7th International Symposium on Embedded Computing and System Design (ISED), 2017, pp. 1–4.