Congr. Int. en Ing. Electrónica. Mem. ELECTRO, Vol. 41, pp. 189-194, Oct 2019, Chihuahua, Chih. México
http://electro.itchihuahua.edu.mx/memorias_electro/MemoriaElectro2019.zip
ISSN 1405-2172

TECLADO DINAMICO PARA MITIGAR ATAQUES CON TERMOGRAFOS

Vega Luna José Ignacio, Lagos Acosta Mario Alberto, Salgado Guzmán Gerardo, Sánchez Rangel Francisco Javier, Cosme Aceves José Francisco
Universidad Autónoma Metropolitana-Azcapotzalco
Área de Sistemas Digitales, Departamento de Electrónica
Av. San Pablo 180, Col. Reynosa, C.P. 02200, Cd. de México
vlji@azc.uam.mx

RESUMEN.

Se presenta un sistema de autenticación usando un teclado numérico, un sistema embebido Raspberry Pi 3 y una pantalla sensible al tacto. El objetivo fue diseñar un sistema cuyas teclas numéricas cambien de posición cada vez que es usado para evitar el robo de códigos de acceso introducidos analizando el desgaste por presión o ralladuras en la pantalla u otra técnica como termografía. Utilizando el sistema embebido Raspberry Pi 3 como hardware y Raspbian como sistema operativo, se programaron en lenguaje Python las rutinas para la generación de teclados dinámicos aleatorios. El sistema se utiliza como dispositivo de autenticación para la apertura de la puerta de acceso a un centro de datos, consultando una base de datos de códigos permitidos. El tiempo de respuesta en la autenticación fue 53 ms.

Palabras Clave: Centro de datos, Python, Raspberry Pi 3, Raspbian, sistema de autenticación, termografía.

ABSTRACT.

This paper presents an authentication system using a numeric keypad, an embedded Raspberry Pi 3 system and a touch-sensitive screen. The objective was to design a system whose numeric keys change position each time it is used to prevent theft of access codes introduced by analyzing pressure wear or scratches on the screen or another technique such as thermography. Using the Raspberry Pi 3 embedded system as hardware and Raspbian as the operating system, routines for the generation of random dynamic keyboards were programmed in Python language. The system is used as an authentication device for opening the access door to a data center, consulting a database of allowed codes. The response time in the authentication was 53 ms.

Keywords: Authentication system, data center, Python, Raspberry Pi 3, Raspbian, thermography.

1. INTRODUCCIÓN

En la actualidad, existen diversos sistemas que validan la autenticación de usuarios usando una clave numérica compuesta de cuatro a ocho dígitos. El uso de sistemas de autenticación de más de ocho dígitos es inviable e impráctico por la dificultad de recordar cadenas numéricas grandes.

Un sistema digital para proporcionar acceso y uso de recursos a personas autorizadas debe detectar y excluir las no autorizadas. El acceso es controlado usando un procedimiento de autentificación para establecer con cierto grado de confianza la identidad del usuario y conceder privilegios y acceso autorizado a recursos e instalaciones. Los ejemplos comunes del control de acceso que implican la autenticación incluyen sistemas de: retiro de efectivo de cajeros automáticos, control y acceso a computadoras y acceso a áreas restringidas, entre otros [1].

Para intentar determinar la identidad de un individuo, se aplica una o varias pruebas declaradas previamente, las cuales deben cumplirse para autorizar el acceso o uso de recursos. Los factores de autenticación aplicados en seres humanos se clasifican generalmente en los tipos siguientes: 1) Algo que el usuario “es”, como por ejemplo la huella digital, el patrón de la retina, la secuencia de ADN, el patrón de la voz, el reconocimiento de la firma, las señales bio-eléctricas únicas producidas por el cuerpo vivo u otro identificador biométrico, 2) Algo que el usuario “tiene”, como por ejemplo una tarjeta de identificación, una llave de software, un certificado de software o un teléfono celular, 3) Algo que el usuario “sabe”, como por ejemplo una contraseña, una frase o un número de identificación personal o PIN, 4) Algo que el usuario “hace”, como por ejemplo reconocimiento de voz, firma o un paso al caminar, 5) Autenticación mediante dos factores "algo que el usuario tiene", como por ejemplo la llave, más "algo que sabe", como por ejemplo un número de PIN o token criptográfico y 6) Autenticación triple factor, compuesta por "algo que el usuario tiene", como por ejemplo el dispositivo criptográfico, más "algo que sabe", como por ejemplo una clave de autenticación tipo PIN, más "quién es", como por ejemplo la huella dactilar que permite autenticarse al dispositivo de forma unívoca [2]. Uno de los métodos de autenticación que lo usuarios consideran más seguro es el biométrico usando la huella dactilar, tal y como se muestra en la gráfica estadística de la Figura 1.

Los métodos de acceso a servicios digitales a través de un proceso de identificación han sido un tema de preocupación desde que el inicio de la Internet. No es un asunto de poca importancia tomando en cuenta que en los últimos seis años han sido robados 112,000 millones de dólares mediante fraudes relacionados con la usurpación de la identidad digital, según un informe de IBM. Es por eso que, la industria no cesa en su empeño de buscar herramientas cada vez más seguras, cómodas y de bajo costo que aseguren que los usuarios son quienes dicen ser. Considerando que cada vez se llevan a cabo más operaciones delicadas en línea, es imperativo superar el sistema de usuario y contraseña usado durante décadas el cual presenta grandes deficiencias [3].

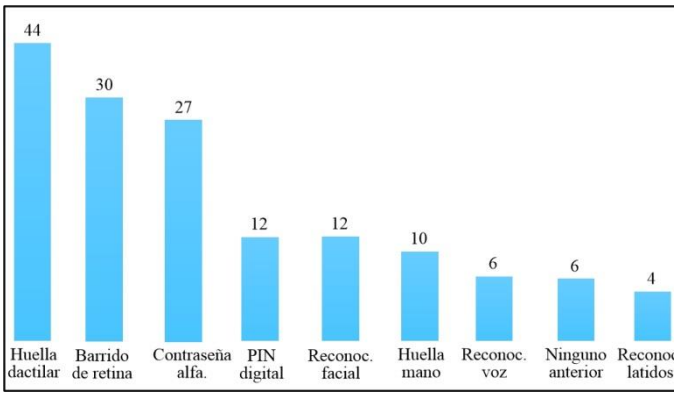


Fig. 1. Métodos de autenticación que los usuarios consideran más seguros

Un estudio realizado por investigadores de la Universidad de California [4] reveló hasta qué punto un atacante puede aprovechar el entorno para obtener contraseñas sin necesidad de malware. Los investigadores descubrieron que es posible detectar las teclas presionadas usando el calor corporal dejado en ellas, incluso siguiendo las recomendaciones de seguridad. Sólo es necesario que el atacante use una cámara térmica para mostrar iluminadas las teclas usadas como se muestra en la Figura 2. El estudio determinó que usando una cámara de rango medio se puede saber las teclas pulsadas en un teclado normal, hasta un minuto después de haberlas presionado, ya que el plástico de las teclas retiene el calor corporal suficiente para distinguirlas durante ese tiempo.

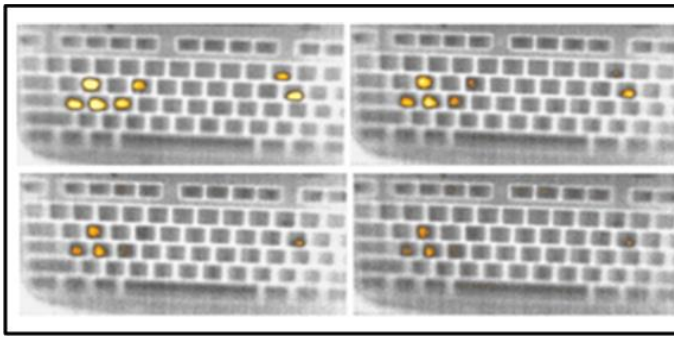


Fig. 2. Marcas térmicas en teclado de equipo de cómputo

Comúnmente, los usuarios realizan la autenticación y se retiran momentáneamente del equipo o sistema de acceso, tiempo suficiente para que alguien pase por delante del sistema con una cámara térmica y registre las teclas que han sido pulsadas al iniciar una sesión. Esta información puede ser suficiente para acceder al sistema, sobre todo si es una contraseña corta, un PIN bancario de cuatro cifras o un código de verificación. No hace falta ser un experto para lograrlo, causando que el ataque sea más peligroso.

Los ataques denominados Thermanator, así llamados porque usan un termógrafo, son realizados por un adversario interno que registra a los usuarios a través de los residuos térmicos dejados al suministrar la contraseña. El objetivo es aprender la contraseña de la víctima utilizando una cámara térmica. El atacante cuenta con un minuto para grabar el teclado antes que los residuos térmicos se disipen. No se necesita presencia de la víctima descuidada, ya que la grabación de la imagen se realiza después que se retira. No es necesario ningún conocimiento previo de la víctima para analizar las imágenes térmicas, aunque ayuda el uso de contraseñas inseguras.

Los sistemas de autenticación usados para acceder a instalaciones se basan típicamente en la utilización de tarjetas de identidad, tarjetas inteligentes o métodos biométricos. Actualmente, los métodos de autenticación más comunes se basan en texto o palabras clave y no ha sido posible crear palabras clave de fácil uso y robustas. Las investigaciones realizadas al respecto han explorado técnicas que no usan palabras claves [5] y en el uso de métodos de autenticación para acceso a la nube basado en SAMl (Security Assertion Markup Language-Lenguaje de Marcado para Confirmaciones de Seguridad) [6] o basados en códigos QR de dos niveles, uno público y el otro privado, el nivel público funciona como los códigos QR clásicos para almacenar información y el nivel privado usa patrones de textura para almacenar información codificada [7]. Otros métodos de autenticación usan palabras clave graficas (GAU-Graphical User Authentication), creados combinando dos imágenes cuyo principio de funcionamiento es que las personas recuerdan más objetos visuales que textos [8] o utilizando memorias SD y tarjetas de encriptación [9].

Los algoritmos de criptografía actuales necesitan mejorar la seguridad de las claves intercambiadas en la transferencia de información. El uso de estos algoritmos incrementa el costo de los sistemas y tiempo de procesamiento, sin embargo son importantes ya que tratan de evitar el robo de información. Desafortunadamente la criptografía puede lograr confidencialidad pero no integridad. De tal forma que los últimos años las investigaciones se han enfocado también en la autenticación en la transmisión de datos en teléfonos inteligentes [10], en redes inalámbricas de sensores usando interpolación polinomial [11], en métodos para detectar plagio de código de programas sin intervención humana [12], para encriptar la información en cajeros automáticos, o ATM, usando códigos QR [13], para prevención de fraudes para transacciones bancarias en línea usando criptografía visual extendida y códigos QR [14], para detección de robo de información confidencial, o Phishing, usando comparación de código fuente HTML y similitud del coseno [15], para el cifrado de información basado en basado en etiquetas de longitud de autenticación usando códigos Reed-Solomon [16], para mantener la confidencialidad e integridad de la información transmitida usando un canal que utiliza el algoritmo AES (Advanced Encryption Standard) y códigos de autenticación de mensajes Hash (HMAC-Hashed Message Authentication Code) [17].

Los centros de datos son la parte medular de la economía digital, big data, la nube, la inteligencia artificial e Internet de las Cosas (IoT-Internet Of Things). El acceso a este tipo de instalaciones debe ser controlado para no comprometer la seguridad de información y equipo [18]. Los últimos desarrollos dirigidos a la autenticación y encriptación para el control de acceso a centros de datos, han trabajado usando: mapas de pixeles de temperatura absoluta y emisión de la palma de la mano obtenidos con un termógrafo infrarrojo [19], códigos convolucionales y la función XOR [20], encriptación a través del protocolo de la generación de claves distribuidas (DKG-Distributed Key Generation) [21] y códigos RaptorQ [22].

Los autores no tienen conocimiento de que se ha realizado hasta ahora un sistema como el presentado en este trabajo, en el cual se utilizan elementos tecnológicos de reciente creación, de fácil uso y precio bajo. Fundamentalmente, la aportación del sistema es el uso del teclado virtual y una pantalla sensible al tacto con los que se logra mayor seguridad que usando algoritmos más sofisticados.

La conducción térmica es la transferencia de calor entre dos objetos en contacto con temperaturas diferentes. Se expresa como el movimiento de la energía térmica del objeto más caliente al objeto más frío. Se aprovecha la vulnerabilidad de esta característica, utilizando la transferencia de energía de un dedo humano a una tecla presionada, para el robo de códigos de acceso. El trabajo aquí presentado tiene como objetivo mitigar esta vulnerabilidad para evitar el ataque Thermanator, usando un simple concepto: el cambio de posición de las teclas en cada autenticación a través de un teclado virtual en una pantalla sensible al tacto que inicialmente muestra dígitos como se muestra en la Figura 3.

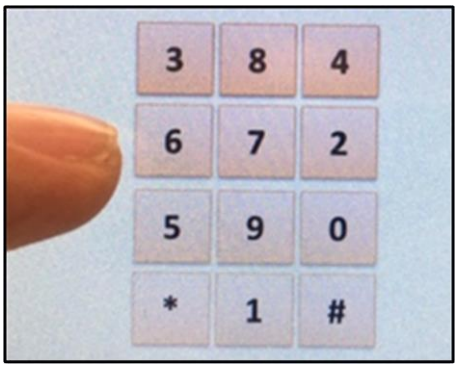


Fig. 3. Teclado virtual en una pantalla sensible al tacto

2. DESARROLLO

En la realización de este trabajo la metodología seguida fue dividir el diseño en cuatro etapas como se muestra en la Figura [4]. Las etapas son las siguientes: la fuente de alimentación, el actuador de la contrachapa eléctrica, la pantalla táctil LCD y el sistema embebido Raspberry Pi 3.

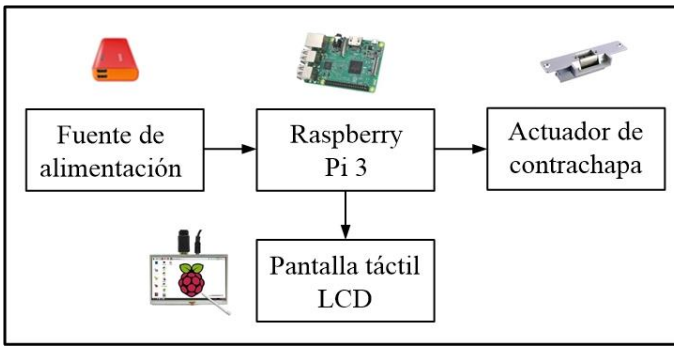


Fig. 4. Diagrama de bloques del sistema desarrollado

2.1. La fuente de alimentación.

En la implantación de la fuente de alimentación se utilizó un banco de baterías de 20,000 mAh, el cual alimenta el sistema y lo mantiene en operación hasta 8 horas en reposo y 2 horas en operación normal. Este banco está conectado a la línea eléctrica para no perder el suministro de energía, a menos que se presente un incidente prolongado en la alimentación eléctrica.

2.2. El actuador de la contrachapa eléctrica.

Este módulo consta de una contrachapa eléctrica Philips modelo 310, que incluye la fuente de alimentación de 12 V y un relevador con entrada de bajo voltaje controlado por la señal generada por el sistema embebido Raspberry para la apertura de la contrachapa.

Cuando el usuario ha suministrado la clave correcta, el microcontrolador del sistema embebido Raspberry activa la contrachapa durante 10 segundos para que el usuario empuje la puerta y pueda acceder al centro de datos.

2.3. La pantalla táctil LCD.

La pantalla con sensor táctil que usada en el sistema es modelo Kuman de 5 pulgadas. Es una pantalla táctil tipo resistiva con una resolución de 800 x 480, cuenta con conector HDMI, módulo de carga micro USB y conector directo a Raspberry Pi, así como controladores para este sistema embebido. En la Figura 5 se muestra la conexión realizada entre de la pantalla con el sistema Raspberry Pi.

2.4. El sistema embebido Raspberry Pi 3.

Para realizar la instalación del sistema operativo y arrancar la tarjeta del sistema embebido Raspberry Pi 3, se utilizó el programa *Win32 Disk Imager*, con el cual se creó la imagen de Raspbian en una tarjeta de memoria SD. Posteriormente, se conectaron los siguientes dispositivos periféricos a la tarjeta Raspberry: teclado, mouse y monitor HDMI. Se insertó la tarjeta SD y se encendió la tarjeta Raspberry Pi 3. Se actualizaron parches y herramientas de red ejecutando desde una sesión de terminal los comandos: *apt-get update* y *apt-get upgrade*. En la puesta a punto es importante no arrancar servicios de red innecesarios, ya que esto podría causar conflictos con los análisis

de red que se soliciten remotamente. El único servicio arrancado con fines administrativos fue *ssh*, para poder conectar al sistema embebido y configurar utilizando una terminal remota. Los parámetros de red dirección IP, máscara de red y puerta de enlace, se establecen de acuerdo a la red donde este sistema trabaje. Se descargó la distribución del lenguaje de programación Python usada para desarrollar las interfaces del teclado dinámico y control del actuador.

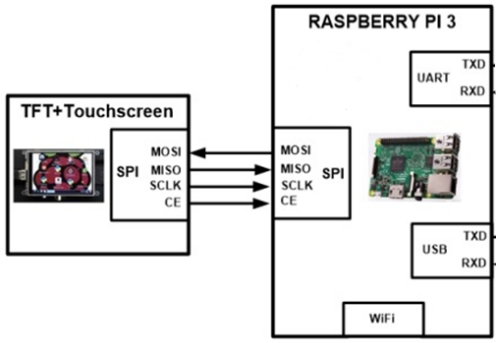


Fig. 5. Conexión de la pantalla táctil con la Raspberry Pi 3

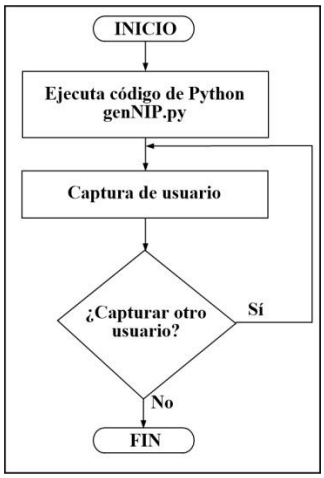
2.4.1 Inicialización de la tarjeta Raspberry Pi 3.

El funcionamiento del sistema consistió en almacenar la información de los usuarios en una base de datos cifrada conjuntamente con los NIP de 4 dígitos. La base de datos de usuarios se almacenó utilizando el formato del archivo *passwd* de las distribuciones de Linux, en el cual la contraseña está cifrada y no puede visualizarse en texto plano, como se muestra en la Figura 6.

La aplicación desarrollada para crear la base de datos se ejecuta en la línea de comandos y basta con invocar un Shell de Linux. La rutina empleada para realizar el cifrado es *crypt* la cual pertenece a la biblioteca de funciones *cryptsetup* de Raspbian y permite realizar cifrados directamente desde Python.

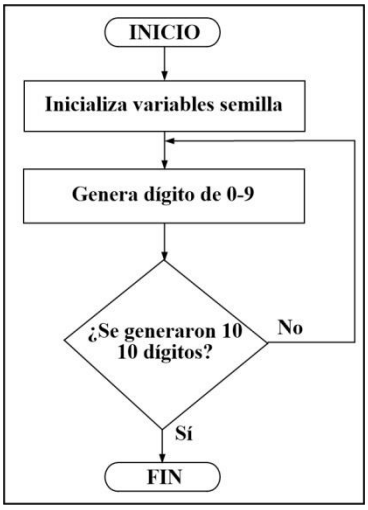
2.4.2 Algoritmo de generación de posicionamiento aleatorio de dígitos.

Para la generación de posicionamiento aleatorio de los dígitos en la pantalla táctil, se utilizó el objeto *random* y la función *radint*. Con esto se genera la posición de cada número que muestra un teclado. El diagrama de generación es el mostrado en la Figura 7.




```
usuario1:PGtm63FZaIE2
usuario2:2Cph1eLFQk0z
usuario3:FeEZd4baAVce
usuario4:PP9MWnRBQ0oy
usuario5:gaHg0ToMZ6h4
usuario6:3E2Ewx23z60q
usuario7:0eQIB4yPS0Lk
```

Fig.6. Diagrama de flujo para archivo de cifrado del NIP



Ubicación	Dígito
0	9
1	2
2	8
3	4
4	3
5	1
6	5
7	6
8	7
9	0

Fig. 7. Diagrama de flujo para la generación aleatoria de dígitos

2.4.3 Algoritmo de posicionamiento en la pantalla táctil.

Para visualizar un nuevo orden del teclado, se hace uso de la tabla generada en el punto 2.4.2 mostrada en la Figura 7, se utiliza el posicionamiento para obtener las coordenadas del teclado y capturar los dígitos presionados en cada momento con el valor seleccionado, como se muestra en la Figura 8. Inmediatamente después que el usuario proporciona un NIP valido, de envía la señal al actuador de la contrachapa y se registra en una bitácora o archivo de accesos (accesos.log) el usuario autentificado.

3. RESULTADOS

Se realizaron tres grupos de pruebas. En el primer grupo de pruebas se usaron siete usuarios y se tomaron veinte muestras, se

evaluaron los aciertos y errores al suministra el NIP asignado. Se realizaron las pruebas asignando al usuario 30 minutos antes su NIP para memorizarlo. La muestra de usuarios fueron personas entre 20 y 45 años de edad sin limitantes físicas. El tiempo entre prueba y prueba fue de 30 segundos. El resultado de autenticaciones positivas y negativas obtenidas se indica en la gráfica de la Figura 9.

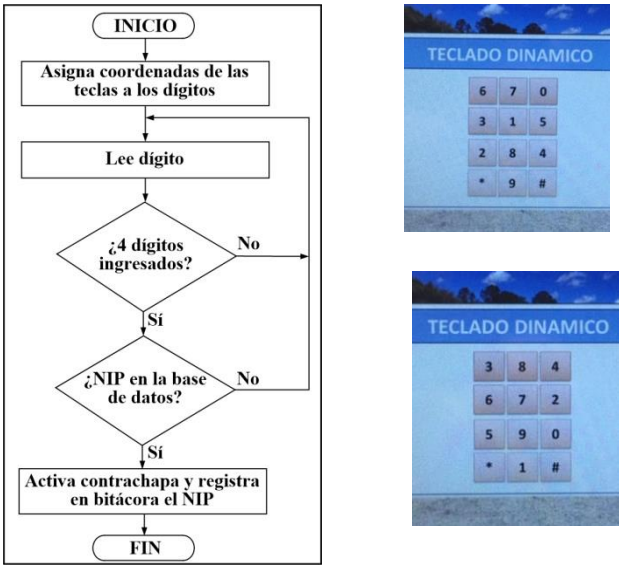


Fig. 8. Diagrama de flujo de captura del NIP

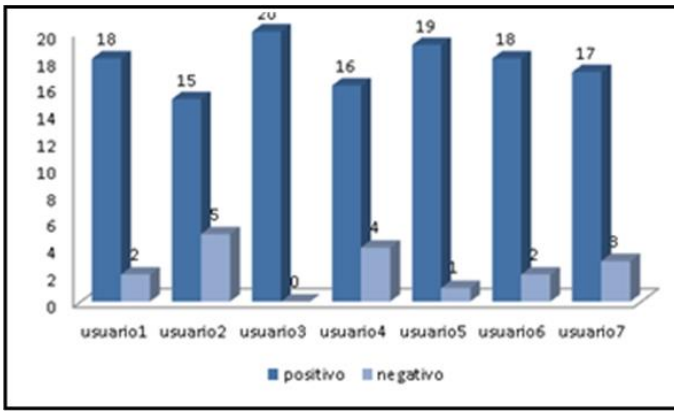


Fig. 9. Autenticaciones exitosas en el primer grupo de pruebas

El segundo grupo de pruebas tuvo como objetivo determinar la precisión del sistema de autenticación de usuarios registrados en la base de datos. En estas pruebas aumentó la cantidad de usuarios usados a 200. Cada usuario suministro una vez el NIP asignado, algunos correctamente y otros no. En los que suministraron el NIP correcto la precisión obtenida fue 98.3%, lo cual se debió a factores físicos como por ejemplo que presionaron más de una tecla al mismo tiempo o movimiento involuntario del dedo de la mano al presionar una tecla, no fue por funcionamiento incorrecto del sistema

El tercer grupo de pruebas tuvo como objetivo medir el tiempo de respuesta del sistema. Para realizar estas pruebas en cada una de las fases del grupo de pruebas anterior, se registró en la hora de captura del NIP de una persona registrada en la base de datos y la hora cuando el sistema activa la contrachapa eléctrica. El tiempo de respuesta fue 53 ms. en promedio.

4. CONCLUSIONES

El resultado de este trabajo fue un sistema de autenticación de usuarios para acceso a un centro de datos usando componentes de bajo costo y tecnología reciente. El sistema cumple con las especificaciones solicitadas: no intrusivo a las instalaciones del centro de datos, confiable y de bajo costo. Con el porcentaje de precisión y tiempo de respuesta logrados, el centro de datos solicitó realizar una segunda versión que incorpore las siguientes funcionalidades: 1) Construir e instalar 10 sistemas distribuidos como el presentado en este trabajo en accesos controlados del centro de datos y 2) Integrar un servidor de base de datos de usuarios autorizados que reciba y valide las solicitudes de autenticación de los sistemas distribuidos. Este servidor debe poder ser accedido remotamente desde la Internet. Los usuarios tenían la costumbre de memorizar el NIP y la posición de las teclas. Al realizar cambios en la posición de los dígitos los usuarios presentaron una resistencia natural, la cual no fue significativa, solo fue cuestión de familiarizarse con el sistema.

5. REFERENCIAS

[1] J. P. Joy, T. S. Jyothis, "Secure authentication", Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-3.

[2] P. Mittra, N. Rakesh, "A desktop application of QR code for data security and authentication", International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2016, pp. 1-5.

[3] L. Zhou, V. Varadharajan, M. Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage", IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 11, 2015, pp. 2381-2395.

[4] T. Kaczmarek, E. Ozturk, G. Tsudik, "Thermanator: Thermal Residue-Based Post Factum Attacks On Keyboard Password Entry", Cornell University [en línea], disponible: https://arxiv.org/abs/1806.10189, July, 2018, sitio visitado Enero, 2019.

[5] M. Morii, H. Tanioka, K. Ohira, "Research on Integrated Authentication Using Passwordless Authentication Method", IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 2017, pp. 682-685.

[6] D. Jing, J. Yan, A. Fujiang, "An Improved Uniform Identity Authentication Method Based on SAML in Cloud Environment", IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 2018, pp. 533-536.

[7] I. Tkachenko, W. Puech, C. Destruel, "Two-Level QR Code for Private Message Sharing and Document Authentication", IEEE Transactions on Information Forensics and Security, Volume: 11, Issue: 3, 2016, pp. 571-583.

[8] B. Bilgi, B. Tugrul, "A Shoulder-Surfing Resistant Graphical Authentication Method", International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, Turkey, 2018, pp. 1-4.

[9] G. Zhao, Y. Li, L. Du, "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment", 2nd International Conference on Information Science and Control Engineering, Shanghai, China, 2015, pp. 156-159.
[10] K. Matsuo, A. Kanai, T. Hatashima, "Dynamic Authentication Method Dependent on Surrounding Environment", IEEE 7th Global Conference on Consumer Electronics (GCCE), Nara, Japan, 2018, pp. 855-857.
[11] P. Zhou, M. Xiao, Z. Xia, "A Message Authentication Method for Wireless Sensor Networks Using Polynomial Interpolation", 2nd International Symposium on Dependable Computing and Internet of Things (DCIT), Wuhan, China, 2015, pp. 151-153.
[12] N. Gupta, V. Gandhi, C. Hariya, "Detection of Code Clones", International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018, pp. 1-4.
[13] V. Malathi, B. Balamurugan, S. Eshwar, "Achieving Privacy and Security Using QR Code by Means of Encryption Technique in ATM", Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), Tindivanam, India, 2017, pp. 281-285.
[14] S. Khairnar, R. Kharat, "Online fraud transaction prevention system using extended visual cryptography and QR code", International Conference on Computing Communication Control and automation (ICCUBEA), Pune, India, 2016, pp. 1-4.
[15] S. Roopak, T. Thomas, "A Novel Phishing Page Detection Mechanism Using HTML Source Code Comparison and Cosine Similarity", Fourth International Conference on Advances in Computing and Communications, Cochin, India, 2014, pp. 167-170.
[16] A. E. Zhilyaev, E. B. Gurova, "On the question of the authentication tag length based on Reed-Solomon codes", Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russia, 2018, pp. 1-5.
[17] S. A. Tamer, "Generated Un-detectability Covert Channel Algorithm for Dynamic Secure Communication Using Encryption and Authentication", Palestinian International Conference on Information and Communication Technology (PICICT), Gaza City, Palestinian Authority, 2017, pp. 6-9.
[18] T. Suresh, A. Murugan, "Strategy for Data Center Optimization : Improve Data Center capability to meet business opportunities", 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Palladam, India, India, 2018, pp. 184-189.
[19] H. L. Yu, Y. L. Li, T. Y. Liao, "Fast and Accurate Emissivity and Absolute Temperature Maps Measurement for Integrated Circuits", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume: 26, Issue: 5, 2018, pp. 912-923.
[20] J. Qiu, H. Li, J. Dong, "Biometrics Encryption Based on Palmprint and Convolutional Code", 2nd International Conference on Multimedia and Image Processing (ICMIP), Wuhan, China, 2017, pp. 187-190.
[21] P. P. Gutal. R. S. Kothe, S. B. Jahveri, "Efficient hierarchical cloud storage data access structure with KDC", IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), Pune, India, 2016, pp. 328-332.
[22] N. Zhao, Y. Zhang, K. Xiong, "On Massive Data Storage Security in Cloud Computing with RaptorQ codes", 14th IEEE International Conference on Signal Processing (ICSP), Beijing, China, China, 2018, pp. 758-761.