ISSN: 2584-0495 Vol. 2, Issue 6, pp. 924-929

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Secure Touch: IoT-Enabled Finger-Touch Authentication for Seamless Mobile Security

D Sai Revanth, M Sai Subhash, M Kesav, and B Harshith Reddy

Cite as: Revanth, D. S., Subhash, M. S., Kesav, M., & Reddy, B. H. (2024). Secure Touch: IoT-Enabled Finger-Touch Authentication for Seamless Mobile Security. International Journal of Microsystems and IoT, 2(6), 924-929. https://doi.org/10.5281/zenodo.13221623

Published online: 24 June 2024

DOI: https://doi.org/10.5281/zenodo.13221623

International Journal of Microsystems and IoT
Vol. 2, Issue 6, pp.; 924-929; DOI: https://doi.org/10.5281/zenodo.13221623

Secure Touch: IoT-Enabled Finger-Touch Authentication for Seamless Mobile Security

D Sai Revanth, M Sai Subhash, M Kesav and B Harshith Reddy

PVP Siddhartha Institute of Technology, Andhra Pradesh, India

ABSTRACT
Source touch is an inventive user authentication system that integrates economical finger inputs with physical vibration on a variety of surfaces. By expanding its verification functionalities to encompass solid substrates as well as touch displays, this system offers viable solutions for intelligent access systems that regulate the entry of vehicles, apartment access, and smart appliance control. By incorporating passcodes, surface dependencies, physiological and behavioral characteristics, and passcodes, Source touch positions itself as a sophisticated, economical, and resilient security solution. By integrating contact sensing with vibration signals on diverse materials, this system integrates advanced algorithms that can recognize PINs, lock patterns, and fundamental gestures. By means of frequency domain feature extraction, Source touch can capture physiological and behavioral attributes that are exceedingly specific. Source touch, which consists of a low-cost vibratory motor and receiver, can be attached with ease to an extensive variety of surfaces. Extensive experimental protocols consistently yield remarkable precision, with two trials eclipsing 95% accuracy, and false- positive rates remaining below 3%, thereby emphasizing the system's resistance to potential threats. By capitalizing on its versatility and economical nature, Source touch possesses considerable promise in augmenting secure user authentication in practical contexts. Operating via Telegram, the system incorporates a camera module for authorized person detection, which enables visual verification and provides information on unauthorized entries. By utilizing the Telegram bot interface, this feature not only enables remote locking and unlocking but also empowers manual intervention via immediate notifications, thereby enhancing the security of the system.

KEYWORDS
Secure touch; lock Patterns; algorithms

1. INTRODUCTION

Authentication, an essential procedure that verifies the identity of users, is ubiquitous in our everyday existence. It has brought about a significant transformation in keyless control across multiple sectors, including smart residences, corporate facilities, apartment buildings, hotel rooms, and vehicle access points, about smart access systems. The increasing prevalence of these systems is supported by market forecasts, which indicate a significant annual growth rate of 7.49%. This growth is expected to reach its peak at $9.8 billion by 2022 [1]. Currently, clever security access systems rely primarily on traditional techniques such as fingerprints, intercoms, cameras, and cards. Nevertheless, these approaches possess certain limitations [2], including exorbitant expenses for apparatus, complex hardware setups, and varied maintenance needs. Utilizing low-power, low-cost Tangible User Interfaces (TUI) to authenticate users at a variety of entry points including facility entrances, apartment doorways, and vehicles is an emerging transformative trend [3]. For example, token devices such as smart rings, gloves, or pens present an innovative method of linking identities via contact interactions [4, 5].

Similarly, ultra-thin sensing pads are used for automobile driver authentication [6].

Contemporary microwave ovens and stove tops are anticipated to adopt technological advancements such as isometric buttons and rotary inputs resembling those found on iPods, which will supplant conventional physical buttons and augment functionality and adaptability [7]. The pervasive implementation of these advancements is hindered by the requirement for electric conductivity and an electric field on surfaces to facilitate energy production and storage. User authentication, which is crucial considering growing privacy concerns, has conventionally relied on text-based passwords, which impose significant memorization burdens on users. Although graphical passwords that utilize gridlock patterns or image selection provide alternatives, shoulder browsing threats continue to exist [8]. Biometric schemes that integrate facial recognition, iris patterns, fingerprints, and other biometric techniques, effectively mitigate security concerns at the expense of privacy. Behavioral attributes such as the dynamics of keystrokes and mouse movements facilitate ongoing verification. Present smart access methods necessitate expensive hardware, including intercoms, cameras, access cards, and biometric readers [9]. The implementation of Source Touch, a novel authentication system that utilizes vibration signals, holds the potential to extend its utility beyond touch displays and fortify security in a multitude of intelligent access environments.

2. LITERATURE REVIEW

Several literature surveys explore user authentication systems, with a focus on touch-based approaches. “Strengthen user authentication on mobile devices by using user’s touch dynamics pattern” investigates touch dynamics biometrics, enhancing security by combining touch patterns with PINs. The “Touch-Free Biometric Authentication System” provides an overview of touch-free modalities like face, iris, voice, and behavioral biometrics. “Multi-Factor Authentication: A Survey” delves into various factors, including touch-based methods, discussing challenges and future trends. Additionally, the “Recent Advances in MobileTouch Screen Security Authentication Methods” review covers developments in PINs, patterns, and biometrics for smartphone security. These surveys collectively contribute valuable insights to the field of secure user authentication.

2.1 Touch Dynamics Biometrics:

The research article titled “Strengthen user authentication on mobile devices by using user’s touch dynamics pattern” explores touch dynamics as a biometric authentication solution for mobile devices. By capturing raw touch dynamics data, the system extracts feature unique to each user’s touch behavior. These features are then combined with traditional PIN-based authentication, significantly enhancing security. The integration of touch dynamics provides an additional layer of protection against impersonation attacks, making it a promising approach for mobile authentication.

2.2 Touch-Free Biometric Authentication:

The concept of [20] touch-free biometric authentication is gaining traction. In the chapter “Touch-Free Biometric Authentication System,” various modalities are discussed, including face recognition, iris scanning, voice authentication, and behavioral biometrics. These methods allow users to authenticate without physical contact, improving convenience while maintaining security. The chapter also addresses challenges faced by both users and service providers in implementing touch-free authentication systems.

2.3 Multi-Factor Authentication (MFA):

Multi-factor authentication (MFA) combines multiple authentication factors to enhance security. In the survey paper titled “Multi-Factor Authentication: A Survey,” touch-based methods are explored alongside other factors such as PINs, graphical passwords, and biometrics. The paper discusses the need for balancing security and usability, proposing multi-objective optimization techniques. It also outlines future trends in MFA, emphasizing the importance of robust and adaptable authentication systems.

2.4 Advancements in Mobile Touch Screen Security:

A systematic review titled “Recent Advances in Mobile Touch Screen Security Authentication Methods” focuses on developments specific to smartphone touch screens. The review covers various techniques, including PINs, lock patterns, and biometrics. By classifying these methods and addressing research challenges, the paper provides insights into the current state of mobile touch screen security. Researchers and practitioners can use this information to design more effective and user-friendly authentication mechanisms.

2.5 Beyond Authentication: Visual Verification and Remote Control:

Beyond traditional touch-based authentication, innovative features are emerging. For instance, the system described in your abstract incorporates a camera module for authorized person detection. This enables visual verification alongside touch-based authentication. Additionally, the system operates via Telegram, allowing remote locking and unlocking. Immediate notifications empower manual intervention, enhancing overall security. By combining touch dynamics with visual cues and remote-control capabilities, such systems offer practical solutions for intelligent access control and secure user authentication.

3. PROPOSED SYSTEM

3.1 OVERVIEW

Source touch presents an innovative methodology for authentication by examining distinct vibration signals emanating from a variety of surfaces, including smart home appliances and doors. Low-power proximity or motion sensors initiate incontestable vibrations upon activation. By subjecting the system to Data Calibration, synchronized vibration signals are maintained, and clock drift effects are mitigated. From vibration signals, features based on spectral points and the Mel-frequency cepstral coefficient (MFCC) are extracted using the Fisher Score to select discriminative features. Users enroll during the profiling phase by placing pressure on their fingertips at various grid points, thereby constructing a Grid Profile. Filtering, SVM-based Grid Point Index Trace Derivation, and PIN/lock pattern recovery are all components of authentication. Source touch additionally enables authentication based on gestures by implementing mechanisms to capture inherent gesture behavior during the profiling phase and rectify inconsistencies via time-distorted feature sequences and distribution analysis. The adaptability of the system permits the utilization of various authentication methods, providing flexibility without compromising security or individuality. As shown in Figure 1, the vibration motor initiates low- intensity vibrations to prepare Source touch for Data Calibration, which serves to synchronize signals and reduce the adverse effects of clock drift. Figure 3, illustrates the block diagram of the proposed device.

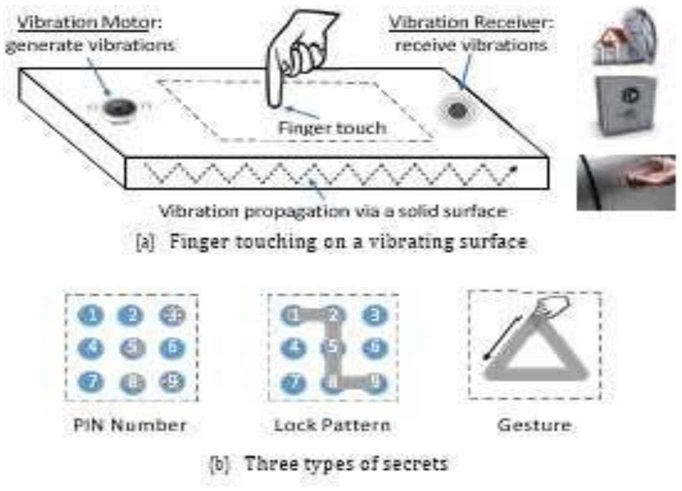

Fig. 1 Finger touch on a vibrating surface

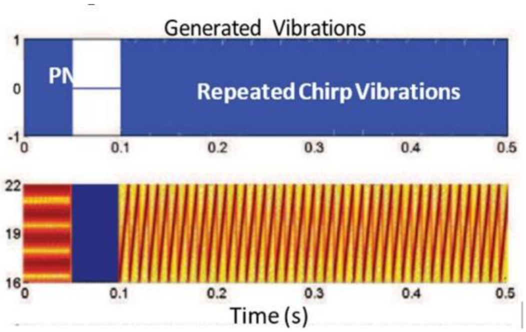

Fig.2 Generated vibration

Where,

- f_k is the frequency in H_z corresponding to bin k,
- S_k is the spectral value at bin k. The magnitude spectrum and power spectrum are both commonly used.
- b1 and b2 are the band edges, in bins, over which to calculate the spectral entropy

4. VIBRATION SIGNAL CALIBRATION

$$Entropty = -\sum_{k=b1}^{b2} \frac{Sk \log(Sk)}{\log(b2-b1)}$$

It is critical to attain synchronization between the vibration motor and receiver of Source touch to derive features from chirp vibration signals consistently. To ensure temporal alignment, the generated chirp vibrations are appended with a pseudo-noise (PN) sequence preamble consisting of 2400 samples that possess optimal autocorrelation properties. By utilizing cross-correlation between the PN sequence of the received vibratory signal and the PN sequence that is known to be generated, this preamble enables synchronization. It is of the utmost importance to address clock drift in the Analog to Digital Converter (ADC) when receiving vibration signals. Inconsistencies between the configured and actual sampling rates may result from clock imperfections. To address this issue, a calibration phase is implemented during which the motor emits periodic brief vibration chirps at consistent time intervals to prevent clock drift. By employing cross-correlation, it is possible to discern a linear progression in sample latencies for received chirps, which indicates a marginally higher actual sampling rate in comparison to the configured rate. By fitting a quadratic curve with least- squares, an approach is found to modify the starting point (Sp) for each received chirp, thereby ensuring synchronization in the face of clock drift.

4.1 Prototyping and Experimental Setup

A user authentication evaluation was performed utilizing PINs and lock patterns on a 3×3 square grid, which was drawn on a solid surface in a typical office environment and could be extended as necessary. Each grid point was separated by 3cm. The experimental setup involved two surfaces a wooden table (e.g., an executive desk) beneath the vibration motor and receiver, and an apartment door panel between the motor and receiver. Gesture-based authentication obviated the necessity to manually strike or traverse grid points, instead emphasizing straightforward finger movements within a 6cm × 6cm area. Vibrations were produced by a Linear Resonant Actuator (LRA) motor featuring frequency and amplitude adjustments. Signals were detected through an audio port using a low-cost piezoelectric sensor equipped with a low-power amplifier. The system, which prioritizes inexpensive sensor configurations, aims for extensive implementation in diverse environments such as apartments, hotels, and offices. The estimated cost of the entire system is in the tens of dollars. Other authentication methods, including biometric and facial recognition, can be quite expensive, reaching several hundred dollars [10].

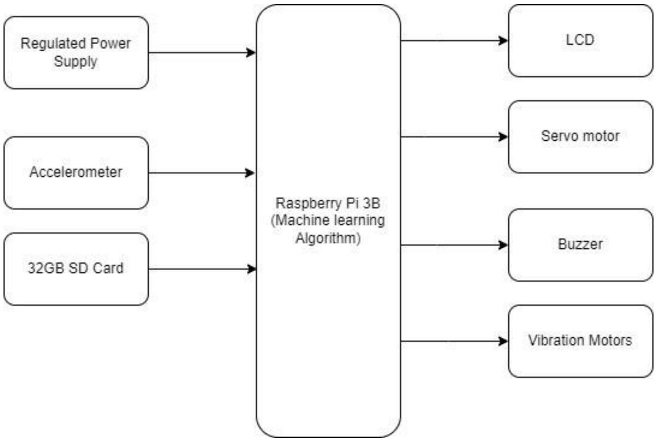

Fig. 3 Block diagram of IoT Enable Authentication System

4.2 AUTHENTICATION USING PIN NUMBERSAND LOCK PATTERNS

Vibration signals that are received by the system occur when the user enters the Adhere sequence or lock plan. By utilizing a sliding window technique, vibration highlights are derived from each window, including spectrum-based and MFCC- based features. Following this, finger-press positions are classified utilizing a machine learning-based system, more precisely a Reinforce Vector Machine (SVM) implemented with LIBSVM, in accordance with the user's customized grid profile. The grid point list that is generated illustrates the approximated locations of finger presses across the complete Stick sequence or lock design input. This inferred grid point list, which takes into account user behavior and physical characteristics, enables precise identification of the Stick sequence or lock design, thereby ensuring user authentication against erroneous inputs

5. HARDWARE DESCRIPTION

In 2006, at the University of Cambridge, Eben Upton, Rob Mullins, Jack Lang, and Alan Mycroft conceived the Raspberry Pi, an inexpensive computer designed for children. In 2008, to combat the waning interest in computer science, [11,12] the undertaking underwent an expansion to include powerful processors and multimedia functionalities. In conjunction with Pete Lomas and David Braben, the Raspberry Pi Foundation was established. With the introduction of mass production of the Model B in 2012 by Element 14/Premier Farnell [13,14,15] and RS Electronics, the foundation reaffirms its dedication to ensuring that young people have extensive opportunities to acquire technological education. [16,17] Within a span of two years, the Model B has surpassed two million units.

5.1 Raspberry Pi 3B

The Raspberry Pi 3B is a diminutive single-board computer that features an integrated wireless capability, a 1.2GHzquad-core processor, and 1GB RAM. GPIO, HDMI, and USB interfaces make it an ideal component for do-it- yourself endeavors. Programming, home automation, and fundamental computing duties are some of the many applications for this inexpensive and energy-efficient device.

5.2 16X2 LCD

A ubiquitous alphanumeric display module, the 16x2 LCD (Liquid Crystal Display) features 16 columns and 2 rows to accommodate 32 characters simultaneously. It is extensively employed in electronic projects and offers a straightforward interface for information presentation, rendering it applicable to a wide range of applications, including temperature displays and rudimentary messaging systems.

5.3 Vibration Motor

When powered by electricity, a vibration motor is a compact electromechanical device that produces vibrations. Frequent implementation in mobile phones and haptic feedback systems, it serves to enhance interactive experiences and alert users through the provision of tactile sensations in accessories and electronic devices.

5.4 5V Regulated Power Supply

A 5V Regulated Power Supply is essential for fueling electronic circuits and components as it guarantees a stable and consistent 5-volt output. It provides a consistent power supply for low-power electronic projects involving microcontrollers, sensors, and other devices by regulating voltage fluctuations.

5.5 Servo Motor

In order to generate precise and controllable angular motions from electrical signals, servo motors are rotary actuators. It is highly applicable in robotics and automation due to its precise position control capabilities, which render it well- suited for implementing in steering mechanisms and robotic limbs.

5.6 Buzzer

When activated, an electronic audio signaling device known as a buzzer emits a distinct sound. Its widespread application in electronic devices, alarms, and timers is to emanate a continuous or pulsed tone that serves as an audible alert system for user notification or signaling purposes.

5.7 Camera module

The system-integrated camera module records images in the event that an erroneous passcode is entered. The user's mobile application is promptly notified of these images, facilitating instantaneous visual verification and affording the capability to authorize or deny access remotely.

An additional layer of security is provided by the door latch via vibration analysis. Upon the entry of a passcode, the system proceeds to analyze the distinct contact vibration pattern. Negative inputs elicit a beep and engage a camera, which proceeds to capture and transmit an image to the user's mobile application. Based on the photograph, the authorized user can remotely grant or deny access. For enhanced property protection, this integrated approach combines physical and digital security, ensuring the correct user's presence via vibration matching and providing real-time surveillance and control via a mobile application

6. SOFTWARE

6.1 Raspberry Pi

Raspberry Pi-specific Raspbian, a free operating system based on Debian, includes more than 35,000 pre-compiled software packages for straightforward installation. Initially introduced in June 2012, continuous enhancements place a premium on efficacy and stability. The Raspberry Pi is configured by downloading Raspbian, unzipping the file, and writing the img file to the SD card using specialized disk imaging software such as win32diskimager-binary. This process, which is distinct from conventional computers, may appear complicated but is quite simple for Windows users who adhere to the following steps.

6.2 Proteus

Printed Circuit Board (PCB) refers to an electronic circuit board that features printed copper connections. Dotted printed circuit boards (PCBs) are characterized by apertures through which wires can be connected and components inserted manually; this characteristic provides adaptability but presents design complexities. The process of layout printed circuit boards (PCBs) entails several steps: software-based circuit design, etching to generate a copper layout, and soldering components into designated locations. Although dotted PCBs provide customization at the expense of intricacy, layout PCBs streamline the design process through the use of software tools. Proteus, Express PCB, Eagle PCB, PCB Elegance, Free PCB, Open Circuit Design, and Zenith PCB [18,19] are among the numerous PCB design software options available. Proteus is an exceptional design suite that integrates the ARES PCB layout program with the ISIS schematic capture program to facilitate comprehensive circuit development. With its inclusion of a SPICE simulator, design principles, and a 3D viewer, this software proves to be highly beneficial in both academic and professional environments.
To construct a frequency generator operating at 38 kHz utilizing a 555 timer IC, one must opt for the following components from the Proteus library: the 555 timer IC, 470Ω and 22Ω resistors, a 10KΩ variable resistor, a 0.001µF capacitor, and an IR LED. The library is accessible via the toolbar or the menu bar.

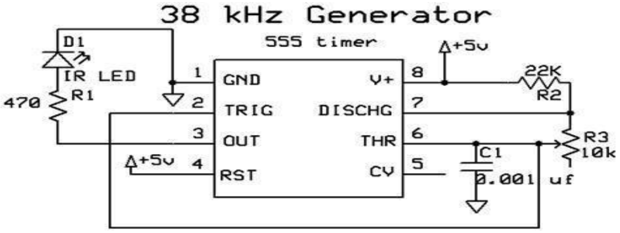

Fig. 4 555 Timer

Arrange the components in the workspace, modify their angles, and draw connections in accordance with the circuit diagram shown in figure 4 using the pen symbol. Once the design is finished, save the file and employ the virtual simulation functionality in Proteus to visually inspect and troubleshoot the circuit without the need to physically construct it. In addition, this software facilitates the design of the circuit's PCB layout.

7. RESULT AND DISCUSSION

7.1 Impact of Grid

By amplifying the virtual lattice on the verification surface, the proposed system enables the implementation of secure virtual keyboards and palm verification, among other things. Systems' robustness is evaluated through implementation on wooden, acrylic, and glass surfaces, with sensors positioned between testing areas. Ten individuals volunteer to create profiles by inputting PINs ten times. On a rudimentary layout, SVM and DNN-based models attain verification accuracy exceeding 95% for all materials; among these, wood exhibits the maximum average accuracy at 97%. The effect of surface dimensions on precision is negligible (less than 2%). Achieving efficiently classifying additional grid points. The application of DNN-enhanced models to sophisticated layouts results in an accuracy of 96% for wood and a minimum of 95% for acrylic and glass. By combining SVM and DNN, the system demonstrates exceptional adaptability. User verification is affected by varying inter-grid point distances (1.5cm, 3cm, and 4.5cm) on a wood board with a 3 3 fundamental grid layout. The accuracy of DNN-based PIN verification is 80% for 1.5cm inter-grid distances and 94% for 4.5cm inter-grid distances. An optimal inter-grid distance of 3cm to 4.5cm is recommended by the study for practical implementation, as it strikes a balance between input efficiency and verification accuracy.

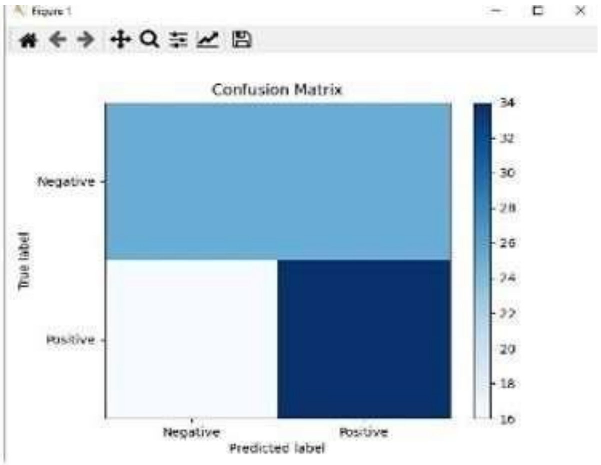

Fig. 5 Confusion Matrix

7.2 Impact of figure touching speed

The figure 6 is performance of authentication and the stability of vibration signals are both substantially impacted by the velocity at which the finger presses during PIN number-based authentication. In order to assess the influence of touching speed, five participants construct their system point list profiles by contacting at an average velocity of approximately 2 seconds per touch. Each participant is then required to input a four-digit PIN code ten times, alternating between fast and slow speeds. The results indicate that the overall accuracy of Stick arrangement confirmation is approximately 64% at high velocities, which is significantly lower than the 86% accuracy observed at moderate speeds. Nevertheless, the accuracy of PIN digit affirmation while moving quickly remains at approximately 90%, indicating resilience to fluctuations in touching velocity. The system effectively detects user physiological and behavioral attributes, attaining a 90% accuracy rate in confirming PIN digits, even in demanding conditions involving rapid finger movements.

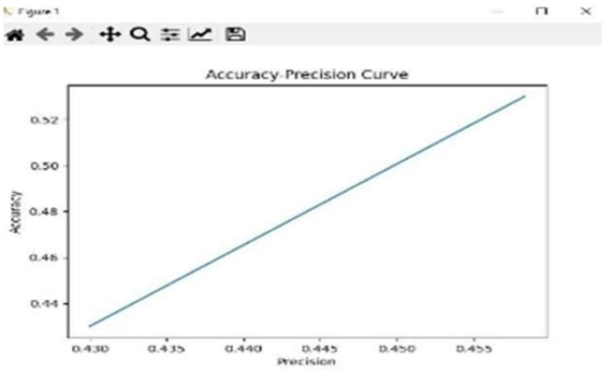

Fig. 6 Accuracy precision curve

Combining smartphone-generated bone-conducted vibrations for user identification, a camera module for visual authentication, and a vibration sensor for security alerts, the proposed door locking system incorporates all three components. The vibration analysis enables remote user validation of captured images while ensuring user authenticity. When unauthorized access attempts are detected, the vibration sensor generates an alert and transmits images of the intruder to the user's smartphone. By implementing this comprehensive strategy, security is fortified across multiple levels, preventing illicit entry and potential intrusions. Physical and digital security measures are seamlessly integrated into the system, which provides a robust solution for a variety of applications.

8. CONCLUSION

In summary, our groundbreaking endeavor, Source touch, introduces an innovative strategy for energy-efficient and economical physical user authentication that exceeds traditional touch screen methods. Source touch, a disruptive solution designed to enhance smart entry security in a variety of environments including vehicle entrances, apartment access points, and smart appliance compartments, leverages cost-effective physical vibrations to integrate physiological, behavioral, and passcode characteristics; surface dependence further strengthens security protocols. Source touch implements finger-input authentication on solid surfaces by utilizing a vibration-based contact sensing mechanism, thereby laying the groundwork for ubiquitous user authentication. By conducting thorough examination of vibration signals in the frequency domain and utilizing sophisticated methods such as cepstral coefficients and frequency response, Source touch is capable of attaining universal and unique user authentication. The system provides a flexible security framework for users, incorporating three distinct authentication modalities: fundamental gestures, PIN numbers, and lock patterns. Source touch offers a comprehensive solution for pervasive and secure access control in intelligent environments through its flexible and user-friendly deployment. An extra level of sophistication is introduced with the integration of a camera module designed to detect authorized individuals. This module can be effortlessly controlled through Telegram and facilitates the retrieval of real-time information and visual substantiation in the case of unauthorized access attempts. By virtue of this integration, the security framework as a whole is further fortified, thereby establishing Source touch as a potentially groundbreaking progression in the domain of tangible user authentication.

REFERENCES

[1] Liu, J., Wang, C., Chen, Y., & Saxena, N. (2017, October). VibWrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 73-87).

[2] Yang, X., Yang, S., Liu, J., Wang, C., Chen, Y., & Saxena, N. (2021). Enabling finger-touch-based mobile user authentication via physical vibrations on IoT devices. *IEEE Transactions on Mobile Computing*, *21*(10), 3565-3580.

[3] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge attacks on smartphone touch screens. In *4th USENIX workshop on offensive technologies (WOOT 10)*.

[4] Chin-Chung, C. (2002). LIBSVM: a library for support vector machines.*http://www. csie. ntu. edu. tw/~ cjlin/libsvm. html*.

[5] Chang, C. C., & Lin, C. J. (2011). LIBSVM: a library for support vector machines. *ACM transactions on intelligent systems and technology (TIST)*, *2*(3), 1-27.

[6] Arakala, A., Jeffers, J., & Horadam, K. J. (2007). Fuzzy extractors for minutiae-based fingerprint authentication. In *Advances in Biometrics: International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007. Proceedings* (pp. 760-769). Springer Berlin Heidelberg.

[7] Puth, M. T., Neuhäuser, M., & Ruxton, G. D. (2014). Effective use of Pearson's product–moment correlation coefficient. *Animal behaviour*, *93*, 183-189.

[8] Bartlett, R. F. (1993). Linear modelling of Pearson's product moment correlation coefficient: An application of Fisher's Z-transformation. *Journal of the Royal Statistical Society: Series D (The Statistician)*, *42*(1), 45-53.

[9] Schober, P., Boer, C., & Schwarte, L. A. (2018). Correlation coefficients: appropriate use and interpretation. *Anesthesia & analgesia*, *126*(5), 1763-1768.

[10] Chen, C. H., Tsai, W. Y., & Chao, W. H. (1996). The product- moment correlation coefficient and linear regression for truncated data. *Journal of the American Statistical Association*, *91*(435), 1181-1186.

[11] Obilor, E. I., & Amadi, E. C. (2018). Test for significance of Pearson’s correlation coefficient. *International Journal of Innovative Mathematics, Statistics & Energy Policies*, *6*(1), 11-23.

[12] Derrick, T. R., Bates, B. T., & Dufek, J. S. (1994). Evaluation of time-series data sets using the Pearson product-moment correlation coefficient. *Medicine and science in sports and exercise*, *26*(7), 919-928.

[13] Kendall, M. G. (1949). Rank and product-moment correlation. *Biometrika*, 177-193.

[14] Mohamad Sobri, N., Midi, P. D. H., Ibrahim, N. B., & Ismail, N. A. (2016). Differences between Pearson’s product moment correlation coefficient and an absolute value correlation coefficient in the presence of outliers. *Journal of Mathematics and Computing Science (JMCS)*, *1*(1), 1- 11.

[15] Symonds, P. M. (1926). Variations of the product-moment (Pearson) coefficient of correlation. *Journal of Educational Psychology*, *17*(7), 458.

[16] Chok, N. S. (2010). *Pearson's versus Spearman's and Kendall's correlation coefficients for continuous data* (Doctoral dissertation, University of Pittsburgh).

[17] Gayen, A. K. (1951). The frequency distribution of the product-moment correlation coefficient in random samples of any size drawn from non-normal universes. *Biometrika*, *38*(1/2), 219-247.

[18] Fieller, E. C., Hartley, H. O., & Pearson, E. S. (1957). Tests for rank correlation coefficients. I. *Biometrika*, *44*(3/4), 470-481.

[19] Quintero-Rincon, A., D'Giano, C., & Risk, M. (2020). Epileptic seizure prediction using Pearson's product-moment correlation coefficient of a linear classifier from generalized Gaussian modeling. *arXiv preprint arXiv:2006.01359*.

[20] M. L. Shuwandy, H. A. Aljubory, N. M. Hammash, M. M. Salih, M.A. Altaha and Z. T. Alqaisy (2022). BAWS3TS: Browsing Authentication Web- Based Smartphone Using 3D Touchscreen Sensor. 2022 *IEEE 18th International Colloquium on Signal Processing & Applications (CSPA), Selangor, Malaysia, pp.* 425-430.

AUTHORS:

D. Sai Revanth completed his Btech degree at the Department of Electronics and Communications Engineering, P.V.P Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India in 2024.

E-mail : dsrevanth7@gmail.com

M. Sai Subhash completed his Btech degree at the Department of Electronics and Communications Engineering, P.V.P Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India in 2024.

E-mail : saisubhashmandavalli@gmail.com

M. Kesav completed his Btech degree at the Department of Electronics and Communications Engineering, P.V.P Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India in 2024.

E-mail : madukesav@gmail.com

B. Harshith Reddy completed his Btech degree at the Department of Electronics and Communications Engineering, P.V.P Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India in 2024.

E-mail : harshithreddy7337@gmail.com