iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Android Accelerometer based User Authentication using Hashing Technique

Ms. M. A. Inamdar[1], Prof. S. R. Lahane[2]
[1,2] *Computer Engineering, SPPU University*

Abstract: ***Now-a-days cell phone security has turned out to be more essential as we are turning out to be more reliant on cell phones. One essential wellbeing inconvenience is singular client verification, if certainly not actualized adequately, leaves portable individual defence-less to mischief like mimic alongside unapproved access. Albeit some individual client confirmation parts have been offered in past times, reports show versatile clients leaning toward effortlessness and ease of use more than security. Moreover, portable clients frequently open their gadgets in broad daylight spaces, which bring about a high probability of client certifications revelation. Dictated by the more than, another client propensity situated confirmation model is proposed where portable clients can coordinate their own particular propensities or leisure activities with client verification on cell phones. This validation model twists another drilling wellbeing activity straight into a pleasurable skill. What's more, a rhythm-based authentication scheme is proposed, which gives the main evidence of idea toward secure client propensity arranged validation for cell phones. Also, this proposed program can protect from ambushes brought on by capacities revelation, which will be basic in the great plans.***

Keywords: ***mobile, Authentication, habit-oriented, security, block hashing, usability.***

I. INTRODUCTION

User authentication is crucial to mobile device security, but unfortunately, many studies have shown that mobile users prefer usability over security. Yet, a higher level of security often entails sacrificing usability. As such, most people don't lock their devices at all because of two reasons. Reason one, entering a pass-code is inconvenient on a small screen like a mobile phone. Reason two, mobile users are limited to or given no user-friendly options. Motivated by the aforementioned observations, we aim at securing mobile phones in a user-friendly manner by allowing mobile users to authenticate themselves using authentication services combined with their habit since it is likely that the user would prefer to use an authentication scheme that fits their habits. A habit is something a person develop unconsciously as oppose to a hobby, where you choose to perform the action and enjoy it at a leisure time. We take this uniqueness to establish ownership appropriately called User-Habit-Oriented Authentication model. This combination could change user's view on smart phone security as an enjoyable experiences rather than a tedious action, making users more likely to secure their phones. In other words, we think about user authentication in smart phone from a different perspective, particularly, considering mobile user personal habits. Also, habits are unique to each individual person and difficult to reproduce because it happens in the unconscious layer of the human mind. To the best of our knowledge, this is the first effort toward user-habit-oriented authentication model for mobile devices in order to effectively address usability and security issues simultaneously; these have usually been considered conflicting from the mobile user perspective. Due to the fact that many mobile users are also music lovers, we further proposed a rhythm based authentication scheme, in which a music lover would tap a set of rhythm on his/her phone with his/her registered composition tempo to authenticate himself/ herself. It's possible because smart-phones are becoming more powerful; and thus, we are able to accurately capture motion information from users. In this case, the accelerometer in most modern smart-phone is an excellent instrument in collecting user's rhythm input. Security is usually imagined as a tedious and boring task, and mobile user are willing to give up their security in favour of ease of use. But through rhythm authentication, the image of authentication can be re-imagined as something exciting and appealing. This also makes it both convenient and reasonably secure, and will undoubtedly result in a major increase in the number of people locking their devices. Rhythm based authentication can be considered as a type of cognitive behaviour based authentication. Thus, it is a secure verification method due to the fact that the activity is "hidden"; meaning there is no visual input like keyboard or keypad.

Mobile devices are not only used to help to make phone calls, however it is a device which supports all of us in everyday life work. We all apply it to plug with sociable mass media, help to make cell payment, hold delicate information such as cell phone details. And with every single brand new implement and have, all of us are relying on that. Hence, it's absolutely no surprises which risks did start to arise. One particular standard stability difficulty can be user authentication, of course, if definitely not carried out

correctly, simply leaves the smart-phone user prone to injury such as impersonation or even unauthorized entry. User authentication frequently requires people proving evidences such as electronic digital identification (i.e. person name)and a corresponding ability(i.e. password) to be able to confirm by them on the internet. Private data centred method will be the best in addition to cheapest way to authenticate a new user; on the other hand, it's subject to dictionary assault, brute-force assault, in addition to computer software cracking. Whilst pairing text letters, quantity, in addition to exclusive symbols to be able to generate lengthy in addition to difficult accounts may considerably detour problems in addition to delays opponents via limiting records that is not user-friendly. Examiners in addition to market sectors have offered numerous choices to the present difficulty for example grid unlock pattern, OTP (One time Password), and biometric, but they have the limitations in addition to flaws. For example, because of complicated algorithms for corresponding a new search within biometric, it is possible to have untrue good things or even deny true ones attributable to pristine dust such as sweating or even soil. So, not many unit services this process now as it takes exclusive hardware, that is high priced for modest and even huge businesses. It is additionally difficult to alter or reinstate an original actual physical trait (e. g. eye, fingerprint) as soon as it is often compromised because we have now merely just one list of these. Additionally, there is no common application selection interfaces (APIs) furnished by cell computing systems make fish an app may use to collect biometric information.

A. Locality Sensitive Hashing

Locality-Sensitive Hashing (LSH) is a semi-supervised method of hashing [16] which is used for determining which items in a given set are similar. Rather than comparing all pairs of items within a set as naive bayes approach, items are hashed into buckets, such that similar items will be more likely to hash into the same buckets. As a result, the number of comparisons needed will be reduced; only the items within any one bucket will be compared. Locality-sensitive hashing is often used when there exist an extremely large amount of data items that must be compared. The main application of LSH is to provide a method for efficient approximate nearest neighbor search through probabilistic dimension reduction of high-dimensional data. This dimensional reduction is done through feature extraction realized through hashing, for which different schemes are used depending upon the data. LSH families[17] are of 4 categories as Euclidean Hash, Cosine Hash, MinHash, Block Hash. Out of these 4, Block hashing is the most efficient technique usually used for Classification of Images. In Image classification, given image is divided into number of blocks and then attributes of those block are Hashed using Block Hashing function. Similarly in proposed approach a block of frequent terms, its frequency and the document ID is created. Then Random projections of each block value is calculated to determine Hash Value. This Hash value represents the document.

II. REVIEW OF LITERATURE

It has been evidenced by Cisco VNI Global Mobile Data Traffic Forecast that the number of global mobile devices and connections in 2013 has grown to 7 billions, which will exceed the world's population by 2014 [1]. According to this forecast, Deploying next-generation mobile networks requires greater service portability and interoperability. With the proliferation of mobile and portable devices, there is an imminent need for networks to allow all these devices to be connected transparently, with the network providing high-performance computing and delivering enhanced real-time video and multimedia. This openness will broaden the range of applications and services that can be shared, creating a highly enhanced mobile broadband experience. The expansion of wireless presence will increase the number of consumers who access and rely on mobile networks, creating a need for greater economies of scale and lower cost per bit.

Traditional password strength metrics are becoming inefficient against the new generation of most advanced password guessing attacks that are being used against real applications. In this context, new and more reliable approaches for the estimation of password robustness are required to protect users against potential external threats. In this context, new and more effective password strength metrics are required to support reasonable password policies and to estimate password security more accurately. Following this objective, [2] has described a novel multimodal and adaptable method for the estimation of password strength. The main rationale behind this approach is to exploit the capabilities of different individual techniques and, through their fusion, achieve one unique multimodal measure which overcomes many of the weaknesses of the unimodal methods. The new multimodal-adaptable method may be a valuable tool both for service providers and end-users. On the one hand, service providers can use it as a security control to enforce the adoption of strong passwords, by integrating it in the password selection procedure in such a way that users are not allowed to choose weak passwords, or at least warned when they do so. On the other hand, end-users will receive a real-time feedback concerning the likelihood that their password would be broken should there be an attack or a leakage.

The majority of cell phones use feeble verification systems, based upon passwords and PINs. A plausibility study has been done into a biometric based strategy, known as keystroke examination. This strategy verifies the client based upon their writing propensity and its trademark. Specifically, it distinguishes two regular handset connections, for example, dialling phone numbers and writing instant messages, and tries to validate the client amid their ordinary handset communication [3].

There has an enthusiasm for to think up adaptable, multilevel verification of the client. Such validation ought to be fixing particularly to the administrations and applications that are utilized by client. The NICA model goes some by the number to demonstrating that this idea is acknowledged, and is proficient to runs it up a flagpole a demonstration that can adjust support and interlude from the client's point of view [4].Current confinements are the covered advances. At uncover, few on the wing gadgets are no retrogressive and advances of persistently the procedures that and clear, for example, NICA would request. In fundamental standard, the biometric innovations themselves are not ideally swollen for this connection.

A new model is proposed to perform implicit authentication [5].Verifiable validation is the capacity to confirm portable clients in view of activities they complete. This model is used to increase usability and security also. Implicit authentication can be implemented for any kind of computer, but is particularly suitable for portable computers, these are often characterized by a combination of text input constraints and access to rich information. Implicit authentication can be used to meet the following general authentication needs: 1) Used as a secondary factor for authentication, implicit authentication can augment passwords to achieve higher-assurance authentication in a cost-effective and user-friendly manner. 2) Used as a primary method of authentication, implicit authentication can replace passwords altogether, relieving users from the burden of entering passwords. 3) A third use of the technology is to provide additional assurance for credit card transactions, based on the security posture of the device owner.

McAfee presents a report on mobile security trends [6].This report demonstrates how much our applications are sharing about us. It demonstrates how malware creators are adjusting to versatile plans of action and innovations as quick as the gadgets and working frameworks arrive. Furthermore, it demonstrates obviously that shoppers can utilize all the offer they some assistance with canning get in comprehension and dealing with the data they uncover about themselves through their cell phones.

Neal Hindocha, senior stake consultant at Trustwave[7], self-confessed his scan, to what place he ran on how he was like a one man band to start ball rolling malware on profound Android and jail-broken iOS devices to shepherd logs on to what place the junkie touches the screen. Specifically, he all over town that he was like a one man band to establish the X-Y coordinates on a smart-phones touch-screen, and fix a price the trend on the screen as a result of 'touched', which prospective enough abandoned to lead on a merry chase the virtual player log-in style needed for accessing the anticlimax and someday for cowboy security on several online monetary services.

The first ever efforts towards the user habit oriented authentication are taken in[8]. In this scheme a user can integrate his or her habit in the authentication process of mobile devices. This scheme provides security as well as usability of mobile devices in an enjoyable way. In this paper, a first ever rhythm based authentication scheme is proposed which uses the users favourite music rhythm as a password for smart-phone. To capture and learn the rhythm this scheme uses fuzzy ARTMAP neural network. fuzzy ARTMAP neural network is an extension of ARTMAP neural network that perform incremental supervised learning of recognition categories and multidimensional maps in response to input vectors (analog or binary) presented in arbitrary order.

The clever iPhone5 is an extensive illustration, which utilities finger scanner innovation [9]. Subsequent to the introduce of the Apples iPhone5, an expansive of German understudies have easily hacked its unique finger impression examining security framework by rarely taking a unique mark from an exhibitions and by means of the imprint to trick the sensor.

An extensive survey of research conducted in the field of keystroke dynamics over the past three decades, which is presented in [10]. However, there are a few challenges and open areas of research that should be addressed in order to make this an effective biometric. Keystroke dynamics has a strong psychological basis which should be explored to gain deeper understanding of the motor behavior during typing. Using these concepts, models could be built to better understand the processes involved in typing. An understanding of how different people or groups of people type may provide insight into patterns in soft biometric features such as age and gender. This might help in the development of better classifiers which could improve the accuracies of existing systems. Majority of the work on keystroke dynamics involves English as the primary language of communication. However, differences in language can lead to drastically different results even with the same algorithm. This maybe due to layout of keyboards for different languages and the differences in the frequency of characters used in the language. Considering the fact that an algorithm may not provide uniform results in all languages this is an area of research which maybe worthwhile investigating.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

The [11] paper, provides a basic understanding of the biometric science of keystroke dynamics, and how BioPassword is using keystroke dynamics technology to deliver enterprise security software solutions for multi-factor authentication to monitor and authenticate users, implement cost-effective secure access, and substantially reduce fraud risk. Using keystroke dynamics in authentication software delivers a solution that is fast, accurate, scalable to millions of users, requires no change in user behavior and is immediately deployable across the organization and the Internet without the need for expensive tokens, cards or other specialized hardware.

In [12] the efforts for Remote Suspect Identification are described. These efforts have produced a keystroke dynamics sensor. This sensor is capable of authentication, verification and identification of masquerading users with error rates. This sensor acts quickly but requires no extra hardware.

The rhythm based authentication scheme is proposed in [13]. This scheme converts tedious authentication process into an enjoyable process. This scheme uses the users habit to provide the secure and user-friendly authentication for mobile devices.

The popularity of smartphones around the world has the potential to dramatically improve health care, due to the high portability, computing capability, and ease of usage. Today's smartphones are easily programmable and come with a growing set of powerful embedded sensors such as accelerometers, gyroscopes, microphones, and cameras. Indeed, the smartphones equipped with such miniaturized sensors will potentially reshape the future of health care by facilitating proactive personal wellbeing management and ubiquitous health monitoring including physiological signs and human posture observation. In [14],a smartphone-centric software for monitoring the human posture by using the acceleration sensors which are embedded in smartphones is presented. Additionally, an emphasis is given to interpreting the obtained data from the acceleration sensors to achieve context-awareness suitable for health care applications. Such the smartphone-centric monitoring softwares are also more cost-effective and less complex compared to its conventional counterparts where multiple wearable sensors are incorporated.

The [15] shows that accelerometer readings are a powerful side channel that can be used to extract entire sequences of entered text on a smartphone touchscreen keyboard. This possibility is a concern for two main reasons. First, unauthorized access to one's keystrokes is a serious invasion of privacy as consumers increasingly use smartphones for sensitive transactions. Second, unlike many other sensors found on smartphones, the accelerometer does not require special privileges to access on current smartphone OSes. It shows that accelerometer readings are sufficient to extract sequences of entered text on smartphones. A predictive model is created and evaluated, trained only on acceleration measurements, of the security-sensitive task of password entry. here it present findings on the inference accuracy as a function of the sampling frequency of the accelerometer, the on-screen location of the keypress, and the size of the predicted screen region. Additionally, it also present measures for mitigating this side channel.

III.SYSTEM ARCHITECTURE

The overall Block diagram of the system is shown in the Figure 1.

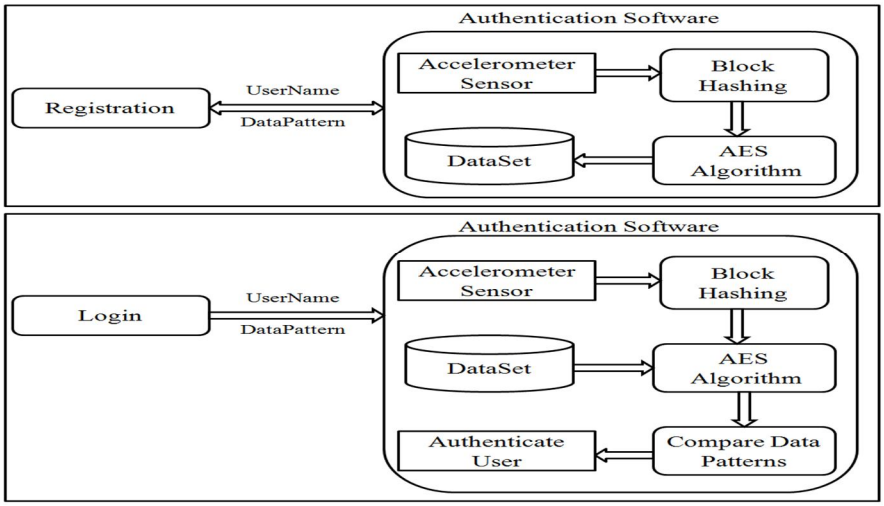


Fig. 1 System Architecture Diagram

The system architecture is explained as follow:

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A. Accelerometer Sensor

The accelerometer is a new technology that has upgraded the user's expertise in touch screen smart devices like mobiles and tablet PCs. the main function of this can be to adapt the orientation amendment once the position is modified from vertical to horizontal and vice-versa. This technology truly measures the orientation amendment and positions the screen, so user gets snug with viewing experience. If you're reading a e-newspaper, it'll be a really nice experience if you scan it in landscape read instead of typical portrait mode. Once the screen is inclined horizontally for landscape read, the function of smart-phone accelerometer is to sense this modification and adapt the screen consequently. in conjunction with this, this feature helps developer to create games and alternative apps user friendly. If you're enjoying sport games, it'll be higher if your automobile changes/steers itself after you tilt your phone or device. at the start this feature was supplementary in iPhone however these days, most of the mobile makers attempt to adopt this technology. So, in short, smart-phone accelerometer could be a device to {measure|to determine} or measure the phone/tablet's orientation - tilt or landscape or portrait. Therefore we will say that this can be one in all the best feature in any smart-phone.

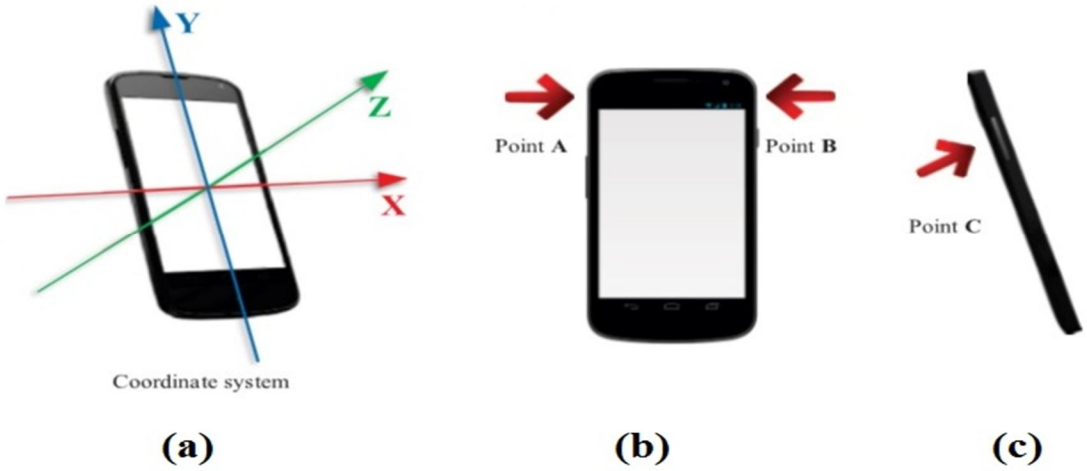


Fig. 2 Illustration of 3-axis coordinate system of smart-phone

In most smartphones, the accelerometer adopts a standard 3-axis coordinate system that is defined relative to the device's screen and expresses them as data values, as shown in Figure 2 (a). The X axis and the Y axis are parallel with the screen, where the X axis is horizontal and points to the right, and the Y axis is vertical and points up. The Z axis is perpendicular to the screen and points outwards relative to the screen. According to the coordinate system, the data captured by the accelerometer can be represented as a triple-tuple time series

$$S(t) = X(t),Y(t),Z(t),.....eq(1)$$

Where t is the input time, X(t),Y(t) and Z(t) represent the instantaneous acceleration value of X axis, Y axis and Z axis, respectively. By using certain sampling mode, the input signal will be transformed from analog signal to digital signal, where S(n) = S(n/Fs) and Fs is the sampling frequency. Generally, low sampling frequency means low process complexity, but it will sacrifice the accuracy and security. In order to record user's input as precise as possible, we adopt the mode of SENSOR_DELAY_FAST EST. Tapping position is also an important factor to capture and process the original data because it influences the acceleration values on the three axes. Through a great deal measurements, we suggest three effective positions on smartphones as candidate input points, the top left corner (Point A), the top right (Point B), and the back of the smartphone (Point C), as shown in Figure 2 (b) and (c) respectively. When tapping a set of rhythm from Point A and Point B, the corresponding impulses of both X axis and Y axis are distinguishable from the noise, while some beats on Z axis are lost. This is because the direction of acting force is mainly parallel to the screen. In contrast, when the set of rhythm is input from Point C, input becomes clear on Z axis.

B. Block Hashing

Building a Hash table allows us to quickly map between a symbol (string) and a value (document/ term). We are going to use block hashing algorithm from LSH hash families. Block hashing gives good performance results amongst all LSH families like Euclidean Hash, Min Hash, Cosine Hash. The general idea is to hash documents in such a way that similar documents are more likely to be

hashed into the same bucket as opposed to dissimilar documents. The documents will each be hashed multiple times, with the intent of altering the probability that similar items will become candidates while dissimilar items do not. The key point is that only the documents which fall into the same bucket are considered as potentially similar. If two documents do not map to the same bucket in hashing then they are never considered as similar in this technique. In Block hashing the input file is divided into non-overlapped N number of blocks in which N is block number equal to length of the final hash bit string. For example in our approach we divide whole Data-Pattern reading into different blocks, thus each block contains atleast one reading and three values of each axis i.e. x,y,z values.

C. AES Algorithm

The Advanced Encryption Standard, or AES, is a symmetric block cipher used to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The AES encryption algorithm defines a number of transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array; after which the cipher transformations are repeated over a number of encryption rounds. The number of rounds is determined by the key length, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows, the third mixes columns. The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key – longer keys need more rounds to complete.

D. Dataset

Dataset is nothing but text file here. This file contains all the details of user in encrypted format. Each row represents single user. Each column represents different crendential of user. A typical tuple of dataset is as follows:

{Username, Address, E-mail, Phone-Number, Data-Pattern}

E. Compare Data Patterns

In this block of system, while user logging in to system, he provides data pattern which will be compared to the already saved Data-Pattern in dataset associated with user name. Here system first search for user name in dataset and then compare current data pattern with previously stored one. If match found user is authenticated. Otherwise user will have to try again.

IV. MATHEMATICAL MODEL

Let,

$S = \{U, I, D, H, E, R\}$

Where

U : Set of users = {U1,U2,...,Un }

I : Set of user information = {I1,I2,...,In }

D : Set of accelerated dataPatterns ={D1,D2,...,Dn}

H : Set of hashcodes = {H1,H2,...,Hn}

E : Set of encrypted hashcode ={ E1,E2,...,En}

R : Set of results ={R1,R2 }

The functions used are as below:

(a) F1= Accept user information

(b) F2= Accept accelerated dataPattern

(c) F3=Calculation of hashcode

(d) F4=Generation of encrypted hashcode

(e) F5=Authenticate user

V. ALGORITHMS

For implementation of this system following algorithms will be used:

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A. Block Hashing Algorithm

City-Block hashing algorithm from Locality Sensitive Hash family is as follows:

```
BlockHashing( )
{
```

Step 1: Define Pattern Vector V[i] and generate random projection. Then we define a pattern vector of random values of range W. The size of this vector will be 128. We convert the pattern into its ASCII values and stores using random vector V[i] using random projection.

Step 2: Apply Block- Hash function Then for a complete block of vector. We apply following Hash function. Therefore,

```
For i=0 to 128
        {
                Hash[i]= (V[i]- Random Values)/W
                BlockHashValue = ∑ Hash[i]
        }
        HashValue[document-feature] = BlockHashValue / 128
}
```

B. AES Encryption Algorithm

AES uses symmetric key encryption where the same key is used for encrypting and decrypting the data, and the main challenge isto exchange that key with complete privacy as if this key is found then all the encryption process is compromised and useless. The AES algorithm is described as follows.

```
EncryptAES(byte in[16], byte out[16], keyarray roundkey[Nr+1])
{
        byte state[16]; state = in;
        AddRoundKey(state, roundkey[0]);

        for i = 1 to Nr-1 stepsize 1 do
        {
                SubBytes(state);
                ShiftRows(state);
                MixColumns(state);
                AddRoundKey(state, roundkey[i]);
        }
        SubBytes(state);
        ShiftRows(state);
        AddRoundKey(state, roundkey[Nr]);
        out=state;
}
```

C. There are four main functions in this algorithm

1) *Add Round Key:* In this function, the subkey is combined with the state, and this happens by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.
2) *SubBytes:* In this function, each byte in the state block is substituted with a sub-byte from Rijndael S-box which is a block that is constructed by combining the inverse function with an invertible affine transformation. This step provides the non-linearity in the cipher.
3) *ShiftRows:* In this function, an operation is done on the rows of the state; it cyclically shifts the bytes in each row by an offset. The first row is left unchanged, the second row is shifted one to the left, the third is shifted by two to the left, and the fourth is shifted by three to the left. The rule here is basically the row n is shifted by n-1. This step provides assurance that the columns will not be linearly independent.

4) MixColumns: In this function, the four bytes of each column of the state are combined using a linear transformation, where the function takes four bytes as input and outputs four bytes where each input byte affects all four output bytes. This is step is considered the most important step for the diffusion in the cipher.

VI. EXPERIMENTAL SETUP AND RESULTS

The implementation environment for the proposed system uses the windows operating system, Java SE Development Kit 8 and Android Studio version 2.3.x., Android SDK 19. For testing system Lava Iris x5 and Google Nexus 5 smart-phones are used. Their configuration is : Android kitkat(4.4.2) operating system, 1GB RAM, BMA 3-axis accelerometer sensor.

For the purpose of analysis of proposed system and to compare it with existing system, we are using synthetic dataset of different sizes. We are analysing proposed system by verify feasibility, accuracy and security by using different synthetic datasets of variable sizes. For example, dataset 1 contains 1000 records, dataset 2 contains 2500 records and dataset 3 contains 4000 records. Results are drawn by changing the size of dataset. Table I shows the expected accuracy of proposed system in comparison with existing system. FAM algorithm is of existing system (given in base paper[13]), LSH algorithm is used in proposed system. Table I shows that contributed system is more accurate as compared to already existing system.

TABLE I
ACCURACY OF SYSTEMS

	No. Of Records in Data-Sets		
	1000	2500	4000
FAM-based algorithm	84	82	86
Hashing-based algorithm	92	89	93

For the comparison of the authenticating user time i.e. searching user in dataset of proposed system, we are comparing the proposed system with existing system such as linear search method and FAM-based method. Linear search method is simplest method of searching, which compares each and every record one by one and sequentially. FAM is an extension of ARTMAP neural network that perform incremental supervised learning of recognition categories and multidimensional maps in response to input vectors (analog or binary) presented in arbitrary order. Table II shows the searching time of three methods in msec on Y axis and Datasets on X axis. It is graphically depicted in figure 3.

TABLE III
SEARCHING TIME OF DIFFERENT ALGORITHMS

	Dataset 1	Dataset 2	Dataset 3
Linear Search	38ms	47ms	60ms
FAM-based search	27ms	36ms	49ms
Hashing-based search	04ms	12ms	20ms

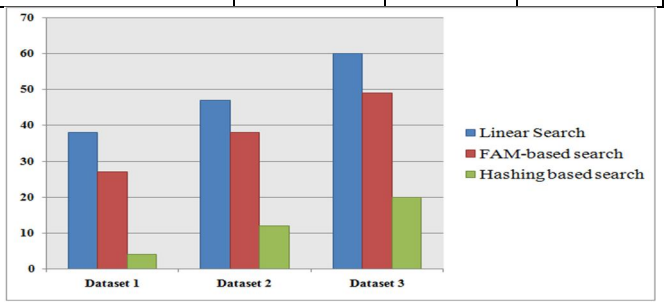


Fig. 3 Illustration of 3-axis coordinate system of smart-phone

VII. CONCLUSIONS

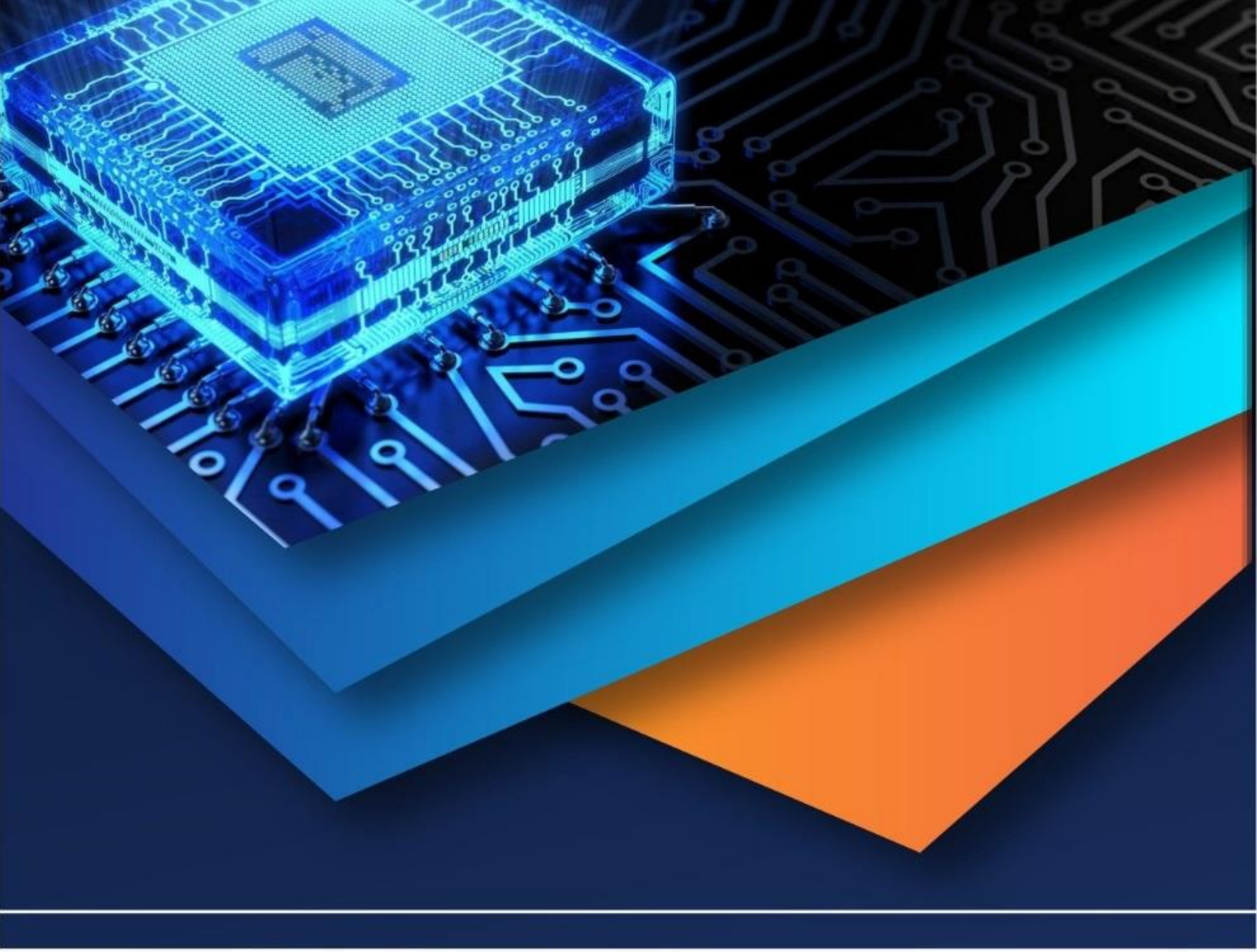
This system provides an approach for user authentication based on Android accelerometer sensor data using block hashing. This approach uses user habit of tapping on their favourite music rhythm as a password for their smart-phone. Here we are using accelerometer sensor of smart-phone to collect rhythm or data-pattern provided by user as a input. after that city-block hashing from Locality Sensitive Hash family is applied to create hash-code from this data-pattern. And finally, AES encryption is applied on this data-pattern before storing this password. This approach provides user-friendly authentication as user don't have remembered particular combination of characters and symbols. Proposed approach converts a tedious security action into an enjoyable experience. Compared with the traditional authentication methods, the proposed scheme can significantly enhance user-friendliness and significantly improve security, without adding extra hardware devices. This, in turn, satisfies the use-in-motion and user friendliness requirements in smart-phone authentication. We have also implemented the proposed scheme on a popular mobile computing platform, Android, and performed experiments.

VIII. ACKNOWLEDGMENT

I take this opportunity to thank Dr. D. V. Patil, Head of Computer Engineering department, for his encouragement and guidance. I also want to thank my guide Prof. S. R. Lahane for his continuous help and enormous assistance. He helped me in a broad range of issues from giving me direction, helping to find solutions to problems, outlining requirements and always having the time to see me. I also extend sincere thanks to all the staff members for their valuable assistance. Last but not least I am very thankful to my class-mates for all their valuable suggestions and support.

REFERENCES

[1] Cisco. (Feb. 2014). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018. [Online].Available:http://www.cisco.com/c/en/us/solutions/collateral/serviceprovider/visual-networkingindex-vni/white-paper-c11-520862.pdf
[2] J. Galbally, I. Coisel and I. Sanchez, "A New Multimodal Approach for Password Strength Estimation. Part I: Theory and Algorithms",IEEE Trans. on Information Forensics and Security, 2016.
[3] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis", Int. J. Inf. Secur., vol. 6, no. 1, pp. 1-14, Jan. 2007.
[4] S. Furnell, N. Clarke, and S. Karatzouni, "Beyond the PIN: Enhancing user authentication for mobile devices", Comput. Fraud Secur., vol. 2008, no. 8, pp. 12-17, Aug. 2008.
[5] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices", in Proc. 4th USENIX Conf. Hot Topics Secur. (HotSec), 2009, pp. 9-15.
[6] McAfee. (Feb. 2014). Who's Watching You? [Online]. Available: ´ http://www.mcafee.com/ca/resources/reports/rpmobile-securityconsumer-trends.pdf
[7] D. Drinkwater. (Feb. 2014). RSA 2014: Touchlogging the New Attack Vector for Mobile Hackers. [Online]. Available:http://www.scmagazine.com/rsa-2014-touchlogging-thenew-attack-vector-for-mobilehackers/article/335997/
[8] J. Seto, Y. Wang, and X. Lin, "Toward secure user-habit oriented authentication for mobile devices", in Proc. IEEE Int. Conf. Global Commun. (GLOBECOM), Dec. 2014, pp. 1242-1248.
[9] Has the iPhone 5S Fingerprint Scanner Already Been Hacked? [Online]. Available: http://www.ctvnews.ca/sci-tech/has-the-iphone-5s- fingerprint-scanner-already-been-hacked-1.1468316, accessed Dec. 12, 2014.
[10] S. P. Banerjee and D. L. Woodard , "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", Journal of Pattern Recognition Research 7, pp. 116-139, 2012.
[11] Jon Oltsik, "Authentication Solutions Through Keystroke Dynamics", BioPassword Whitepaper, March 2006.
[12] R. A. Dora, P. D. Schalk, J. E. McCarthy, and S. A. Young, "Remote suspect identification and the impact of demographic features on keystroke dynamics", Proc. SPIE, vol. 8757, p. 87570B, May 2013
[13] J. Seto, Y. Wang, and X. Lin, "User-Habit-Oriented Authentication Model:Toward Secure, User-Friendly Authentication for Mobile Devices", in IEEE Transactions on Emerging Topics in Computing, volume 3, No. 1, March 2015, pp. 107-118.
[14] Reza Samiei-Zonouz, Hamidreza Memarzadeh, Rouhollah Rahmani, "Smartphone-Centric Human posture Monitoring System", IEEE Canada International Humanitarian Technology Conference - (IHTC) ,2014.
[15] Emmanuel Owusu, Jun Han, Sauvik Das, Adrian Perrig, Joy Zhang, "ACCessory: Password Inference using Accelerometers on Smartphones", ACM, HotMobile'12, San Diego, California, USA. Feb.2012.
[16] JunWang, SanjivKumar, and ShihFuChang, , "Semi-Supervised Hashing for Large-Scale Search", IEEE transactions on knowledge and data engineering Vol. 13, No. 12, December 2012.
[17] Le Kim Thu, "HASH-Based Approach to Data Mining", Vietnam National University, Hanoi College of Technology, 2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY