Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

Hybrid Encryption Technique with smartphone sensors with app and spacio Location for detection authentication System

Ms.Shital M.Gujarathi [#1] Prof. Vikas Nandgaonkar[2], Prof. Dhanashri Patil[3]

[1]*Department of Computer Engineering, NMIET Talegaon Dabhade,Pune,India*
[2]*Project Guide,Department of Computer Engineering, NMIET Talegaon Dabhade,Pune,India*
[3]*Seminar Guide,Department of Computer Engineering, NMIET Talegaon Dabhade,Pune,India*

Abstract —*At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information securities are major concerns for customers, merchants and banks specifically in the case of Card Not Present. Many web applications supply secondary authentication methods i.e., top secret question (or password recovery questions), to reset the account password when a user's login fails. Today's prevalence of smart phones has approved us new opportunity to observe and understand how the personal data collected by smart phone sensors and apps can help create modified secret questions without violating the users' privacy concerns. We present a new login method where users provide username, secrete location and secret keyword to login. We also use Secret-Question based Authentication system, called "Secret-QA" that creates a set of secret questions on basic of people's smart phone usage. If some of reason user forgot password or mistype password then user can't access his/her account. To get the access of account user have to answer the security question. Security question and answer are recorded at the time user registration. After long time it's difficult to remember the security answer. At the same time for hacker or malicious user it's easy to guise the password. To avoid these problems we propose system that can over all thread from existing system. In existing system User provide password recovery email id, mobile number at the time of registration. System user can reset his/her password by email, mobile. Third party authentication system generates set of secret questions created based on the data of user's daily activity. We evaluated the reliability and security by using true/false type secret questions. To provide the extra security to secret location and secret keyword will be dual encrypted with AES & blowfish algorithm. The ultimate objective of the research presented in this paper is to develop both AES and Blowfish to be low power, high throughput, real-time, reliable and extremely secure cryptography algorithm and in addition to making estimation of both AES and Blowfish more difficult seems impossible*

Keywords-*smart phone sensor, Geo-location, AES algorithm, blowfish algorithm, Annotation password*

I. INTRODUCTION

Android Security plays a major role in today's scenario. Android Security is a technology that provides access to information and computing resources from anywhere that a network is available. There is a need to secure the data stored on server. The main goal behind the design of encryption algorithm must be security against unauthorized attacks. However, for all Android applications, performance and cost of implementation are also major concerns. The security and performance of encryption algorithms must be balanced.

In this paper, encryption algorithms (AES, Blowfish) has been discussed to analyse the performance level of each algorithm.

Secondary Authentication can be categorized in 2 types.

1) When user forgets their password and wants to log in to their account by proving answer to the security Question.

2) When the users want to get access to the very secure form of information like banking then also he/she should provide answer to the Security Question.

Password recovery questions are widely used by many web Services as the secondary authentication method for resetting the account password when user forgets their primary credential. When User creates their account on usually used websites like Gmail, yahoo, msn etc. user have to choose questions from predetermined list of the Questions. All these are blank fillings. User can reset his account password by providing the correct answer to the security Question.

For the easiness of setting and memorizing the answers, most of the secret questions are blank-fillings and that are created based on the long-term remembrance of a user's personal history that may not change over months/years (e.g., "What's the model of your first car?"). So the research has revealed that such kind of blank-filling questions created upon the user's long-term personal history may lead to poor security and reliability as answers of such Questions can be guessed by the usage of social networking sites. The prevalence of smart phone has provided a source of the user's personal data related to the knowledge of his short-term history, i.e., the data collected by the smart phone sensors and apps can be used for creating the secret Questions. Short - term personal history (typically within one month) can be used. Short-term personal history is less likely exposed to a stranger or acquaintance, because the rapid changes of an event that a person has experienced within a short term will increase the resilience to guess attacks. This implies improved security for such secret questions.

Propose system present a Secret-Question based Authentication system, with the advantage of the data of smart phone sensors and apps without violating the user privacy. In this Authentication system questions are True/false for easier remembrance of user.
Hybrid Encryption Algorithm is a keyed, symmetric block cipher, designed in 2012. It is a combination of two known algorithms (Blowfish & AES 128) . Hybrid Encryption Algorithm takes the advantages of blowfish algorithm and Advanced Encryption-Standard (AES) algorithm makes it harder for any attacker to try to decrypt the cipher text

II.LITERATURE REVIEW

1. Paper Name: Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions
Author: Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan
Paper Publication: IEEE Transactions on Mobile Computing
Year:2016
Description:
Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account password when a user's login fails. However, the answers to many such secret questions can be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools (e.g., online social networks); moreover, a user may forget her/his answers long after creating the secret questions. Today's prevalence of smartphones has granted us new opportunities to observe and understand how the personal data collected by smartphone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. In this paper, we present a Secret-Question based Authentication system, called "Secret-QA", that creates a set of secret questions on basic of people's smartphone usage. We develop a prototype on Android smartphones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools; meanwhile, we observe the questions' reliability by asking participants to answer their own questions. Our experimental results reveal that the secret questions related to motion sensors, calendar, app installment, and part of legacy app usage history (e.g., phone calls) have the best memorability for users as well as the highest robustness to attacks.
Method:
DES algorithm is used for data encryption
Method Description: DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).
Advantage:
Encrypt data using DES algorithm
Disadvantage:
System does not provide that much any security to user data

2. Paper Name: When the Password Doesn't Work: Secondary Authentication for Websites
Author: Robert Reeder; Stuart Schechter
Paper Publication: IEEE Security & Privacy
Year: 2011, Volume: 9, Issue: 2
Description:
Nearly all websites that maintain user-specific accounts use passwords to verify that a user associate degree attempt} to access an account is, in fact, the account holder. However, websites should still be able to determine users United Nations agency can't offer their correct parole, as passwords could be lost, forgotten, or stolen. During this case, users would require a variety of secondary authentication to prove that they're United Nations agency they assert they're and regain account access.
Method:
Knowledge Based Secondary Authentication Mechanisms.
Transitive Secondary Authentication Mechanisms.
Method Description:
1. Knowledge Based Secondary Authentication Mechanisms.
Knowledge-based authentication systems are popular with websites and other service providers because they're relatively simple to implement and don't rely on external infrastructure, such as other systems or special hardware. If a user's infrastructure is working well enough to connect to a website, knowledge-based authentication can be used.

2. Transitive Secondary Authentication Mechanisms.
Transitive authentication systems "pass the buck" for au-thenticating users to a system or person that's hopefully better equipped to authenticate users than the website.

Advantages:
Easy to use
Disadvantages:
User need to pay for secondary authentication (email/SMS).

3. Paper name: Design of Smartphone based Authentication Protocol for Beacon Detection in Disaster System
Author: Jae-Pil Lee, Jae-Gwang Lee, Eun-su Mo, Jun-hyeon Lee, Ki-su Yoon, Jae-Kwang Lee
Paper publication: IEEE(ICEICT)
Year: 2016
Description:
Sensor network technology has received increasing interest recently. Sensing element network technology is to sense Associate in Nursing object or environmental data and collect, analyze and method necessary data so as to predict and forestall Disasters. Sensing element network technology consists of wireless communication and as a result of the lower computing capability and restricted power provides, security risk will increase. During this study, authentication protocol is meant to spot etch sensors by exploitation HIGHT writing rule within the good phone setting. And therefore the authentication record within the authentication server is inspected to supply solely traditional sensing element data to Disaster service users during this planned authentication protocol.
Method:
HIGHT algorithm is used for data encryption.
Method Description:
To protect Beacon sensor authentication information generated in Disaster areas and Disaster service data, the 64bits block ciphering algorithm, HIGHT (TTAS.KO-12.0040) is employed in this study. HIGHT was designed in consideration of low-power computing environment, using 6bits plain blocks and 128bits key as input to output 64bits cryptogram block.
Advantages:
64-bit block length and 128-bit key length
Same algorithm use for other application for data encryption
Disadvantages:
Complex system

4. Paper Name: Biometric authentication technique using smartphone sensor
Author: Asadullah Laghari; Waheed-ur-Rehman; Zulfiqar Ali Memon
Paper Publication: 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST)
Year: 2016
Description:
This paper presents a identity verification mechanism exploitation motion sensing element of good phone. The user needs to perform signature by moving his phone, the motion pattern is detected exploitation measuring instrument of the good phone. We've got used the ideas of signal matching for identification mechanism. Results depict that legitimate user will be known employing a bound level of error threshold.
Method:
CROSS CORRELATION OF SIGNATURE
Method Description:
Accelerometer of the Smartphone provides data obtained for all three axes separately. Therefore, data of each axis is to be matched with its corresponding axis in the template data. The data for each axis can be plotted as function of time.
Advantages:
This technique is more secure than traditional username password and similar kind of methods.
Disadvantages:
System is not reliable for daily usage use.

5. Paper Name: An HMM-based multi-sensor approach for continuous mobile authentication
Author: Aditi Roy; Tzipora Halevi; Nasir Memon
Paper Publication: IEEE Military Communications Conference
Year: 2015
Description:
This paper studies continuous authentication for bit interface primarily based mobile devices. A Hidden Andre Mark off Model (HMM) primarily based behavioral guide coaching approach is bestowed, that doesn't need coaching information from different subjects aside from the owner of the mobile device and might get updated with new information over time. The gesture patterns of the user area unit sculptured from multiple sensors - bit, measuring system and rotating mechanism information employing a continuous left-right HMM. The approach models the faucet and stroke patterns of a user since these area unit the fundamental and most often used interactions on a mobile device. to judge the effectiveness of the projected technique a replacement information set has been created from forty two users UN agency

interacted with off-the-rack applications on their good phones. Results show that the performance of the projected approach is promising and probably higher than different progressive approaches.

Method:
Hidden Markov Model

Method Description:
The authentication method is based on multi-sensor data recorded from the owner's touch interactions on his mobile device. HMM method is used in this paper.

Advantages:
CHAS framework is applicable in a variety of situations, both using only touch data as well as multi-sensor data, to execute continuous authentication based on natural touch interactions.

Disadvantages:
Power consumption of application is high

6. Paper Name: SIFT-based algorithm for fingerprint authentication on smartphone
Author: Masao Yamazaki; Dongju Li; Tsuyoshi Isshiki; Hiroaki Kunieda
Paper Publication: 6th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES)
Year: 2015
Description:
In this paper, we tend to specialize in model enlargement on registration so as to simply accept any tiny a part of the question finger for verification. The planned formula merges 2 totally different pictures for constant finger that have 2 trivialities or curvature changes in overlapped space with a minimum. The merge results are improved within the case of the proper matches by these. However, within the current planned formula, once the input is integrated by mistake, the influence of it continues to stay. To avoid this, the thresholds of the planned formula are strict.

Method:
Scale invariant Feature transform

Method Description:
SIFT features are generated after four major stages: Scale-
spase extrama detection, Keypoint localization, Orientation
assignment and the Keypoint descriptor.

Advantages:
SIFT descriptor is a classic approach, also the "original" inspiration for most of the descriptors proposed later.
It is more accurate than any other descriptors.
It is Rotation and scale invariant.

Disadvantages:
System contains many unstable and false key points.

III. PROBLEM STATMENT

To remember the tricky password is very inconvenient job, because it's a combination of alphanumeric and special symbol. If some of reason user forgot password or mistype password then user can't access his/her account. To get the access of account user have to answer the security question. Security question and answer are recorded at the time user registration. After long time it's difficult to remember the security answer. At the same time for hacker or malicious user it's easy to guise the password. To avoid these problems we propose system that can over all thread from existing system.
Encryption algorithm would not be of much use if it is very much secure but slow in performance
The blowfish algorithm is best as compare to other algorithms but it has not as much of security than the AES. To overcome these weaknesses, we use combinational model implementation which is AES with Blowfish algorithm

IV. EXISTING SYSTEM

Existing authentication methods depend mainly on blank-filling questions, because the lightweight questions are subject to the random guessing attacks, e.g., a 50% success rate for an attacker given a true-false question.

In existing system User provide password recovery email id, mobile number at the time of registration. System user can reset his/her password by email, mobile. Third party authentication system generates set of secret questions created based on the data of user's daily activity and short-term smart phone usage. Daily activity contain call logs, user visited location.

In Existing Symmetric techniques like DES, IDEA, Blowfish, RC4, RC5, RC2, Triple DES, and AES. DES algorithm use feistel system, the key size is 56bit. Due to small key size DES is insecure and has weaknesses. Triple DES which is an improvement to DES, the original DES algorithm was applied thrice to enhance the protection. But it was found to be

very slow. Blowfish algorithm runs earlier than other symmetric algorithms. The AES is recommended symmetrical based encryption standard by NIST.AES algorithm is the best encryption algorithm.

V.DISADVANTAGE OF EXISTING SYSTEM

- Need to remember combination of alphanumeric and special symbol string called as password.
- Change in spelling cause wrong answer. Need to remember exact spelling.
- System does not provide any security to user data.

VI.PROPOSE SYSTEM

We design a user authentication system where user register into system by providing name, mobile number, email id. User login with user name and secret location with secret keyword. If user forgets the secret location or secret keyword then user will answer set of secret questions created based on the data of user's daily activity and short-term smart phone usage. Feature selection will be applied to select question type by data collected from mobile sensors. We evaluated the reliability and security by using true/false type secret questions. These questions are easy to answer and no need to remember because those are on based on user personal life and events. Due to this application security will be enhance because only user knew the events and things he/she did recently. To provide the extra security to secret location and secret keyword will be dual encrypted with AES & blowfish algorithm. This new generated encrypted information will be use as encryption key of blowfish algorithm. With the help of blowfish algorithm encrypted keyword again get encrypt. If user failed to authenticate himself then current location will be fetched and system will capture image of user by using front camera and information will be send to users registered on email id or mobile number. If users personal activity data is not available for more than a month at that time user will be authenticated with its registered email id and mobile number and if authentication passed successfully then user will receive a reset password notification on his registered mail Id.

VII.ADVANTAGE OF PROPOSE SYSTEM

- No need to remember password for login.
- No need to remember question answer for long time.
- Terminate part of spelling mistakes.
- Secrete location and secret key word is encrypted by AES and blowfish.
- Propose system provide double security by dual encryption.
- The hybrid of AES and Blowfish algorithm has characteristics of both the algorithms and it makes the algorithm strong against vulnerabilities.
- This hybrid structure of enhanced AES and Blowfish provides more security by increasing the complexity
- It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement.

VIII.METHODOLOGIES AND ALGORITHM

1. Hybrid Encryption technique

AES-Blowfish algorithm

First we use two symmetric encryption algorithms AES and Blowfish. Combining these two algorithms, will increases the run time for encryption/decryption. The total time required for hybrid algorithms will be the addition of both the algorithm's run time (processing time). Blowfish requires less time as compared to others algorithms, Blowfish algorithm adds the additional time for processing but it will enhance the overall security.

AES

AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. AES performs following steps for encryption/decryption:

First step is to generate round keys, round keys are generated using Rijndael's key schedule.

- The plaintext is converted to 4 x 4 state matrix.
- Each byte of the state is combined with the round key using bitwise xor.

- This is followed by ten rounds. In each of the first nine rounds, it performs four steps.
- Byte substitution in which each byte of state is replaced with the byte of S-Box in case of encryption and with the
- byte of Inverse S-Box in case of decryption depending upon its value. Shift rows in which first row of state matrix remains unchanged, second row shifts by 1 bit to the left, third row
- shifts by 2 bits to the left and fourth row shifts by 3 bits to the left. In case of decryption, shifting is to the right. Mix Columns in which each byte is replaced by a value dependent on all 4 bytes in the column.
- Fourth step is Add Round Key in which each byte of the state is combined with the round key using bitwise xor.
- In last round, it performs three steps only, the mix columns step is not performed in last step.

BLOWFISH

Blowfish is a symmetric block cipher designed by Bruce Schneier in 1993. It is a variable length key, 64-bit block cipher. It uses a 32 to 448 bit key. It consists of two parts:

The expansion of the key: break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.

The encryption of the data: 64-bit input is denoted with an x, while the P-array is denoted with a Pi (where i is the iteration).

The input is a 64-bit data element, x.

- Divide x into two 32-bit halves: xL, xR.
- Then, for i = 1 to 16.
- xL = xL XOR Pi xR = F(xL) XOR xR
- Swap xL and xR
- After the sixteenth round, swap xL and xR again to undo the last swap
- Then, xR = xR XOR P17 and xL = xL XOR P18.
- Finally, recombine xL and xR to get the cipher text

2. Haversine algorithm to calculate the distance from target point to origin point

1. R is the radius of earth in meters.
   Lat_O = latitude of origin point, $Long_O$ = longitude of origin point
   Lat_T= latitude of target point, $Long_T$= longitude of target point
2. Difference in latitude = Lat_O-Lat_T
   Difference in longitude = $Long_O$ -$Long_T$
3. Φ =Difference in latitude in radians
   Λ =Difference in longitude in radians
   O= Lat_O in radians.
   T= Lat_T in radians.
4. A= sin(Φ/2) * sin(Φ/2) + cos(O) *cos(T)*sin(Λ/2)*sin(Λ/2)
5. B= min(1,sqrt(A))
   Distance = 2*R*B

3. K-nearest neighbors KNN algorithm:

1. Determine parameter K = number of nearest neighbors

2. Calculate the distance between the query-instance and all the training samples

3. Sort the distance and determine nearest neighbors based on the K-th minimum distance

4. Gather the category y of the nearest neighbors

5. Use simple majority of the category of nearest neighbors as the prediction value of the query instance

KNN psudocode

```
Classify (X, Y, x) // X: training data, Y: class labels of X, x: unknown sample
for i=1 to m do
Compute distance d(Xi, x)
end for
Compute set I containing indices for the k smallest distances d(Xi, x).
return majority label for {Yi where i E I}
```


VIII.SYSTEM ARCHITECTURE

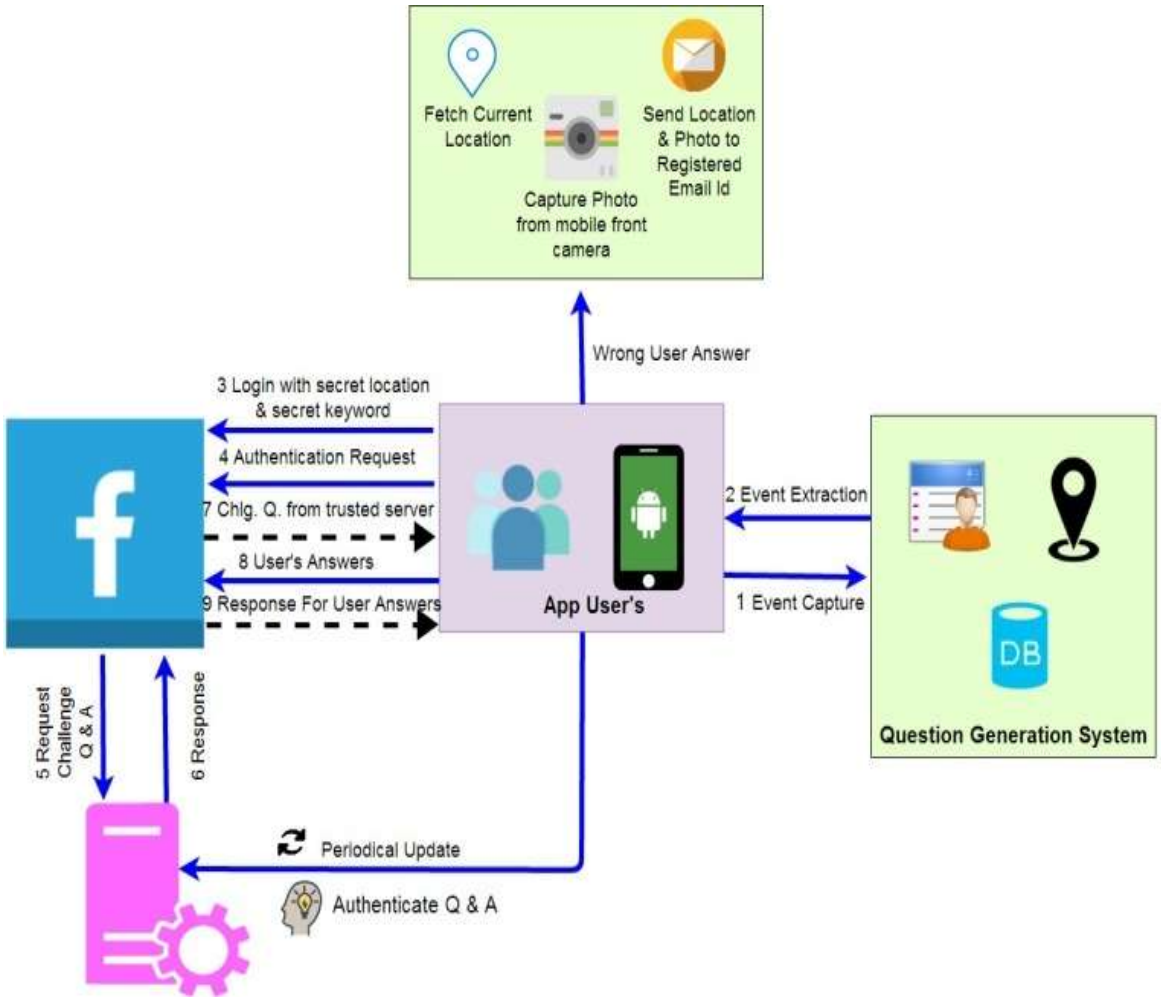

FIG.SYSTEM ARCHITECTURE

Application user performs daily activity. At background user event like location of user, call log history capture and store into database. Event extraction performs on this data. This data periodically updated into server. User will login to system with user name, secret location, and secret keyword. If user forget secret location or secret keyword then user request to reset password on dummy social networking site. This request sends to server. Server sends questions & answer into response.

IX. CONCLUSION

In propose system user login with user name, secret location and secret keyword. So no need to remember password for login. If user forget the secret location or secret keyword then propose system ask question to user which are basis on users personal life on the basis of short time period and recent activity. Question generated on the basis of data collected by smart phone sensor and app. Propose system ask secret questions without violating the users privacy. In propose system user no need to remember question answer for long time period. Those question answer based on user activity. User answers those questions. If given answers are correct then password will reset successfully. Evaluated the reliability and security by using true/false type secret questions. To provide the extra security to secret location and secret keyword will be dual encrypted with AES & blowfish algorithm. If user failed to authenticate himself then current location will be fetched and system will capture image of user by using front camera and information will be send to users registered on email id or mobile number.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

References

1.Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min "Jerry" Park, Xiaoming Li, Fan Ye, Wei Yan, Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions, pp.99, 2016.

2.R. Reeder and S. Schechter, When the password doesn't work: Secondary authentication for websites, S & P., IEEE, vol. 9, no. 2, pp. 43–49, March 2011.

3.H. Kim, J. Tang, and R. Anderson, Social authentication: harder than it looks, in Financial Cryptography and Data Security. Springer, 2012, pp. 1–15.

4.M. Oner, J. A. Pulcifer-Stump, P. Seeling, and T. Kaya, Towards the run and walk activity classification through step detection-an android application, in EMBC. IEEE, 2012, pp. 1980–1983.

5. S. Schechter, A. B. Brush, and S. Egelman, It's no secret. Measuring the security and reliability of authentication via secret questions,in S & P., IEEE. IEEE, 2009, pp. 375–390.

6.S. Hemminki, P. Nurmi, and S. Tarkoma, "Accelerometer-based transportation mode detection on smartphones," in Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems, ser. SenSys '13. New York, NY, USA: ACM, 2013, pp. 13:1–13:14. [Online]. Available: http://doi.acm.org/10.1145/2517351.2517367

7. M. Zviran and W. J. Haga, "User authentication by cognitive passwords: an empirical assessment," in Information Technology, 1990.'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on (Cat. No.90TH0326-9). IEEE, 1990, pp. 137–144.

8.N. Roy, H. Wang, and R. R. Choudhury, I am a smartphone and I can tell my user's walking direction, in Proc. ACM MobiSys, 2014, pp.329–342.

