Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/108010, December 2016*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Vehicle Intruder Alert System using Multi-Layered Authentication Technique

R. Padmanaban and J. Jennifer Ranjani*

School of Computing, Sastra University, Thanjavur - 613401, Tamil Nadu, India;
r.padmanaban27@gmail.com, jenny@cse.sastra.edu

Abstract

Objectives: In the recent past, vehicle theft is increasingly prevalent. The objective of the study is to propose a method to overcome the problem. **Methods:** In this paper, a technique is proposed that resolves the above mentioned problem. The primary purpose of the proposed scheme is to protect the vehicle from any unauthorized access using a cryptographic algorithm. **Findings:** The surety of the algorithm is achieved by combining cryptographic algorithm with a secret key. A randomly chosen binary template is used as a secret key which is then integrated with the input in order to generate the hash value using an MD5 hashing algorithm. This hash value is then compared with the stored hash value in order to operate the vehicle. In hashing algorithm, the hidden key is a data in which it is applied as an additional input to a one-way function that hashes a password. The principal use of the private key is to defend against dictionary attack and a rainbow table attack. **Improvements/Applications:** Thus, this technique achieves data confidentiality, data integrity, data privacy, authentication, and also is efficient in terms of processing time.

Keywords: Authentication, Cryptography, Hashing Algorithm, Intrusion Prevention

1. Introduction

The evolution of applied sciences made the automotive industry one of the biggest economic sectors and the latest modern vehicles come equipped with new degrees of functionality, safety, performance and comfort. Common automobile anti-theft systems are key/keyless entry system and engine immobilizers. Usually, thieves use low-tech approaches in order to steal cars, such as ruining the window, jimmying the lock, cutting alarm wires, hot wiring the ignition, or looking for keys left by the owner carelessly. Nevertheless, hackers are likely to sweep up the advanced attacks that are possible now as soon as it becomes cost efficient. Mechanism in car keys has evolved through various generations, from the effortless physical keys to more sophisticated keyless entry systems. The keyless entry system is commonly employed to avoid unauthorized substantial access to machines. It has a radio transmitter and should be in a range of about 5 to 20 meters of the automobile. When the button is pressed, it sends a coded signal to the receiver which is installed inside the car which is used to lock or unlock the door of an automobile. Various anti-theft systems have been developed over a few decades. The original intrusion detection signature combines the hash based appropriate signature with the hash function and contextual information. By the use of the hash functions, the work is to build an adaptive hash based non-critical alarm filter[1]. In this, the negative aspect is the speed of matching has to be improved and the non-critical alarms have to be reduced more efficiently. In[2], a scheme of protection of fingerprint template is proposed and it is based on the encryption process known as chaotic encryption and an algorithm called Murillo-Escobar's algorithm and also a secure authentication system based on 32-bit micro controller. A method that alleviates the vehicle security assessment issue and measures the power of the vehicle in order to defend against theft by testing the immobilizer locks and vehicle recognition is presented[3]. In[4], a unique and secure process of authentication of the biometric templates is presented. This technique ensures the safety of the biometric information. The key feature of this method is the session key generation. The generator is based on a chaotic phenomenon and

* *Author for correspondence*

it is composed from two generators known as Rossler map and a pseudo random bit generator. The weakness of this method is that, the algorithm encrypts only text and it can be further improved to handle video and images. This technique also collides in the hash space. In[5] stated a technique for personality based encryption system and eliminates key damage that might occur due to exposure. The cipher text in any time period is secure even after arbitrary compromises of the base and the user. Moreover, the burglar can't decrypt the cipher text having to do with previous time periods, yet if it compromises the base and the user at the same time[5]. In[6], a symmetric encryption mechanism for instantaneous text messaging in mobile devices is stated. This applies a succession of a prime numbers which is obtained from a secret key and a bi-dimensional matrix for the encoding process. This work focuses on reaching a trade-off between low complexity and robustness for instantaneous text messages in mobile technology communication. In[7], the authors stated that light weight cryptographic algorithms are suitable for applications like wireless sensor networks. It proposes a lightweight, one-way hash algorithm which makes a hash digest with fixed and relatively small length and applicable for securing energy-starved wireless network. In[8], the authors proposed approach which protects the fingerprint template. The primary idea of this method is to create the special spiral curves using any information from the extracted minutiae. In order to use the spiral curve for recognition process, the curves will be stored in the database. In[9], the generation of hash function is proposed which is based on a random Latin squares and is generated through padding, non-linear transformations and shift operations. In[10], the phase retrieval and RSA algorithms are used to provide a secret key. In this method, an encryption keys which includes the fingerprint as one input and the public key of the RSA algorithm as another input and also the decryption key consists of the private key of RSA algorithm and the fingerprint. The main limitation of this work is sharing of user's fingerprint which is used to authenticate with the receiver at once. If the user fingerprint and a public key are known by an attacker then the message can be easily decrypted. In[11], the work analyses the patterns and standards of the automobile industry, highlighting several vulnerabilities that stress needs to modify the way that the in-vehicle communication is handled. This system supports two features that users with different access rights and roles, and mutual authentication of ECUs (Electronic Control Unit). The keyless entry system broadcast on a frequency between 300 and 400 MHz's. However, it is easy to hack the frequency generated by the key fob. Hence, it is necessary to eliminate a frequency of the key fob. In[12], the work proposes a security mechanism for vehicle authentication for efficient and safe transmission of the communication between the vehicles. This method uses a time random numbers and encoded algorithm for mutual authentication between road side unit and on-board unit. The effect of environmental parameters on GSM and GPS has been proposed in[13] and it discuss about the variation in GSM signal strength with respect to the weather parameters. This paper addresses the following sections: Section 2 proposes a multi-layer authentication scheme which deals with an algorithm to generate a secret key and then it is integrated with a user input in order to operate the vehicle. Section 3 shows the implementation and results of the proposed work. Section 4 describe the conclusion.

2. Proposed Multi-Layer Authentication Scheme

The diagrammatic representation of the proposed work is shown in Figure 1 and Figure 2. Nowadays, it is possible to decipher a code or signal which is used for various applications. So it is significant to give security to the data in which we are using everywhere. The binary template which is a binary data is read as a secret key (SALT) and the four digit pin is read as another input to the MD5 hashing algorithm. After performing the MD5 hash function the generated hash value of the remote device is sent to the device which is installed in the car to lock or unlock the door wirelessly. By generating the hash value the device compares to the hash value which is already stored, if both the values are equal, and so the device leaves the door to move consequently.

This methodology consists of two modules. They are

- Transmitter Unit - Processing with inputs in order to generate MD5 hash value.
- Receiver Unit - Perform an operation accordingly by receiving a hash value.

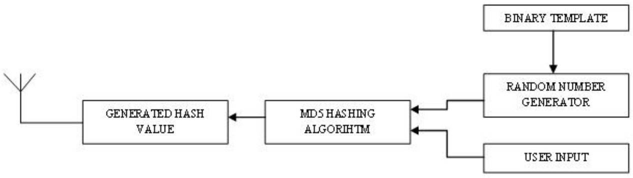


Figure 1. Diagrammatic representation of the transmission unit.

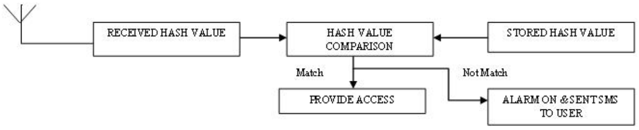


Figure 2. Diagrammatic representation of the receiving unit.

2.1 Transmitter Unit

2.1.1 Binary Template

In this step, the binary template is acquired for key generation. Then the template is stored in the memory which is allocated for storage. The template is a binary data which maps the binary value of each and every point and then it is used for key generation.

2.1.2 Random Number Generation Algorithm

In this section, the detailed description of a random number key generation algorithm is present. The design was driven by the binary templates in which the key is of 128 bytes in length. By getting the templates of the binary values which is stored in the memory, the value can be chosen randomly and is used as a secret key or SALT in hashing. The secret key depends on the mixture of both the token and the binary template. The token is the one which is applied to get the random values from the binary templates. The binary key 'k' has been generated first as a sequence of random bits. After then, it performs a logical operation with an input which is given by the user. Then the result is converted into hexadecimal value. Then the converted hexadecimal value is applied as an input to the MD5 hashing algorithm to get the hash value. Then each and every time it generates the different hash value for same or different input. Hence it is really difficult to identify which hash is for which input. Let us assume that the binary template is of mxn matrices' and is denoted by T.

m = No of Rows in the template

n = No of Columns in the template

$$T = \begin{bmatrix} x11 & x12 & x13 & \cdots & x1n \\ x21 & x22 & x23 & \ldots & x2n \\ x31 & x32 & x33 & \ldots & x3n \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ xm1 & xm2 & xm3 & \ldots & xmn \end{bmatrix} \quad (1)$$

Let 'a' be a randomly selected row and 'Xn' be the randomly generated column from the equation:

$$Xn+1 = (aXn + b) \bmod m \quad (2)$$

where a, b is an integer and m=m+n+1.

By taking the equation, the row and column of the template matrix are chosen in a random manner and then the row of a matrix is incremented until to get four values and it will get [1X4] matrix as one of the input of the private key. And so the operation is repeated for three times to draw another three a [1X4] matrix values which will be handled as a single [4X4] matrix randomly generated secret key input and is denoted by R (T).

$$R\,(T) = \begin{bmatrix} x21 & x13 & x54 & x22 \\ x31 & x23 & x14 & x32 \\ x41 & x33 & x24 & x42 \\ x51 & x43 & x34 & x52 \end{bmatrix} \quad (3)$$

Where a [0] = First column of R (T)
a [1] = Second column of R (T)
a [2] = Third column of R (T)
a [3] = Fourth column of R (T)

By considering the values provided by each column as binary values and then convert the values into decimal.

$$a[0] = [(x21 \text{ x } 1000) + (x31 \text{x } 100) + (x41 \text{x } 10) + (x51 \text{x } 1)] \quad (4)$$

Convert a [0] into Hexadecimal Value and then do the same for a [1], a [2], a[3]

$$D[R\,(T)] = a\,[3] \text{ x } 16^3 + a\,[2] \text{ x } 16^2 + a\,[1] \text{ x } 16^1 + a\,[0] \text{ x } 16^0 \quad (5)$$

Then,

$$H\,(K) = I \oplus D[R(T)] \quad (6)$$

Where H (K) = Hash Key
I = User Input
R (T) = Randomly Generated Secret Key

Then,

$$H\ (K1) = \text{Hex}\ \{H\ (K)\} \quad (7)$$

H (K1) = Hexadecimal Value of H (K)

Then the hashing algorithm computes the hash value based on a hash key.

$$\textbf{Hash} \Rightarrow \text{MD5}\textit{hash}\ \{H\ (K1)\} \quad (8)$$

2.1.3 Hashing Algorithm

The hash function is applied to assure the reliability of the information which is stored. It is sometimes called as digest of a message. The function of a hashing algorithm generates the fixed size of a message digest for a given input. Then the message digest is treated as a mark of that message. The mathematical expression that produces a hash function is given as MD5 = $f(x)$. It is also known as a one way function and it is easy to compute MD5 from the message, but it is not possible to calculate the message using the value of MD5. It should be hard to discover two such messages that are having the same message digest.

$$f(x1) \neq f(x2)$$

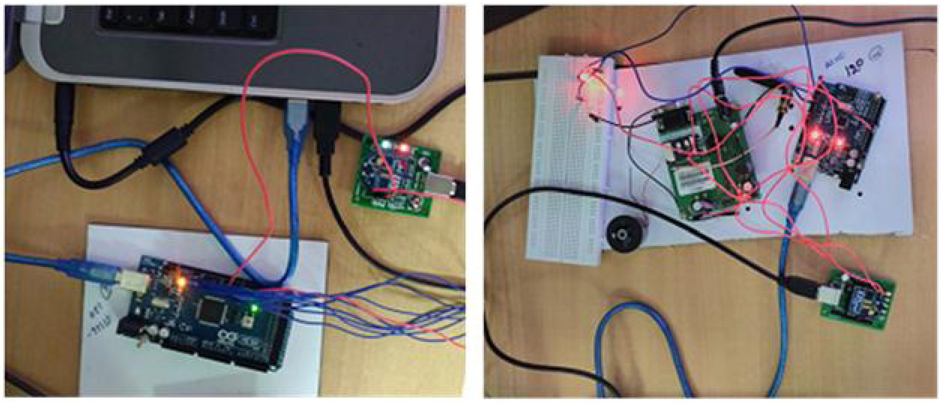
There are a lot of algorithms intended to execute the hash function such as MD2, MD4, MD5, SHA0, SHA1 and SHA2. After this, many researchers have also provided their own algorithms for the same such as SHA192.The MD5 hashing algorithm provides a 32 bit hexadecimal value as an output and it is a non reversible process because it performs a modulus operation. It is a long process to find the input by having the hash value. But it is somewhat possible to identify the input through the hash value using rainbow tables. It is a table that contains the known value of a hash function. So it is then compared with the whole table in order to find out the input. If the hash present in this table then it will be easy to find. If the hash value is not in the table, it is not possible to find the result. In order to resolve this rainbow tale problem, the only way is adding salt to the input value. Salting is process of generating the random data which is unique to the user. If we combine the input with the salt, it would provide a better security than the normal hashing function. Hash (Password + Salt).

2.2 Receiver Unit

By receiving the hash value from the transmitter, the device inside the car performs a comparison operation between the received hash value and the stored hash value. If both are the same values then only the door will get unlocked. Otherwise it will sound an alert and sent a message to the owner of the vehicle about the situation through GSM module.

3. Output and Result

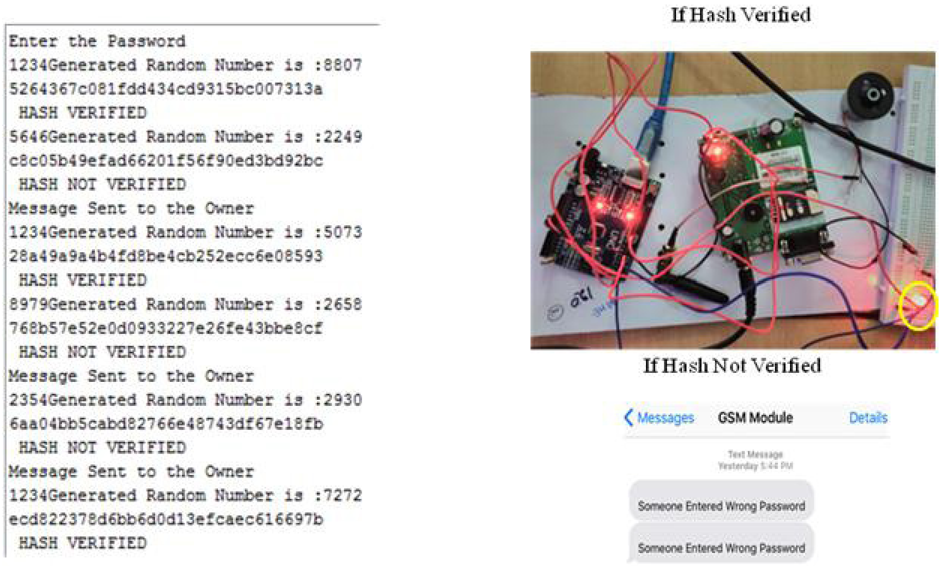
The implementation of the proposed method is done by using Arduino UNO board and a zigbee module. The experimental analysis of the generations of MD5 hash value with the inputs of randomly generated key and the user in put is transferred to the receiver in order to process an operation with respect to the locking of the door. As shown in Figure 3, the user input which is acquired from the 4x4 matrix keypad and then the secret key is derived



Transmitter Unit

Receiver Unit

Figure 3. Transmission unit and reception unit.



```
Enter the Password
1234Generated Random Number is :8807
5264367c081fdd434cd9315bc007313a
 HASH VERIFIED
5646Generated Random Number is :2249
c8c05b49efad66201f56f90ed3bd92bc
 HASH NOT VERIFIED
Message Sent to the Owner
1234Generated Random Number is :5073
28a49a9a4b4fd8be4cb252ecc6e08593
 HASH VERIFIED
8979Generated Random Number is :2658
768b57e52e0d0933227e26fe43bbe8cf
 HASH NOT VERIFIED
Message Sent to the Owner
2354Generated Random Number is :2930
6aa04bb5cabd82766e48743df67e18fb
 HASH NOT VERIFIED
Message Sent to the Owner
1234Generated Random Number is :7272
ecd822378d6bb6d0d13efcaec616697b
 HASH VERIFIED
```

If Hash Verified

If Hash Not Verified

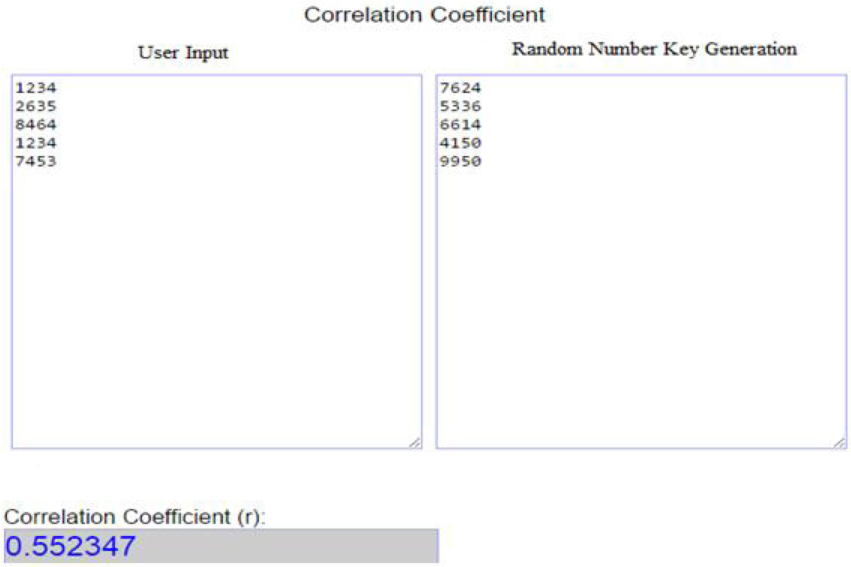
< Messages GSM Module Details

Text Message
Yesterday 5:44 PM

Someone Entered Wrong Password

Someone Entered Wrong Password

Figure 4. Output of the proposed work.



Correlation Coefficient

User Input

```
1234
2635
8464
1234
7453
```

Random Number Key Generation

```
7624
5336
6614
4150
9950
```

Correlation Coefficient (r):

0.552347

Figure 5. Correlation factor.

from the random number generation algorithm. Then the generation of hash value is transmitted to another Arduino board through a zigbee module1. The value is received using zigbee module2 and then it is processed accordingly in another Arduino UNO board in order to access the vehicle. Figure 4 shows that the vehicle is allowed to unlock the door only when we enter the correct pin otherwise it will send a message to the owner of the vehicle about the wrong pin which is entered to unlock the door. If we enter the correct pin, it will produce a hash value and then it is compared with the stored hash value. If both the values are same, the transmitter will send a signal to the receiver in order to operate the vehicle. If we enter a wrong pin, the generated hash of that particular pin will not match with the stored hash. So it will send a message to the owner of the vehicle about the issue. Figure 5 and Figure 6 shows the correlation coefficients and the scatter plots for the given inputs. The correlation coefficients for the given inputs are calculated and the value of *r* is 0.552 and then the scatter plots for the given

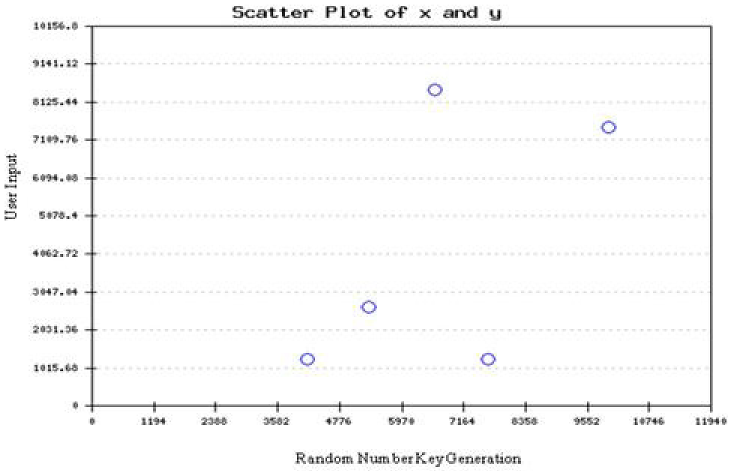


Figure 6. Scatter plot.

inputs are plotted. Table 1 shows that the generation of a hash value for a given input along with the random number key generation.

Table 1. Representation of hash value generated vs. input

Input	Random Key Generation	Generated Hash
1234	7624	ec5a9922acec4dad14377237d38fe193
2635	5336	276c2f2bff48d7930c717a6a01457c00
8464	6614	a414e9f523a5ac020356a8bb467c3397
1234	4150	f0599bef811233125c682ac5b1649150
7453	9950	c57d70034892e3efe871c12f022486ca

4. Conclusion

The proposed work secures the data from any unauthorized access with the help of a cryptographic algorithm and the security of the algorithm is achieved by combining cryptography with the secret key. The implementation is done by using Arduino UNO and the aim of this system is to permit the authentication of a user. It can also be used in a wide variety of applications. The security services provided by the system are data confidentiality and authentication. It is hard to find out the value of the input with the help of rainbow table attack and dictionary attack when compared with the existing method of hash function. The further work can be done by using a mobile application in order to control the vehicle and an algorithm which is used for mobile application has to be taken care in order to provide better security policies.

5. Acknowledgement

The authors wish to express their sincere thanks to the Department of Science and Technology, New Delhi, India (Project ID: SR/FST/ETI-371/2014).We also thank SASTRA University, Thanjavur, India for extending the infrastructural support to carry out this work.

6. References

1. Meng YK, Wok L. Adaptive non-critical alarm reduction using hash-based contextual signatures in intrusion detection. Computer Communications. 2014 Feb; 38:50-9.
2. Murillo-Escobar M, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez R. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. Expert Systems with Applications. 2015 Nov; 42(21):8198-211.
3. Mason S. Vehicle remote keyless entry systems and engine immobilisers: Do not believe the insurer that this technology is perfect. Computer Law and Security Review. 2012 Apr; 28(2):195-200.
4. Mihailescu M. New enrollment scheme for biometric template using hash chaos-based cryptography. Procedia Engineering. 2014 Mar; 69:1459-68.
5. Yu J, Hao R, Zhao H, Shu M, Fan J. IRIBE: Intrusion-Resilient Identity-Based Encryption. Information Sciences. 2016 Feb; 329:90-104.
6. Del Pozo Iturralde M. CI: A new encryption mechanism for instant messaging in mobile devices. Procedia Computer Science. 2015 Sep; 63:533-8.
7. Chowdhury A, Chatterjee T, Das Bit S. LOCHA: A light-weight one-way cryptographic hash algorithm for wireless

sensor network. Procedia Computer Science. 2014 Jun; 32:497-504.

8. Moujahdi C, Bebis G, Ghouzali S, Rziza M. Fingerprint shell: Secure representation of fingerprint template. Pattern Recognition Letters. 2014 Aug; 45:189-96.
9. Ghosh R, Verma S, Kumar R, Kumar S, Ram S. Design of hash algorithm using Latin square. Procedia Computer Science. 2015 Apr; 46:759-65.
10. Zhao T, Ran Q, Yuan L, Chi Y, Ma J. Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography. Optics and Lasers in Engineering. 2015 Sep; 72:12-7.
11. Patsakis C, Dellios K, Bouroche M. Towards distributed secure in-vehicle communication architecture for modern vehicles. Computers and Security. 2014 Feb; 40:60-74.
12. Kim Y, Song Y, Lee J. Vehicular authentication security mechanism modeling using Petri Net. Indian Journal of Science and Technology. 2015 Apr; 8(S7):443-7.
13. Dalip, Vijay Kumar. Effect of environmental parameters on GSM and GPS. Indian Journal of Science and Technology. 2014 Aug; 7(8):1183–8.