Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Geometric Authentication Mechanism of V/C Ratio Based on Road Geometrical Elements Using Iot Sensors

[1]A. Shivakrishna, [2]Dr. K.M. Lakshman Rao

[1]Research Scholar, Department of Civil Engineering, JNTU Hyderabad, Telangana

[2]Professor and Director of BICS, Department of Civil Engineering, JNTU Hyderabad, Telangana,

Abstract

In the Internet of things (IoT) environment, many applications access services through remote methods. In this paper, we designed a new geometric authentication mechanism to enhance security. The solution is based on geometric characteristics to achieve rapid authentication at low computational cost. In addition, we use the user's biometrics to improve the security level of the system. Our solution meets the following security features: anonymity, resistance to forgery attacks and replay attacks, fast error detection, resistance to offline password guessing attacks, resistance to server overload attacks, mutual authentication, session key agreement, and flexibility in users choosing and changing their passwords easily.

Keywords: *IoT Sensors, Neural Networks, Linear Regression, Machine Learning, Geometrical Elements*

1.0 Introduction

Wireless and mobile communication systems have become increasingly popular. Many service providers are beginning to propose convenient Internet of things (IoT) services and cloud applications for users [1-5]. People usually use mobile devices to access all kinds of services, e.g., web-browsing, remote monitoring, and multimedia applications anytime and anywhere [6]. Figure 1 shows an example where the user logs in to the IoT gateway (IGW) to access or control IoT devices remotely [7-10]. There is no doubt that an authentication mechanism is essential to protect valid users against different types of attacks. Remote user authentication schemes are the easiest and most practical authentication mechanisms for nonsecure networks [11-15].

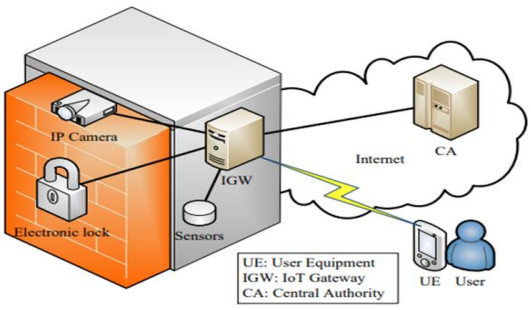

Figure 1: Remote access via gateway in IoT environment.

However, previous authentication schemes suffer from high computational cost and insufficient security. Some schemes use asymmetric cryptography, which results in high computational cost [16-18]. Most schemes use ID/password-based authentication, but the security robustness of these schemes is insufficient. Therefore, we

propose a new three-factor (i.e., smart device, biometrics, and password) remote user authentication scheme for improving the performance and enhancing security in the IoT environment in this paper The contributions of this paper are as follows.

- **Lightweight authentication:** The computational performance of our scheme is better than the traditional authentication schemes (e.g., asymmetric or symmetric encryption scheme) because our scheme uses only a hash function and arithmetic.
- **Three-factor authentication:** A higher-entropy password increases the difficulty in brute forcing it. Many papers have proven that the three-factor authentication scheme has better security (i.e., higher password entropy) and robustness.
- **Reduced IGW computing load:** Many authentication methods require full participation of the IGW. However, in an IoT environment, the number of IoT devices is large. Therefore, previous schemes are not suitable for use in an IoT environment because the IGW easily suffers from the single-point failure problem due to a distributed denial-of service (DDoS) attack. In our scheme, GAME supports the fast error detection process on the client side. If the user access is illegal, the smartphone immediately detects an error event and then rejects the login. In this way, the computational load of the IGW can be effectively reduced.

2.0 Materials and Methods

In this section, we describe our geometric authentication mechanism for enhancing security, called GAME, in an IoT environment. GAME is a lightweight authentication scheme. Moreover, we combine biometric technology and a password to enhance the level of security. The proposed geometric authentication mechanism involves four procedures: registration, login, authentication, and changing passwords. The notation used throughout this paper is listed in Table 1.

Table 1. Notation

Symbol	Description
BIO_i	Biometric information of user i
ID_i	The public identification of a user i
AID_i	The alias of user i
SID_j	The public identification of an IGW j
(x_0,y_0)	A secret point stored in the IoT gateway (IGW) and the central authority (CA)
r_i	A random number i
T	The current timestamp
$\oplus$	The bitwise XOR operator
$h(\,)$	A one-way collision-resistant hash function
$\|\,\|$	The combination of strings
PW_i	The password of user i
P	A large prime
SK_{ij}	The session key between i and j

3. Study Area

Vijayawada city, capital of Telangana state is chosen as the study area. The city of Vijayawada also serves as the central hub of transport and logistics within the state. Five mid-block sections and five signalized intersections were chosen to calculate the v/c ratio.

4. Field data collection

Different type of field data is collected to determine the v/c ratio for mid-block sections and signalized intersections chosen for the study. The type of data collected from the field are traffic volume using video-graphic method. The average speed of the traffic stream is collected using OHP sheet on wide-screen display for a trap

length of 30m. The number of lanes, effective green time of intersections etc., different road geometrics data such as width of the road, number of footpaths, are observed form the field.

5. Modelling the v/c ratio

Variable compression ratio (VCR) is a technology to adjust the compression ratio of an internal combustion engine while the engine is in operation. This is done to increase fuel efficiency while under varying loads. Variable compression engines allow the volume above the piston at top dead centre to be changed. Higher loads require lower ratios to increase power, while lower loads need higher ratios to increase efficiency, i.e. to lower fuel consumption. For automotive use this needs to be done as the engine is running in response to the load and driving demands. The 2019 Infiniti QX50 is the first commercially available vehicle that uses a variable compression ratio engine.

Advantages

Gasoline engines have a limit on the maximum pressure during the compression stroke, after which the fuel/air mixture detonates rather than burns. To achieve higher power outputs at the same speed, more fuel must be burned and therefore more air is needed. To achieve this, turbochargers or superchargers are used to increase the inlet pressure. This would result in detonation of the fuel/air mixture unless the compression ratio was decreased, i.e. the volume above the piston made greater. This can be done to a greater or lesser extent with massive increases in power being possible. The down side of this is that under light loading, the engine can lack power and torque. The solution is to be able to vary the inlet pressure and adjust the compression ratio to suit. This gives the best of both worlds, a small efficient engine capable of great power on demand. In addition, VCR allows free use of different fuels besides petrol e.g. LPG or ethanol .

Cylinder displacement is altered by using a hydraulic system connected to the crankshaft, and adjusted according to the load and acceleration required.

6. Results and Discussions

6.1 Multiple Linear regression (MLR) model

Multiple Linear Regression (MLR) model is developed to predict v/c ratio with respect to different road geometric parameters such as traffic volume (V), number of lanes (L), width of the Right of Way (W), number of foot paths (F), length of the road (L), speed (S), types of vehicles (M). The results of the MLR model developed is presented in Table 2.

Table 2: Results of the MLR model

Dependent variable: v/c ratio			
Independent variable	Coefficient	p-value	t-stat value
Intercept	0.29	0.00	2.97
V	0.00002	0.00	3.53
L	-0.009	0.00	4.83
W	0.012	0.00	2.55
F	-0.048	0.00	3.86
L	0.0038	0.001	2.11
S	-0.0030	0.001	2.22
M	0.035	0.00	3.88
R^2 value: 0.65			

The MLR developed in the study is used to predict the v/c ratio with respect to the road way geometric parameters such as traffic volume (V), number of lanes (L), width of the Right of Way (W), number of foot paths (F), length of the road (L), speed (S), types of vehicles (M). The regression statistics such as p-value and t-stat value indicates that all the independent variables have significant impact on v/c ratio. The change in each of these variables will reflect a considerable change in the v/c ratio values.

6.2. Artificial Neural Network (ANN) model

ANN comprises the input layer, the hidden layer for calculating input weights, and the output layer. ANN is developed in three steps: network training, selecting optimal network structure, and testing. ANN utilizes 70% of the data for training, 15% for testing, and 15% for validation. The number of hidden layers and neurons is decided based on the trial and method iterations. The network structure with less error between the measured and ANN modelled values is the optimal structure.

The present study also used the ANN technique to predict v/c ratio based on road network geometrics. Multi-layered feed-forward ANN is used by considering v/c ratio as the output layer in this study, and V, L, W, F, L, S and M as input layers. Different iterations were carried out by changing the number of hidden layers and neurons to obtain the optimal network structure. The network structure with less error between the measured and ANN modelled values is the optimal structure. The network structure for predicting the v/c ratio was optimized at two layers (one hidden layer and one output layer) and ten neurons. The output of the ANN model is presented in Figure 2.

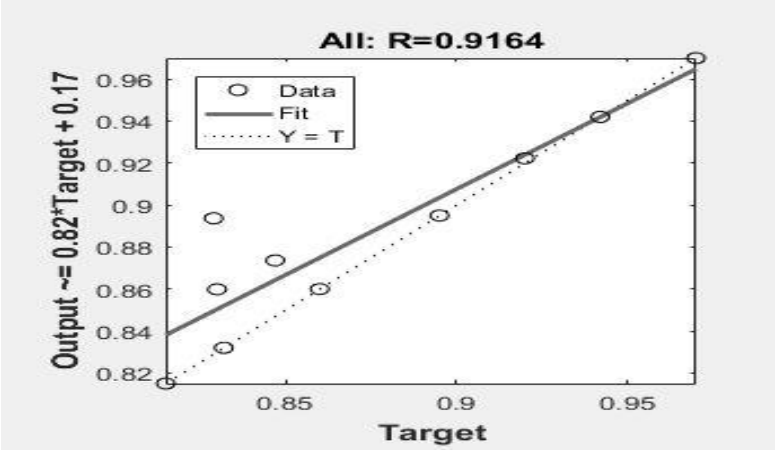

Figure 2: Output of ANN model

Conclusions

The study attempted to analyze the variation of v/c ratio with respect to the road way geometric parameters. Two different methods are used in the study such as Multiple Linear Regression (MLR) and Artificial Neural Networks (ANN) to develop models in order to predict the v/c ratio. Based on the R^2 value obtained in the models, it is observed that ANN has better prediction capability than MLR model. The analysis of variation of v/c ratio with respect road geometric variables is a novel approach. The study acts as a guide to the urban transportation planners to understand the change in v/c ratio when there is a change in road geometric variables.

DECLARATION

Conflict of interest:

The authors declare that this manuscript has no conflict of interest with any other published source and has not been published previously (partly or in full).

- No data have been fabricated or manipulated to support our conclusions.
- No funding is applicable and declaration for no financial Interest.

References

[1] Chuang, M.-C.; Chen, M.C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Syst. Appl. 2014, 41, 1411–1418.
[2] AL-Turjman, F.; Deebak, D.B. Seamless authentication: For IoT-big data technologies in smart industrial application systems. IEEE Trans. Ind. Inform. 2021, 17, 2919–2927.
[3] Wu, T.-C. Remote login authentication scheme based on a geometric approach. Comput. Commun. 1995, 18, 959–963.
[4] Hwang, M.-S. Cryptanalysis of a remote login authentication scheme. Comput. Commun. 1999, 22, 742–744.
[5] Chien, H.-Y.; Jan, J.-K.; Tseng, Y.-M. A modified remote login authentication scheme based on geometric approach. J. Syst. Softw. 2001, 55, 287–290.
[6] Chang, C.-C.; Lin, I.-C. Cryptanalysis of the modified remote login authentication scheme based on a geometric approach. Informatica 2005, 16, 37–44.
[7] Ku, W.-C.; Chang, S.-T.; Chen, H.-H.; Tsaur, M.-J. Weakness and simple improvement of a password authentication scheme based on geometric approach. In Proceedings of the IEEE Conference on Local Computer Networks (LCN), Sydney, Australia, 17 November 2005; pp. 472–473.
[8] Chuang, M.-C.; Lee, J.-F. An anonymous remote user authentication scheme based on a geometric approach for wireless networks. In Proceedings of the IEEE International Conference on Consumer Electronics, Communications and Networks (CECNet), Xianning, China, 16–18 April 2011; pp. 1015–1018.
[9] Lee, J.K.; Ryu, S.R.; Yoo, K.Y. Fingerprint-based remote user authentication scheme using smart cards. Electron. Lett. 2002, 38, 554–555.
[10] Ku, W.; Chang, S.; Chiang, M. Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. Electron. Lett. 2005, 41, 240–241.
[11] Chang, C.-C.; Lin, I.-C. Remarks on fingerprint-based remote user authentication scheme using smart cards. ACM SIGOPS Oper. Syst. Rev. 2004, 38, 91–96.
[12] Lin, C.-H.; Lai, Y.-Y. A flexible biometrics remote user authentication scheme. Comput. Stand. Interfaces 2004, 27, 19–23.
[13] Mitchell, C.J.; Tang, Q. Security of the Lin-Lai Smart Card Based User Authentication Scheme, Technical Report. 2005. Available online: http://www.rhul.ac.uk/mathematics/techreports (accessed on 1 May 2021).
[14] Fan, C.-I.; Lin, Y.-H. Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Trans. Inform. Forensics Secur. 2009, 4, 933–945.
[15] Khan, M.K.; Zhang, J. An efficient and practical fingerprint-based remote user authentication scheme with smart cards. In Springer Lecture Notes in Computer Science, Proceedings of the International Conference on Information Security Practice and Experience, Hangzhou, China, 11–14 April 2006; Springer: Berlin, Germany, 2006; pp. 260–268.
[16] Khan, M.K.; Zhang, J.; Wang, X. Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos Solitons Fractals 2008, 35, 519–524.
[17] Xu, J.; Zhu, W.; Feng, D. Improvement of a fingerprint-based remote user authentication scheme. In Proceedings of the IEEE International Conference on Information Security and Assurance (ISA), Busan, Korea, 24–26 April 2008; pp. 87–92.
[18] Li, C.-T.; Hwang, M.-S. An efficient biometrics-based remote user authentication scheme using smart cards. J. Netw. Comput. Appl. 2010, 33, 1–5.