A DECENTRALIZED MULTI-FACTOR USER AUTHENTICATION SCHEME FOR THE INTERNET OF THINGS SYSTEM

IKENNA RENE CHIADIGHIKAOBI

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2024

Awang Had Salleh
Graduate School
of Arts And Sciences

Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

IKENNA RENE CHIADIGHIKAOBI

calon untuk Ijazah
(candidate for the degree of) **PhD**

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

"A DECENTRALIZED MULTI-FACTOR USER AUTHENTICATION SCHEME FOR THE INTERNET OF THINGS SYSTEM"

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : ***10 April 2024.***
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on:
10 April 2024.

Pengerusi Viva: *(Chairman for VIVA)*	**Assoc. Prof. Dr. Massudi Mahmuddin**	Tandatangan *(Signature)*
Pemeriksa Luar: *(External Examiner)*	**Assoc. Prof. Dr. Rayner Alfred**	Tandatangan *(Signature)*
Pemeriksa Dalam: *(Internal Examiner)*	**Assoc. Prof. Ts. Dr. Mohamad Fadli Zolkipli**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Assoc. Prof. Ts. Dr. Norliza Katuk**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Dr. Baharudin Osman**	Tandatangan *(Signature)*

Tarikh:
(Date) ***10 April 2024***

Permission to Use

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for the scholarly purpose may be granted by the supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without written permission. It is also understood that due recognition shall be given to me and Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Pengesahan pengguna adalah bahagian penting dalam komunikasi dalam persekitaran IoT. Data yang dijana dan disampaikan dalam persekitaran adalah penting untuk kebolehkendalian dan keselamatan, yang menjadikan pengesahan pengguna sebagai langkah keselamatan penting terhadap serangan. Keterbatasan peranti IoT telah membawa kepada cabaran kos pengiraan dan keperluan untuk skim pengesahan yang ringan. Penyelesaian sedia ada telah melaksanakan pengesahan pengguna berpusat, meninggalkannya dengan pengehadan serangan seperti penyamaran, serangan lelaki dalam tengah (MITM), serangan meneka kata laluan dan kos pengiraan yang tinggi. Oleh itu, kajian ini mencadangkan skim pengesahan pengguna berbilang faktor terdesentralisasi (iaitu, imej muka, ID peranti pengguna, dan pautan pengesahan e-mel). Algoritma penyulitan PRESENT yang dipertingkatkan dan algoritma Kriptografi Lengkung Eliptik telah disesuaikan untuk mencapai skim pengesahan ringan, satu keperluan bagi peranti kekangan sumber. Hasilnya menunjukkan bahawa PRESENT yang dipertingkatkan mengatasi PRESENT asal dari segi keselamatan dan kos pengiraan. Juga, ujian Mann-Whitney U secara statistik menunjukkan perbezaan yang ketara antara PRESENT asal dan dipertingkatkan. Kajian itu dinilai dengan BAN-Logic, ProVerif dan AVISPA, dan ia menunjukkan ia dilindungi daripada serangan yang diketahui seperti MITM, tekaan kata laluan, orang dalam keistimewaan, dan serangan penyamaran. Melalui analisis keselamatan dan prestasi (iaitu, kos pengiraan), kami membuat kesimpulan bahawa skim yang dicadangkan adalah lebih selamat daripada kemungkinan serangan dan memperoleh kos pengiraan yang lebih rendah untuk persekitaran IoT. Selain itu, aplikasi berasaskan Python telah dibangunkan untuk mengkaji skim yang dicadangkan dalam seni bina kehidupan sebenar di mana didapati penyelesaian itu berjaya mengesahkan pengguna yang dibenarkan dan menolak sebarang permintaan akses tanpa kebenaran dengan tahap perlindungan keselamatan yang mencukupi dan kos pengiraan yang boleh diterima, kerana ia mencapai kos pengiraan sebanyak 0.58% pada telefon pintar, 1.68% pada Raspberry PI dan 0.87% pada komputer riba. Kajian ini menunjukkan bahawa reka bentuk dan pendekatan pelaksanaan sesuatu skim pengesahan menentukan prestasi keselamatan dan kos pengiraan. Juga, pendekatan pengesahan muka seperti yang dibentangkan dalam kajian ini mencadangkan penyelesaian kepada akses tanpa kebenaran dalam persekitaran IoT sambil mengekalkan pendekatan yang ringan.

Kata Kunci: Pengesahan ringan, Algoritma penyulitan, Skema pengesahan, Berbilang faktor terdesentralisasi dan Rumah pintar.

Abstract

User authentication is an essential part of communication in an Internet of Things (IoT) environment. For example, it is necessary for a smart home to utilize user authentication as a security measure against various attacks. However, the limitations of IoT devices have led to computation cost challenges and the need for a lightweight authentication scheme. The existing solutions have implemented centralized user authentication, leaving it with the limitation of attacks such as impersonation, man-in-the-middle (MITM), password guessing attacks, and high computation costs. Hence, this study proposed a decentralized multi-factor (i.e., face image, user device ID, and e-mail authentication link) user authentication scheme. An enhanced PRESENT encryption and an Elliptic-Curve Cryptography algorithm were adapted to achieve a lightweight authentication scheme, a necessity of the resource-constraint devices. The result shows that the enhanced PRESENT outperformed the original, particularly in terms of the security and computation cost. Besides, the Mann-Whitney U test statistically shows a significant difference in security and computation cost between the two algorithms. When evaluated with BAN-Logic, ProVerif, and AVISPA, PRESENT is secured against known attacks such as MITM, password guessing, privilege insider, and impersonation attacks. Through the security and performance (i.e., computation cost) analyses, it is concluded that the proposed user authentication scheme is more secure against potential attacks and obtains lower computation costs for the IoT environment. Moreover, a Python-based application was developed to examine the proposed user authentication scheme in a real-life architecture where it was found that the solution can successfully authenticate authorized users and reject any unauthorized access request with an adequate security protection level and an acceptable computation cost. For example, the achievement of a computation cost of 0.58%, 1.68%, and 0.87% on a smartphone, Raspberry PI, and laptop, respectively. This study shows that an authentication scheme's design and implementation approach determine the security and computation cost performance. The approach of face authentication as presented in this study provides a solution to unauthorized access in an IoT environment while maintaining a lightweight approach. A theoretical contribution was made by designing a decentralized multi-factor user authentication scheme, which eliminated the security challenges and computation cost limitations faced by the existing schemes.

.

Keywords: Lightweight authentication, Encryption algorithm, Authentication scheme, Decentralized multi-factor, and Smart home.

Acknowledgment

I am grateful to the Almighty God, the Father of our Lord Jesus Christ, for His mercies, love, and provision in my Ph.D. journey. I am grateful to my supervisors, Associate Prof. Dr. Norliza Binti Katuk and Dr. Baharudin Bin Osman who provided invaluable mentoring, advice, and feedback. They have been invaluable in offering painstaking guidance and thorough direction throughout the study process. I pray to God to reward their efforts.

I am grateful for the FRGS research grant and the opportunity to be appointed as a graduate research assistant, which my supervisor Associate Prof. Dr. Norliza Binti Katuk made possible. The offer was a financial strength that made the Ph.D. possible.

I appreciate my family's sacrifices in bearing the brunt of my extended absence from home and their support in every aspect to make sure I finished the program. I appreciate REMGS and MailZip company for the opportunity given to me to pursue and accomplish my Ph.D. goal.

Finally, I want to express my gratitude to all of my family and friends who have supported me during the program. May God continue to bless them all.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

AES	Advanced Encryption Standard
BBF	Biometric-Based Factor
CCTV	Closed-Circuit Television
CSS	Cascading Style Sheets
CVC	Color Visual Cryptography
DES	Data Encryption Standard
DoS	Denial-of-Service
HMAC	hash-based message authentication code
IoT	Internet of Things
KBF	Knowledge-Based Factor
NFC	Nearest Frequency Communication
OBF	Ownership-Based Factor
OS	Operating System
OTP	One-Time Passwords
PCA	Principal Component Analysis
PI	Raspberry PI
RFID	Radio-Frequency Identification
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithms
TEA	Tiny Encryption Algorithm
WSNs	Wireless Sensor Networks

CHAPTER ONE

INTRODUCTION

1.1 Research Background

The Internet of Things (IoT) is a system of intercommunication, connection of devices, and sensors such as a smart home application. The development of smart home applications is through the combination of other technologies such as wireless sensor networks (WSNs), Bluetooth technology, radio-frequency identification (RFID), cloud services, and machine-to-machine interfaces (M2M) (Anaya et al., 2020; Mohamed et al., 2020). IoT is an emerging technology area focusing on the interconnectivity of things to users and vice versa (Ali, 2016). The IoT application is made up of sensors, devices, and appliances such as low-cost sensors, smart window shutters, smart door unlock, fire detectors, and LED lights (Amintoosi et al., 2022; Bahache et al., 2022; Kumar & Chouhan, 2021). The devices and entities communicate within the network and other external environments such as cloud servers. Sensors and devices are limited in communication, computational power, memory usage, and security (Banerjee et al., 2021; Chiadighikaobi et al., 2022; Kim et al., 2023; Naoui et al., 2019a). Based on the impact of the IoT technology, smart home applications have emerged as the world-leading technology powered by the implementation of IPv6, thus enabling every single device to have communication and network establishment ability.

Several scholars revealed that many application domains, such as homes, automotive, healthcare, logistics, and environmental monitoring, have evolved since the existence of IoT (Banerjee et al., 2021; Roman et al., 2013; Taher et al., 2021). An IoT environment

REFERENCES

Abdalla, P. A., & Varol, C. (2020). Testing IoT Security: The Case Study of an IP Camera. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, *June*. https://doi.org/10.1109/ISDFS49300.2020.9116392

Abdi Nasib Far, H., Bayat, M., Kumar Das, A., Fotouhi, M., Pournaghi, S. M., & Doostari, M. A. (2021). LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wireless Networks*, *27*(2), 1389–1412. https://doi.org/10.1007/s11276-020-02523-9

Abidalreda, M., & Alrammahi, M. (2014). *Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol Available Online at www.ijarcs.info Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol*. *February 2014*. https://doi.org/10.13140/RG.2.2.20993.97124

Adeli, M., Bagheri, N., & Meimani, H. R. (2021). On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 3075–3089. https://doi.org/10.1007/s12652-020-02465-2

Adhikari, S., & Ray, S. (2019). *Recent Trends in Communication, Computing, and Electronics* (Vol. 524). Springer Singapore. https://doi.org/10.1007/978-981-13-2685-1

Afifi, M. H., Member, S., Zhou, L., & Member, S. (2018). Dynamic Authentication Protocol Using Self-Powered Timers for Passive Internet of Things. *IEEE Internet of Things Journal*, *5*(4), 2927–2935.

Al-Assam, H., Sellahewa, H., & Jassim, S. (2010). Multi-factor biometrics for authentication: A false sense of security. *MM and Sec'10 - Proceedings of the 2010 ACM SIGMM Multimedia and Security Workshop*, *September*, 81–87. https://doi.org/10.1145/1854229.1854246

Al-Assam, H., Sellahewa, H., Jassim, S., Wang, D., Gu, Q., Cheng, H., Wang, P., Go, W., Lee, K., Kwak, J., Mahto, D., Yadav, D. K., Fissore, L., Kaltenmeier, A., Laface, P., Micca, G., Pieraccini, R., Rahman, M., Hossen, M., … Sahula, V. (2017). A Study and Comparison of Lightweight Cryptographic Algorithm. *Future Generation Computer Systems*, *5*(1), 1–6. https://doi.org/10.1016/j.future.2017.07.040

Albazar, H., Abdel-Wahab, A., Alshar'e, M., & Abualkishik, A. (2023). An Adaptive Two-Factor Authentication Scheme Based on the Usage of Schnorr Signcryption Algorithm. *Informatica*, *47*(5). https://doi.org/10.31449/inf.v47i5.4627

Ali, B. (2016). Internet of Things Based Smart Homes: Security Risk Assessment and Recommendations. *Master's Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden. Retrieved from http://www.diva-portal.org/smash/get/diva2:1032194/FULLTEXT02.pdf*

Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M., & Salah, K. (2019). A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, *2018-Novem*(November). https://doi.org/10.1109/AICCSA.2018.8612856

Almulhim, M., & Zaman, N. (2018). Paper presented at 2018 20th International Conference on Advanced Communication Technology, ICACT, South Korea, 481–487. https://doi.org/10.23919/ICACT.201 8.8323802

Al-saggaf, A. A., Sheltami, T., Alkhzaimi, H., & Ahmed, G. (2023). Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing. *Arabian Journal for Science and Engineering*, *48*(2), 2347–2357. https://doi.org/10.1007/s13369-022-07235-0

Alsahlani, A. Y. F., & Popa, A. (2020). Analyzing of LAM-CIoT: Lightweight Authentication Mechanism in Cloud-based IoT Environment. *2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020*, 1837–1844. https://doi.org/10.1109/SSCI47803.2020.9308139

Alsahlani, A. Y. F., & Popa, A. (2021). LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *Journal of Network and Computer Applications*, *192*. https://doi.org/10.1016/j.jnca.2021.103177

Althobaiti, M. M., & Mayhew, P. (2014). Security and usability of authenticating process of online banking: User experience study. *Proceedings - International Carnahan Conference on Security Technology*, *2014-Octob*(October). https://doi.org/10.1109/CCST.2014.6986978

Amin, R., & Biswas, G. P. (2015). Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment. *Wireless Personal Communications*, *84*(1), 439–462. https://doi.org/10.1007/s11277-015-2616-7

Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., & Chang, V. (2018). A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. *Future Generation Computer Systems*, *78*, 1005–1019. https://doi.org/10.1016/j.future.2016.12.028

Amintoosi, H., Nikooghadam, M., Kumari, S., Kumar, S., & Chen, C. (2021). TAMA : Three-Factor Authentication for Multi-server Architecture. *Human-Centric Computing and Information Sciences*, *11*, 1.

Amintoosi, H., Nikooghadam, M., Shojafar, M., Kumari, S., & Alazab, M. (2022). Slight: A lightweight authentication scheme for smart healthcare services. *Computers and Electrical Engineering*, *99*. https://doi.org/10.1016/j.compeleceng.2022.107803

Anaya, E., Patel, J., Shah, P., Shah, V., & Cheng, Y. (2020). A Performance Study on Cryptographic Algorithms for IoT Devices. *CODASPY 2020 - Proceedings of the 10th ACM Conference on Data and Application Security and Privacy*, 159–161. https://doi.org/10.1145/3374664.3379531

Arasan, A., Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, *22*. https://doi.org/10.1007/s10586-017-1181-0

Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. *Academic Journal of Nawroz University*, *10*(1), 7. https://doi.org/10.25007/ajnu.v10n1a998

Bahache, A. N., Chikouche, N., & Mezrag, F. (2022). Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *SN Computer Science*, *3*(5). https://doi.org/10.1007/s42979-022-01300-z

Bakkiam, D., & AL-Turjman, F. (2021). Lightweight privacy-aware secure authentication scheme for cyber-physical systems in the edge intelligence era. *Concurrency and Computation: Practice and Experience*. https://doi.org/10.1002/cpe.6510

Balakrishnan, S., Vasudavan, H., & Murugesan, R. K. (2018). Smart home technologies: A preliminary review. *ACM International Conference Proceeding Series*, 120–127. https://doi.org/10.1145/3301551.3301575

Banerjee, S., Odelu, V., Das, A. K., Chattopadhyay, S., & Park, Y. (2021). An efficient, anonymous and robust authentication scheme for smart home environments. *Sensors (Switzerland)*, *20*(4), 1–19. https://doi.org/10.3390/s20041215

Bao, S., Hathal, W., Cruickshank, H., Sun, Z., Asuquo, P., & Lei, A. (2018). A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters. *ICT Express*, *4*(4), 221–227. https://doi.org/10.1016/j.icte.2017.12.001

Barbierato, L., Estebsari, A., Pons, E., Pau, M., Salassa, F., Ghirardi, M., & Patti, E. (2019). A Distributed IoT Infrastructure to Test and Deploy Real-Time Demand Response in Smart Grids. *IEEE Internet of Things Journal*, *6*(1), 1136–1146. https://doi.org/10.1109/JIOT.2018.2867511

Battaglia, F., Iannizzotto, G., & Lo Bello, L. (2014). A biometric authentication system based on face recognition and rfid tags. *Mondo Digitale*, *13*(49), 340-346

Benssalah, M., Djeddou, M., & Drouiche, K. (2014). Security enhancement of the authenticated rfid security mechanism based on chaotic maps. *Security and Communication Networks, 7*(12), 2356–2372. https://doi.org/10.1002/sec.946

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., & Poschmann, A. (2007). *PRESENT : An Ultra-Lightweight Block Cipher*. 450–466.

Bouras, M. A., Xia, B., Abuassba, A. O., Ning, H., & Lu, Q. (2021). IoT-CCAC: a blockchain-based consortium capability access control approach for IoT. *PeerJ Computer Science*, *7*, 1–22. https://doi.org/10.7717/PEERJ-CS.455

Bromiley, M. (2019). *Passwords Are Making You Weak Bye Bye Passwords: New Ways to Authenticate A SANS Spotlight*. Retrieved from https://www.sans.org/white-papers/39075/

Burrows, M., Abadi, M., & Needham, R. (1999). A Logic of Authentication. *Digital Equipment Corporation and ROGER NEEDHAM*, *8*(1), 1–19. Retrieved from: http://citeseer.nj.nec.com/details/burrows90logic.html.

Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., & Vasilakos, A. V. (2018). An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Computers and Electrical Engineering*, *69*, 534–554. https://doi.org/10.1016/j.compeleceng.2017.08.003

Chandrakar, P., & Om, H. (2017). A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. *Computer Communications*, *110*, 26–34. https://doi.org/10.1016/j.comcom.2017.05.009

Chandu Thota, Revathi Sundarasekar, Gunasekaran Manogaran, Varatharajan R, P. M. K. (2018). *Centralized Fog Computing Security Platform for IoT and Cloud in Healthcare System*. Fog Computing: Breakthroughs in Research and Practice. https://doi.org/10.4018/978-1-5225-5649-7.ch018

Chaitra, B., Kiran, V.G., & Rai, C. (2017). A Survey on Various Lightweight Cryptographic Algorithms on FPGA. *IOSR Journal of Electronics and Communication Engineering*, *12*(01), 54–59. https://doi.org/10.9790/2834-1201025459

Chang, C. C., Wu, H. L., & Sun, C. Y. (2017). Notes on "Secure authentication scheme for IoT and cloud servers." *Pervasive and Mobile Computing*, *38*(100), 275–278. https://doi.org/10.1016/j.pmcj.2015.12.003

Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., & Vasilakos, A. V. (2018). Secure Biometric-Based Authentication Scheme Using Chebyshev Chaotic Map for Multi-Server Environment. *IEEE Transactions on Dependable and Secure Computing*, *15*(5), 824–839. https://doi.org/10.1109/TDSC.2016.2616876

Chaudhry, S. A. (2016). A secure biometric based multi-server authentication scheme for social multimedia networks. *Multimedia Tools and Applications*, *75*(20), 12705–12725. https://doi.org/10.1007/s11042-015-3194-0

Chaudhry, S. A., Mahmood, K., Naqvi, H., & Khan, M. K. (2015). An Improved and Secure Biometric Authentication Scheme for Telecare Medicine Information Systems Based on Elliptic Curve Cryptography. *Journal of Medical Systems*, *39*(11). https://doi.org/10.1007/s10916-015-0335-y

Chaudhry, S. A., Naqvi, H., & Khan, M. K. (2018). An enhanced lightweight anonymous biometric based authentication scheme for TMIS. *Multimedia Tools and Applications*, *77*(5), 5503–5524. https://doi.org/10.1007/s11042-017-4464-9

Cheikhrouhou, O., Koubâa, A., Boujelben, M., & Abid, M. (2010). A lightweight user authentication scheme for wireless sensor networks. *2010 ACS/IEEE International*

Conference on Computer Systems and Applications, AICCSA 2010. https://doi.org/10.1109/AICCSA.2010.5586995

Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a Secure Medical Data Sharing Scheme Based on Blockchain. *Journal of Medical Systems*, *44*(2). https://doi.org/10.1007/s10916-019-1468-1

Chiadighikaobi, I. R., Katuk, N., & Osman, B. (2022). DMUAS-IoT: A Decentralised Multi-Factor User Authentication Scheme for IoT Systems. *International Journal of Computing*, *21*(4), 424–434. https://doi.org/10.47839/ijc.21.4.2777

Chifor, B. C., Bica, I., Patriciu, V. V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems*, *86*, 740–749. https://doi.org/10.1016/j.future.2017.05.048

Dammak, M., Boudia, O. R. M., Messous, M. A., Senouci, S. M., & Gransart, C. (2019). Token-Based Lightweight Authentication to Secure IoT Networks. *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 1–4. https://doi.org/10.1109/ccnc.2019.8651825

Das, A. K., Bera, B., Wazid, M., Jamal, S. S., & Park, Y. (2021). On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure. *IEEE Access*, *9*, 71856–71867. https://doi.org/10.1109/ACCESS.2021.3079312

Das, S., & Namasudra, S. (2023). Lightweight and efficient privacy-preserving mutual authentication scheme to secure Internet of Things-based smart healthcare. *Transactions on Emerging Telecommunications Technologies*. https://doi.org/10.1002/ett.4716

Dai, L., Qi, P., Lu, H., Liu, X., Hua, D., & Guo, X. (2023). Image Enhancement Method in Underground Coal Mines Based on an Improved Particle Swarm Optimization Algorithm. Applied Sciences, 13(5), 3254. MDPI AG. Retrieved from http://dx.doi.org/10.3390/app13053254

De Santis, A., Flores, M., & Masucci, B. (2017). *One-Message Unilateral Entity Authentication Schemes*, presented at the Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 2017, pp. 1-6. https://doi.org/10.1145/3098954.3098982

Deebak, B. D., & Hwang, S. O. (2023). Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT. *Electronics (Switzerland)*, *12*(5). https://doi.org/10.3390/electronics12051250

Delac, K., Grgic, M., & Grgic, S. (2005). Independent comparative study of PCA, ICA, and LDA on the FERET data set. *International Journal of Imaging Systems and Technology*, *15*(5), 252–260. https://doi.org/10.1002/ima.20059

Dey, S., & Hossain, A. (2019). Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography. *IEEE Sensors Letters*, *3*(4), 1–4. https://doi.org/10.1109/LSENS.2019.2905020

Dhillon, P. K., & Kalra, S. (2017a). A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications*, *34*, 255–270. https://doi.org/10.1016/j.jisa.2017.01.003

Dhillon, P. K., & Kalra, S. (2017b). Secure multi-factor remote user authentication scheme for Internet of Things environments. *International Journal of Communication Systems*, *30*(16), 1–20. https://doi.org/10.1002/dac.3323

Dhillon, P. K., & Kalra, S. (2018). Multi-factor user authentication scheme for IoT-based healthcare services. *Journal of Reliable Intelligent Environments*, *4*(3), 141–160. https://doi.org/10.1007/s40860-018-0062-5

El Hadj Youssef, W., Abdelli, A., Dridi, F., & Machhout, M. (2020). Hardware implementation of secure lightweight cryptographic designs for IoT applications. *Security and Communication Networks*, *2020*. https://doi.org/10.1155/2020/8860598

Eldefrawy, M. H., Alghathbar, K., & Khan, M. K. (2011). OTP-based two-factor authentication using mobile phones. *Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011*, 327–331. https://doi.org/10.1109/ITNG.2011.64

Emerson, S., Choi, Y. K., Hwang, D. Y., Kim, K. S., & Kim, K. H. (2015). An OAuth based authentication mechanism for IoT networks. *International Conference on ICT Convergence 2015: Innovations Toward the IoT, 5G, and Smart Media Era, ICTC 2015*, 1072–1074. https://doi.org/10.1109/ICTC.2015.7354740

Enciso, L., Baez, R., Maldonado, A., Zelaya-Policarpo, E., & Quezada-Sarmiento, P. A. (2018). *E-Mail Client Multiplatform for the Transfer of Information Using the SMTP Java Protocol Without Access to a Browser* (pp. 1124–1130). https://doi.org/10.1007/978-3-319-77703-0_109

Fakroon, M., Alshahrani, M., Gebali, F., & Traore, I. (2020). Secure remote anonymous user authentication scheme for smart home environment. *Internet of Things (Netherlands)*, *9*, 100158. https://doi.org/10.1016/j.iot.2020.100158

Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2019). Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*(2), 317–348. https://doi.org/10.1007/s11235-019-00612-5

Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*(2), 317–348. https://doi.org/10.1007/s11235-019-00612-5

Feng, J., Xu, J., Deng, Y., & Gao, J. (2023). A Fechner multiscale local descriptor for face recognition. J Supercomput. https://doi.org/10.1007/s11227-023-05421-x

Galterio, M. G., Shavit, S. A., & Hayajneh, T. (2018). A review of facial biometrics security for smart devices. *Computers*, *7*(3). https://doi.org/10.3390/computers7030037

Gudivada, S., & Bors, A. (2012). Face recognition using ortho-diffusion bases. European Signal Processing Conference.

Ghani, A., Mansoor, K., Mehmood, S., Chaudhry, S. A., Rahman, A. U., & Najmus Saqib, M. (2019). Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key. *International Journal of Communication Systems*, *32*(16), 1–18. https://doi.org/10.1002/dac.4139

Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal of Intelligent Manufacturing*, *25*(2), 217–230. https://doi.org/10.1007/s10845-012-0669-y

Gopal, S., Kumar, B., & Kiran, V. (2015). Analysis and Applications of IOT using Raspberry Pi. *International Journal of Creative Research Thoughts (IJCRT)*, *4*(12), 2044–2051. Retrieved from http://ijrcct.org/index.php/ojs/article/view/1318

Gope, P., Amin, R., Hafizul Islam, S. K., Kumar, N., & Bhalla, V. K. (2018). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems*, *83*, 629–637. https://doi.org/10.1016/j.future.2017.06.023

Gope, P., & Sikdar, B. (2019). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. *IEEE Internet of Things Journal*, *6*(1), 580–589. https://doi.org/10.1109/JIOT.2018.2846299

Goyal, T. K., & Sahula, V. (2016). Lightweight security algorithm for low power IoT devices. *2016 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016*, *July 2018*, 1725–1729. https://doi.org/10.1109/ICACCI.2016.7732296

Griffin, P. H. (2015). Biometric Knowledge Extraction for Multi-factor Authentication and Key Exchange. *Procedia Computer Science*, *61*, 66–71. https://doi.org/10.1016/j.procs.2015.09.150

Groves, A., & Schulte, P. (2020). "Verizon," World Scientific Book Chapters, in: THE RACE FOR 5G SUPREMACY Why China Is Surging, Where Millennials Struggle,

& How America Can Prevail, chapter 9, pages 145-159, World Scientific Publishing Co. Pte. Ltd. Retrieved from https://ideas.repec.org/h/wsi/wschap/9789811218712_0009 .html

Gunawan, T. S., Gani, M. H. H., Rahman, F. D. A., & Kartiwi, M. (2017). Development of face recognition on raspberry pi for security enhancement of smart home system. *Indonesian Journal of Electrical Engineering and Informatics*, *5*(4), 317–325. https://doi.org/10.11591/ijeei.v5i4.361

Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, *149*, 29–42. https://doi.org/10.1016/j.comnet.2018.11.021

Gupta, U. (2015). Application of Multi Factor Authentication in Internet of Things Domain. *International Journal of Computer Applications*, *123*(1), 29–31. https://doi.org/10.5120/ijca2015905221

Harini, N., & Padmanabhan, T. R. (2016). 3C-Auth: A new scheme for enhancing security. *International Journal of Network Security*, *18*(1), 143–150.

Hassan, M. A., & Shukur, Z. (2021). A Secure Multi Factor User Authentication Framework for Electronic Payment System. *2021 3rd International Cyber Resilience Conference, CRC 2021*, *January*. https://doi.org/10.1109/CRC50527.2021.9392564

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, *8*(2), 141–184. https://doi.org/10.1007/s13389-017-0160-y

Hossain, M. J., Xu, C., Li, C., Mahmud, S. M. H., Zhang, X., & Li, W. (2021). ICAS: Two-factor identity-concealed authentication scheme for remote-servers. *Journal of*

Systems Architecture, *117*(July 2020), 102077. https://doi.org/10.1016/j.sysarc.2021.102077

Hu, P., Ning, H., Qiu, T., Xu, Y., Luo, X., & Sangaiah, A. K. (2018). A unified face identification and resolution scheme using cloud computing in Internet of Things. *Future Generation Computer Systems*, *81*, 582–592. https://doi.org/10.1016/j.future.2017.03.030

Hussain, K., Jhanjhi, N. Z., Rahman, H. M., Hussain, J., & Hasan Islam, M. (2021). Using a systematic framework to critically analyze proposed smart card based two factor authentication schemes. *Journal of King Saud University - Computer and Information Sciences*, *33*(4), 417–425. https://doi.org/10.1016/j.jksuci.2019.01.015

Ibharalu, F. T., Falowo, M. O., & Akinwale, A. T. (2017). Rsa Encryption Algorithm Augumented With Bit-Stuffing Technique For Data Security. *Journal of Natural Science, Engineering and Technology*, *6*(1), 19-34.

Ibrahim, D. R., Abdullah, R., Teh, J. S., & Alsalibi, B. (2019). Authentication for ID cards based on colour visual cryptography and facial recognition. *ACM International Conference Proceeding Series*, 164–167. https://doi.org/10.1145/3309074.3309077

Ibrokhimov, S., Hui, K. L., Abdulhakim Al-Absi, A., Lee, H. J., & Sain, M. (2019). Multi-Factor Authentication in Cyber Physical System: A State of Art Survey. *International Conference on Advanced Communication Technology, ICACT*, *2019-Febru*, 279–284. https://doi.org/10.23919/ICACT.2019.8701960

Imran, M. A., Mridha, M. F., & Rahman, M. M. (2017). A Lightweight One Time Pad (OTP) and Biometric based Secure Authentication Scheme for IoT Environment.

Journal of Telecommunication, Electronic and Computer Engineering ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. X No. X, *10*(10), 2180–1843.

Jadoon, A. K., Wang, L., Li, T., & Zia, M. A. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wireless Communications and Mobile Computing*, *2018*. https://doi.org/10.1155/2018/1640167

Jain, A. K., Sharma, R., & Sharma, A. (2018). A Review of Face Recognition System Using Raspberry Pi in the Field of IoT. *Kalpa Publications in Engineering, 2*, 7-14. https://doi.org/10.29007/1xq9

Jiang, Q., Zeadally, S., Ma, J., & He, D. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access*, *5*, 3376–3392. https://doi.org/10.1109/ACCESS.2017.2673239

Kakkad, V., Patel, M., & Shah, M. (2019). Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design*. https://doi.org/10.1007/s41939-019-00049-y

Kandar, S., Pal, S., & Dhara, B. C. (2021). A Biometric based Remote User Authentication Technique Using Smart Card in Multi-Server Environment. *Wireless Personal Communications*, *0123456789*. https://doi.org/10.1007/s11277-021-08501-4

Kang, D., Lee, H., Lee, Y., & Won, D. (2021). Lightweight user authentication scheme for roaming service in GLOMONET with privacy preserving. *PLoS ONE*, *16*(2 Febuary). https://doi.org/10.1371/journal.pone.0247441

Karimi, K., & Krit, S. (2019). Smart home-smartphone systems: Threats, security requirements and open research challenges. *Proceedings of 2019 International*

Conference of Computer Science and Renewable Energies, ICCSRE 2019, 1–5. https://doi.org/10.1109/ICCSRE.2019.8807756

Kaur, D., & Kumar, D. (2021). Cryptanalysis and improvement of a two-factor user authentication scheme for smart home. *Journal of Information Security and Applications*, *58*(February), 102787. https://doi.org/10.1016/j.jisa.2021.102787

Khalid, H., Hashim, S. J., Ahmad, S. M. S., Hashim, F., & Chaudhary, M. A. (2021). Selamat: A new secure and lightweight multi-factor authentication scheme for cross-platform industrial iot systems. *Sensors*, *21*(4), 1–32. https://doi.org/10.3390/s21041428

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), 2067–2087. https://doi.org/10.1007/s10586-020-03058-6

Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., Abbasi, I. A., & Khan, N. A. (2022). Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks. *IEEE Access*, *10*, 31273–31288. https://doi.org/10.1109/ACCESS.2022.3159686

Khan, S. H., Ali Akbar, M., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Pattern Recognition*, *48*(2), 458–472. https://doi.org/10.1016/j.patcog.2014.08.024

Khashan, O. A., Alamri, S., Alomoush, W., Alsmadi, M. K., Atawneh, S., & Mir, U. (2023). Blockchain-Based Decentralized Authentication Model for IoT-Based E-

Learning and Educational Environments. *Computers, Materials and Continua*, *75*(2), 3133–3158. https://doi.org/10.32604/cmc.2023.036217

Khemissa, H., & Tandjaoui, D. (2016). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Khemissa, H., Tandjaoui, D., & Bouzefrane, S. (2017). An ultra-lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10566 LNCS*, 49–62. https://doi.org/10.1007/978-3-319-67807-8_4

Kim, J. T. (2017). Analyses of secure authentication scheme for smart home system based on internet on things. *Proceedings of the 2017 IEEE International Conference on Applied System Innovation: Applied System Innovation for Modern Technology, ICASI 2017*, 335–336. https://doi.org/10.1109/ICASI.2017.7988420

Kim, K., Ryu, J., Lee, H., Lee, Y., & Won, D. (2023). Distributed and Federated Authentication Schemes Based on Updatable Smart Contracts. *Electronics (Switzerland)*, *12*(5). https://doi.org/10.3390/electronics12051217

Kim, K., Ryu, J., Lee, Y., & Won, D. (2023). An Improved Lightweight User Authentication Scheme for the Internet of Medical Things. *Sensors*, *23*(3). https://doi.org/10.3390/s23031122

Koteshwara, S., & Das, A. (2017). Comparative Study of Authenticated Encryption Targeting Lightweight IoT Applications. *IEEE Design and Test*, *34*(4), 26–33. https://doi.org/10.1109/MDAT.2017.2682234

Kou, L., Shi, Y., Zhang, L., Liu, D., & Yang, Q. (2019). A Lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT. *Computers, Materials & Continua*, *58*(2), 545–565. https://doi.org/10.32604/cmc.2019.03760

Kulkarni, S., Bagul, M., Dukare, A., & Gaikwad, P. A. (2017). *Face Recognition System Using IoT*. *6*(11), 1720–1723.

Kumar, A., & Om, H. (2018). An improved and secure multiserver authentication scheme based on biometrics and smartcard. *Digital Communications and Networks*, *4*(1), 27–38. https://doi.org/10.1016/j.dcan.2017.09.004

Khedgaonkar, R.S., Singh, K.R. (2023). Designing face resemblance technique using near set theory under varying facial features. Multimed Tools Appl 82, 33161–33182. https://doi.org/10.1007/s11042-023-14927-8

Kumar, P., & Chouhan, L. (2021). A secure authentication scheme for IoT application in smart home. *Peer-to-Peer Networking and Applications*, *14*(1), 420–438. https://doi.org/10.1007/s12083-020-00973-8

Kumar, R. M., & Krishnan, M. (2017). An Open Source Contact-Free Palm Vein Recognition System. *International Journal of Advances in Applied Sciences (IJAAS)*, *6*(4), 319–324.

Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Kumar, N. (2018). A secure authentication scheme based on elliptic curve cryptography for IoT and cloud

servers. *Journal of Supercomputing*, *74*(12), 6428–6453. https://doi.org/10.1007/s11227-017-2048-0

Lakshmipathi, N. (2021, January 2). IMDB Dataset. *Kaggle*. https://www.kaggle.com/datasets/lakshmi25npathi/imdb-dataset-of-50k-movie-reviews

Lee, C. I., & Chien, H. Y. (2015). An Elliptic Curve Cryptography-Based RFID Authentication Securing E-Health System. *International Journal of Distributed Sensor Networks*, *2015*. https://doi.org/10.1155/2015/642425

Lee, D. H., & Lee, I. Y. (2020). A lightweight authentication and key agreement schemes for IoT environments. *Sensors (Switzerland)*, *20*(18), 1–18. https://doi.org/10.3390/s20185350

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lee, J., Yu, S., Park, K., Park, Y., & Park, Y. (2019). Secure three-factor authentication protocol for multi-gateway IoT environments. *Sensors (Switzerland)*, *19*(10), 1–25. https://doi.org/10.3390/s19102358

Li, H., Hu, L., Chu, J., & Chi, L. (2017). *The maximum matching degree sifting algorithm for steganography pretreatment applied to IoT*. *2699*. https://doi.org/10.1007/s11042-017-5075-1

Li, Z., Li, J., Zhao, S., Chen, X., Feng, K., & Wang, W. (2022). A blockchain-based lightweight identity authentication scheme for the IEDs of security and stability

control system. *PLoS ONE*, *17*(3 March). https://doi.org/10.1371/journal.pone.0265937

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information (Switzerland)*, *7*(3). https://doi.org/10.3390/info7030044

Lin, W. H., Wu, B. H., & Huang, Q. H. (2018). A face-recognition approach based on secret sharing for user authentication in public-transportation security. *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, 1350–1353. https://doi.org/10.1109/ICASI.2018.8394545

Liou, J. C., Egan, G., Patel, J. K., & Bhashyam, S. (2011). A sophisticated RFID application on multi-factor authentication. *Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011*, 180–185. https://doi.org/10.1109/ITNG.2011.38

Liu, C. H., & Chung, Y. F. (2017). Secure user authentication scheme for wireless healthcare sensor networks. *Computers and Electrical Engineering*, *59*, 250–261. https://doi.org/10.1016/j.compeleceng.2016.01.002

Liu, W., Wang, X., & Peng, W. (2019). Secure Remote Multi-factor Authentication Scheme Based on Chaotic Map Zero-knowledge proof for Crowdsourcing Internet of Things. *IEEE Access*, *8*, 1–1. https://doi.org/10.1109/access.2019.2962912

Liu, W., Wang, X., & Peng, W. (2020). Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things. *IEEE Access*, *8*, 8754–8767. https://doi.org/10.1109/ACCESS.2019.2962912

Lu, Y., Li, L., Yang, X., & Yang, Y. (2015). Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. *PLoS ONE*, *10*(5), 1–13. https://doi.org/10.1371/journal.pone.0126323

Lucas, L., Loscos, C., & Remion, Y. (2013). Digital Cameras: Definitions and Principles. In *3D Video* (pp. 23–41). John Wiley & Sons, Inc. https://doi.org/10.1002/9781118761915.ch2

Luo, X., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C., & Tian, Z. (2020). A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access*, *8*, 67192–67204. https://doi.org/10.1109/ACCESS.2020.2978525

Lwamo, N. M. R., Zhu, L., Xu, C., Sharif, K., Liu, X., & Zhang, C. (2019). SUAA: A Secure User Authentication Scheme with Anonymity for the Single & Multi-server Environments. *Information Sciences*, *477*, 369–385. https://doi.org/10.1016/j.ins.2018.10.037

Mahmood, K., Ashraf Chaudhry, S., Naqvi, H., Shon, T., & Farooq Ahmad, H. (2016). A lightweight message authentication scheme for Smart Grid communications in power sector. *Computers and Electrical Engineering*, *52*(May), 114–124. https://doi.org/10.1016/j.compeleceng.2016.02.017

Mahmood, Z., & Ning, H. (2016). *LightWeight Two-level Session Key Management for End User Authentication in Internet of Things*. "2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, pp. 323-327. https://doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.78.

Mart, R., Toral-cruz, H., Parra-michel, J. R., & Garc, V. (2019). An Enhanced Lightweight IoT-based Authentication Scheme in Cloud Computing Circumstances. *Sensors*, 19, 2098. https://doi.org/10.3390/s19092098

Masud, M., Gaba, G. S., Choudhary, K., Hossain, M. S., Alhamid, M. F., & Muhammad, G. (2022). Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. *IEEE Internet of Things Journal*, *9*(4), 2649–2656. https://doi.org/10.1109/JIOT.2021.3080461

Mbarek, B., Ge, M., & Pitner, T. (2020). An Efficient Mutual Authentication Scheme for Internet of Things. *Internet of Things*, *9*, 100160. https://doi.org/10.1016/j.iot.2020.100160

Mbarek, B., Ge, M., & Pitner, T. (2021). Trust-Based Authentication for Smart Home Systems. *Wireless Personal Communications*, *117*(3), 2157–2172. https://doi.org/10.1007/s11277-020-07965-0

Mehta, G., Dutta, M. K., Burget, R., & Povoda, L. (2016). Biometric data security using Fractional Fourier Transform and chaotic theory. *2016 39th International Conference on Telecommunications and Signal Processing, TSP 2016*, 533–537. https://doi.org/10.1109/TSP.2016.7760937

Mihailescu, M. I., & Pirloaga, M. D. (2012). A new framework for biometric face recognition using visual cryptograpy. *23rd DAAAM International Symposium on Intelligent Manufacturing and Automation 2012*, *1*(1), 163–166.

Mir, O., van der Weide, T., & Lee, C. C. (2015). A Secure User Anonymity and Authentication Scheme Using AVISPA for Telecare Medical Information Systems. *Journal of Medical Systems*, *39*(9). https://doi.org/10.1007/s10916-015-0265-8

Mishra, D., Das, A. K., & Mukhopadhyay, S. (2014). A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Systems with Applications*, *41*(18), 8129–8143. https://doi.org/10.1016/j.eswa.2014.07.004

Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid cryptographic approach for internet of things applications: A review. *Journal of Information and Communication Technology*, *19*(3), 279–319. https://doi.org/10.32890/jict2020.19.3.1

Mohammedi, M., Omar, M., Aitabdelmalek, W., Mansouri, A., & Bouabdallah, A. (2018). Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems. *Proceedings of the 2018 13th International Symposium on Programming and Systems, ISPS 2018*, 1–6. https://doi.org/10.1109/ISPS.2018.8379017

Mohammedi, M., Omar, M., & Bouabdallah, A. (2018). Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments. *Journal of Ambient Intelligence and Humanized Computing*, *9*(5), 1527–1539. https://doi.org/10.1007/s12652-017-0574-5Manoj, R., Biradar, Y., Rekha, R., Raju, R., & Sharad, A. (2020). Smart Home Security System using Iot, Face Recognition and Raspberry Pi. *International Journal of Computer Applications*, *176*(13), 45–47. https://doi.org/10.5120/ijca2020920105

Mohanta, B. K., Sahoo, A., Patel, S., Panda, S. S., Jena, D., & Gountia, D. (2019). DecAuth: Decentralized Authentication Scheme for IoT Device Using Ethereum Blockchain. *IEEE Region 10 Annual International Conference,*

Proceedings/TENCON, *2019-Octob*, 558–563. https://doi.org/10.1109/TENCON.2019.8929720

Mwinuka, L. J., Agghey, A. Z., Kaijage, S. F., & Ndibwile, J. D. (2022). FakeAP Detector: An Android-based Client-side Application for Detecting Wi-Fi Hotspot Spoofing. *IEEE Access*, *10*, 1–1. https://doi.org/10.1109/access.2022.3146802

Naoui, S., Elhdhili, M. E., & Saidane, L. A. (2019a). Lightweight and Secure Password Based Smart Home Authentication Protocol: LSP-SHAP. *Journal of Network and Systems Management*, *27*(4), 1020–1042. https://doi.org/10.1007/s10922-019-09496-x

Naoui, S., Elhdhili, M. H., & Saidane, L. A. (2019b). Novel Smart Home Authentication Protocol LRP-SHAP. *IEEE Wireless Communications and Networking Conference, WCNC*, *2019-April*, 1–6. https://doi.org/10.1109/WCNC.2019.8885493

Naresh Boddeti, V. (2018). Secure face matching using fully homomorphic encryption. *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems, BTAS 2018*. https://doi.org/10.1109/BTAS.2018.8698601

Netflix. (2020). Netflix Prize data. *Kaggle Dataset*. Retrieved from https://www.kaggle.com/netflix-inc/netflix-prize-data?select=movie_titles.csv

Nikooghadam, M., Amintoosi, H., & Kumari, S. (2021). On the Security of "Secure and Lightweight Authentication with Key Agreement for Smart Wearable Systems." *Wireless Personal Communications*, *0123456789*. https://doi.org/10.1007/s11277-021-08430-2

Nikooghadam, M., Jahantigh, R., & Arshad, H. (2017). A lightweight authentication and key agreement protocol preserving user anonymity. *Multimedia Tools and Applications*, *76*(11), 13401–13423. https://doi.org/10.1007/s11042-016-3704-8

Novose, R., Meden, B., Emersic, Z., Struc, V., & Peter, P. (2017). Face recognition with Raspberry Pi for IoT Environments. *International Electrotechnical and Computer Science Conference ERK 2017*, *September*, 477–480.

Oliver, S. G., & Purusothaman, T. (2022). Lightweight and secure mutual authentication scheme for IoT devices using CoAP protocol. *Computer Systems Science and Engineering*, *41*(2), 767–780. https://doi.org/10.32604/csse.2022.020888

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., Koucheryavy, Y., Andreev, S., Ometov, A., Mäkitalo, N., Koucheryavy, Y., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Ostad-Sharif, A., Arshad, H., Nikooghadam, M., & Abbasinezhad-Mood, D. (2019). Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems*, *100*, 882–892. https://doi.org/10.1016/j.future.2019.04.019

Panagiotou, P., Sklavos, N., Darra, E., & Zaharakis, I. D. (2020). Cryptographic system for data applications, in the context of internet of things. *Microprocessors and Microsystems*, *72*, 102921. https://doi.org/10.1016/j.micpro.2019.102921

Park, Y. (2018). A Secure User Authentication Scheme with Biometrics for IoT Medical Environments. *International Journal of Advanced Computer Science and Applications*, *9*(11). https://doi.org/10.14569/ijacsa.2018.091185

Patel, A., & Verma, A. (2017). IOT based Facial Recognition Door Access Control Home Security System. *International Journal of Computer Applications*, *172*(7), 11–17. https://doi.org/10.5120/ijca2017915177

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014). PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications. *International Journal of Distributed Sensor Networks*, *2014*. https://doi.org/10.1155/2014/357430

Poschmann, A. Y. (2009). Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. *Ph. D. Thesis*, *February*, 1–197. https://doi.org/10.1.1.182.1450%20

Pothumarti, R., Jain, K., & Krishnan, P. (2021). A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. *Journal of Ambient Intelligence and Humanized Computing*, *0123456789*. https://doi.org/10.1007/s12652-020-02857-4

Prabu, M., & Shanmugalakshmi, R. (2010). A study of elliptic curve cryptography and its application. *ICWET 2010 - International Conference and Workshop on Emerging*

Trends in Technology 2010, Conference Proceedings, *Icwet*, 425–427. https://doi.org/10.1145/1741906.1741997

Pramana, M. D., Lestyea, A., & Amiruddin, A. (2020). Development of a Secure Access Control System Based on Two-Factor Authentication Using Face Recognition and OTP SMS-Token. *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, 52–57. https://doi.org/10.1109/ICIMCIS51567.2020.9354328

Qiu, S., Xu, G., & Ahmad, H. (2019). An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography. *KSII Transactions on Internet and Information Systems*, *13*(2). https://doi.org/10.3837/tiis.2019.02.027

Rana, M., Shafiq, A., Altaf, I., Alazab, M., Mahmood, K., Chaudhry, S. A., & Zikria, Y. Bin. (2021). A secure and lightweight authentication scheme for next generation IoT infrastructure. *Computer Communications*, *165*, 85–96. https://doi.org/10.1016/j.comcom.2020.11.002

Rao, V., & Prema, K. V. (2019). Light-weight hashing method for user authentication in Internet-of-Things. *Ad Hoc Networks*, *89*, 97–106. https://doi.org/10.1016/j.adhoc.2019.03.003

Reddy, A. G., Das, A. K., Odelu, V., & Yoo, K. Y. (2016). An enhanced biometric based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. *PLoS ONE*, *11*(5), 1–28. https://doi.org/10.1371/journal.pone.0154308

Rene, C. I., Katuk, N., & Osman, B. (2022). A Survey of Cryptographic Algorithms for Lightweight Authentication Schemes in the Internet of Things Environment. *2022 5th International Conference on Computer and Informatics Engineering, IC2IE 2022*. https://doi.org/10.1109/IC2IE56416.2022.9970015

Rodrigues, B., Pawar, R., Patil, P., & Gour, A. (2019). *Encryption and Decryption of Biometric Traits*. *Journal of Computer Engineering (IOSR-JCE)*, *21*(3), 6–12. https://doi.org/10.9790/0661-2103010612

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2018). Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. *IEEE Internet of Things Journal*, *5*(4), 2884–2895. https://doi.org/10.1109/JIOT.2017.2714179

Roy, S., Chatterjee, S., & Mahapatra, G. (2018). An efficient biometric based remote user authentication scheme for secure internet of things environment. *Journal of Intelligent and Fuzzy Systems*, *34*(3), 1403–1410. https://doi.org/10.3233/JIFS-169435

Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *Journal of Supercomputing*, *77*(2), 1114–1151. https://doi.org/10.1007/s11227-020-03318-7

Shiratudin, N., & Hassan, S. (2010). Design Research in Software Development: Constructing and Linking Research Questions, Objectives, Methods and Outcomes. Sintok, Kedah: Universiti Utara Malaysia Press.

Sahani, M., Nanda, C., Sahu, A. K., & Pattnaik, B. (2015). Home Security System Based on Face Recognition. *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, 1–6. https://doi.org/10.1109/ICCPCT.2015.7159473

Sahoo, S., Sahoo, S. S., Maiti, P., Sahoo, B., & Turuk, A. K. (2019). A Lightweight Authentication Scheme for Cloud-Centric IoT Applications. *2019 6th International Conference on Signal Processing and Integrated Networks, SPIN 2019*, 1024–1029. https://doi.org/10.1109/SPIN.2019.8711757

Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., Elhoseny, M., & Baik, S. W. (2017). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.11.013

Santos, A. F., Marinho, J., & Bernardino, J. (2023). Blockchain-Based Loyalty Management System. *Future Internet*, *15*(5). https://doi.org/10.3390/fi15050161

Sehrawat, D., Gill, N. S., & Devi, M. (2019). Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment. *2019 6th International Conference on Signal Processing and Integrated Networks, SPIN 2019*, *June 2020*, 915–920. https://doi.org/10.1109/SPIN.2019.8711697

Sergiu, G. (2021). *CISA: Don't use single-factor auth on Internet-exposed system*. CISA's Bad Practices Catalog. https://www.bleepingcomputer.com/news/security/cisa-don-t-use-single-factor-auth-on-internet-exposed-systems/

Shaikh, Z. A., Khan, A. A., Baitenova, L., Zambinova, G., Yegina, N., Ivolgina, N., Laghari, A. A., & Barykin, S. E. (2022). A Blockchain Hyperledger and Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture. *Applied Sciences (Switzerland)*, *12*(5). https://doi.org/10.3390/app12052534

Shamim Hossain, M., Muhammad, G., Rahman, S. M. M., Abdul, W., Alelaiwi, A., & Alamri, A. (2016). Toward end-to-end biomet rics-based security for IoT infrastructure. *IEEE Wireless Communications*, *23*(5), 44–51. https://doi.org/10.1109/MWC.2016.7721741

Sharma, G., & Kalra, S. (2019). Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications. *Journal of Ambient Intelligence and Humanized Computing*, *0*(0), 0. https://doi.org/10.1007/s12652-019-01225-1

Shen, J. J. J., Chang, S., Shen, J. J. J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems*, *78*, 956–963. https://doi.org/10.1016/j.future.2016.11.033

Shivraj, V. L., Rajan, M. A., Singh, M., & Balamuralidhar, P. (2015). One time password authentication scheme based on elliptic curves for Internet of Things (IoT). *2015 5th National Symposium on Information Technology: Towards New Smart World, NSITNSW 2015*, *c*, 1–6. https://doi.org/10.1109/NSITNSW.2015.7176384

Shuai, M., Liu, B., Yu, N., Xiong, L., & Radenkovic, M. (2019). Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/8145087

Shuai, M., Yu, N., Wang, H., & Xiong, L. (2019). Anonymous authentication scheme for smart home environment with provable security. *Computers and Security*, *86*, 132–146. https://doi.org/10.1016/j.cose.2019.06.002

Shuai, M., Yu, N., Wang, H., Xiong, L., & Li, Y. (2021). A lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications. *Journal of Organizational and End User Computing*, *33*(3), 1–18. https://doi.org/10.4018/JOEUC.20210501.oa1

Siddiqui, F., Beley, J., Zeadally, S., & Braught, G. (2021). Secure and lightweight communication in heterogeneous IoT environments. *Internet of Things (Netherlands)*, *14*, 100093. https://doi.org/10.1016/j.iot.2019.100093

Singh, S., & Chaurasiya, V. K. (2021). Mutual authentication scheme of IoT devices in fog computing environment. *Cluster Computing*, *24*(3), 1643–1657. https://doi.org/10.1007/s10586-020-03211-1

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, *0*(0), 1–18. https://doi.org/10.1007/s12652-017-0494-4

Siswanto, A., Katuk, N., & Ku-Mahamud, K. R. (2020). Chaotic-based encryption algorithm using henon and logistic maps for fingerprint template protection.

International Journal of Communication Networks and Information Security, *12*(1), 1–9.

Son, S., Park, Y., & Park, Y. (2021). A secure, lightweight, and anonymous user authentication protocol for IoT environments. *Sustainability (Switzerland)*, *13*(16). https://doi.org/10.3390/su13169241

Soni, P., Ali, R., & Pal, A. K. (2017). *A Two-factor based Remote User Authentication Scheme using ElGamal Cryptosystem*. 1–6. https://doi.org/10.1145/3084030.3084031

Sree Vidya, B., & Chandra, E. (2018). Multimodal biometric hashkey cryptography based authentication and encryption for advanced security in cloud. *Biomedical Research (India)*, *2018*(Special Issue MedicalDiagnosisandStudyofBiomedicalImagingSystemsandApplications), S506–S516.

Sreemathi, M., Thangavel, K., & Sasirekha, K. (2014). *Elliptic Curve Cryptography based key generation from the fusion of ECG and Fingerprint*. *4*(3), 221–228.

Surendran, S., Nassef, A., & Beheshti, B. D. (2018). A survey of cryptographic algorithms for IoT devices. *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*, 1–8. https://doi.org/10.1109/LISAT.2018.8378034

Suresh, M., & Neema, M. (2016). Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things. *Procedia Technology*, *25*(Raerest), 248–255. https://doi.org/10.1016/j.protcy.2016.08.104

Taelman, R., Vander Sande, M., & Verborgh, R. (2019). Bridges between GraphQL and RDF. *W3C Workshop on Web Standardization for Graph Data*, 4–7.

Taher, B. H., Liu, H., Abedi, F., Lu, H., Yassin, A. A., & Mohammed, A. J. (2021). A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications. *Journal of Sensors*, *2021*. https://doi.org/10.1155/2021/8871204

Tan, C., & Lu, X. (2021). *Research on user security authentication method of eco-environmental monitoring database*. 1–11.

Tewari, A., & Gupta, B. B. (2017a). A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms*, *9*(2/3), 111. https://doi.org/10.1504/ijaip.2017.082962

Tewari, A., & Gupta, B. B. (2017b). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *Journal of Supercomputing*, *73*(3), 1085–1102. https://doi.org/10.1007/s11227-016-1849-x

Thabit, F., Alhomdy, A. P. S., Al-Ahdal, A. H. A., & Jagtap, P. D. S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91–99. https://doi.org/10.1016/j.gltp.2021.01.013

Towhidi, F., Manaf, A. A., Daud, S. M., & Lashkari, A. H. (2011). The Knowledge Based Authentication Attacks. *World Congress in Computer Science*. Retrieved from http://www.lidi.info.unlp.edu.ar/WorldComp2011-Mirror/SAM8123.pdf

Ulkadhim, Ahmed. (2020). Chaos-Modified Lightweight Present Algorithm for Image Encryption. *International Journal of Engineering Research and Advanced Technology*, *06*(02), 26–30. https://doi.org/10.31695/ijerat.2020.3601

Umoren, O., Singh, R., Pervez, Z., & Dahal, K. (2022). Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain. *Sensors*, *22*(10). https://doi.org/10.3390/s22103956Umar, S.S.I., Iro, Z.S., Zandam, A.Y., & Shitu, S.S. (2023). Accelerated Histogram of Oriented Gradients for Human Detection. *Journal of Pure and Applied Sciences (DUJOPAS),* 9(1), 44-56. https://doi:10.4314/dujopas.v9i1a.5

Usman, M. (2020). *Lightweight Encryption for the Low Powered IoT Devices*. *November*. http://arxiv.org/abs/2012.00193

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. *Information and Software Technology*, *94*(July 2017), 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

Velásquez, I., Caro, A., & Rodríguez, A. (2018b). Kontun: A Framework for recommendation of authentication schemes and methods. *Information and Software Technology*, *96*(September), 27–37. https://doi.org/10.1016/j.infsof.2017.11.004

Wang, C., Wang, D., Xu, G., & Guo, Y. (2017). A lightweight password-based authentication protocol using smart card. *International Journal of Communication Systems*, *30*(16), 1–11. https://doi.org/10.1002/dac.3336

Wang, D., & Wang, P. (2018). Two Birds with One Stone: Two-Factor Authentication with Security beyond Conventional Bound. *IEEE Transactions on Dependable and Secure Computing*, *15*(4), 708–722. https://doi.org/10.1109/TDSC.2016.2605087

WatchGuard. (2017). Internet security report. *Symantec,* 1–35. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_ 2011_ 212 39364.en-us.pdf

Wazid, M., Das, A. K., Bhat K, V., & Vasilakos, A. V. (2020). LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Applications*, *150*(November 2019), 102496. https://doi.org/10.1016/j.jnca.2019.102496

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law and Security Review*, *26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Wei, F., Ma, J., Jiang, Q., Shen, J., & Ma, C. (2016). Cryptanalysis and Improvement of an Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks. *Information Technology And Control*, *45*(1), 62–70. https://doi.org/10.5755/j01.itc.45.1.11949

Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. *Semiconductor Science and Information Devices*, *3*(1), 16–23. https://doi.org/10.30564/ssid.v3i1.3152

Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo, K. K. R., Wazid, M., & Das, A. K. (2017). An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *Journal of Network and Computer Applications*, *89*(December 2016), 72–85. https://doi.org/10.1016/j.jnca.2016.12.008

Wu, T. Y., Lee, Y. Q., Chen, C. M., Tian, Y., & Al-Nabhan, N. A. (2021). An enhanced pairing-based authentication scheme for smart grid communications. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02740-2

Wu, T., Yang, L., Lee, Z., Chen, C., Pan, J., & Islam, S. K. H. (2021). Improved ECC-based three-factor multiserver authentication scheme. *Security and Communication Networks, 2021.* https://doi.org/10.1155/2021/6627956

Xie, Q., Tang, Z., & Chen, K. (2017). Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks. *Computers and Electrical Engineering*, *59*, 218–230. https://doi.org/10.1016/j.compeleceng.2016.11.038

Xu, L., & Wu, F. (2015). Cryptanalysis and Improvement of a User Authentication Scheme Preserving Uniqueness and Anonymity for Connected Health Care. *Journal of Medical Systems*, *39*(2), 3–11. https://doi.org/10.1007/s10916-014-0179-x

Xu, L., & Wu, F. (2019). A Lightweight Authentication Scheme for Multi-gateway Wireless Sensor Networks Under IoT Conception. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-019-03752-7

Xue, K., Luo, X., Ma, Y., Li, J., Liu, J., & Wei, D. S. L. (2022). A Distributed Authentication Scheme Based on Smart Contract for Roaming Service in Mobile Vehicular Networks. *IEEE Transactions on Vehicular Technology*, *71*(5), 5284–5297. https://doi.org/10.1109/TVT.2022.3148303

Yang, W., Wang, S., Zheng, G., Yang, J., & Valli, C. (2019). A Privacy-Preserving Lightweight Biometric System for Internet of Things Security. *IEEE Communications Magazine*, *57*(3), 84–89. https://doi.org/10.1109/MCOM.2019.1800378

Yaleface Projects (1997). Yale-face-database. http://vision.ucsd.edu/content/yale-face-database

Yao, X., Chen, Z., & Tian, Y. (2015). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112. https://doi.org/10.1016/j.future.2014.10.010

Yao, X., Han, X., Du, X., & Zhou, X. (2013). A lightweight multicast authentication mechanism for small scale IoT applications. *IEEE Sensors Journal*, *13*(10), 3693–3701. https://doi.org/10.1109/JSEN.2013.2266116

Yu, S., Jho, N., & Park, Y. (2021). Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes. *IEEE Access*, *9*, 126186–126197. https://doi.org/10.1109/ACCESS.2021.3111443

Yu, S., Park, K., & Park, Y. (2019). A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Sensors*, *19*(16), 3598. https://doi.org/10.3390/s19163598

Zafaruddin, G. M., & Fadewar, H. S. (2018). Face recognition using eigenfaces. *Advances in Intelligent Systems and Computing*, *810*(3), 855–864. https://doi.org/10.1007/978-981-13-1513-8_87

Zaidan, A. A., & Zaidan, B. B. (2020). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artificial Intelligence Review*, *53*(1), 141–165. https://doi.org/10.1007/s10462-018-9648-9

Zargar, S., Shahidinejad, A., & Ghobaei-Arani, M. (2021). A lightweight authentication protocol for IoT-based cloud environment. *International Journal of Communication Systems*, *34*(11), 1–17. https://doi.org/10.1002/dac.4849

Zhao, C., Huang, M., Huang, L., Du, X., & Guizani, M. (2017). A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks. *Computer Networks*, *128*, 164–171. https://doi.org/10.1016/j.comnet.2017.05.028

Zhao, X., Zhong, B., & Cui, Z. (2023). Design of a Decentralized Identifier-Based Authentication and Access Control Model for Smart Homes. *Electronics (Switzerland)*, *12*(15). https://doi.org/10.3390/electronics12153334

Zheng, J., Wang, X., Yang, Q., Xiao, W., Sun, Y., & Liang, W. (2022). A blockchain-based lightweight authentication and key agreement scheme for internet of vehicles. *Connection Science*, *34*(1), 1430–1453. https://doi.org/10.1080/09540091.2022.2032602

Zheng, Q., Wang, X., Khurram Khan, M., Zhang, W., Gupta, B. B., & Guo, W. (2017). A Lightweight Authenticated Encryption Scheme Based on Chaotic SCML for Railway Cloud Service. *IEEE Access*, *6*, 711–722. https://doi.org/10.1109/ACCESS.2017.2775038

APPENDIX A

ENCRYPTION ALGORITHM AND PROCESS

A.1 ORIGINAL PRESENT

The source code of the original PRESENT encryption can be found here:

https://www.dropbox.com/s/dk3gpqvcvtjgc5z/Original%20PRESENT%20code.txt?dl=0

A.2 ENHANCED PRESENT

The enhanced PRESENT source code can be found here:

https://www.dropbox.com/s/tgjp5qp4z46euk2/Enhanced%20PRESENT%20code.txt?dl=0

A.3 ACCESS TO THE ENCRYPTION SYSTEM

The encryption system can be accessed through this link:

https://drive.google.com/drive/folders/1MP5fGTG_kRWus5RuZyWwARXOPqWq8ozf?usp=sharing

APPENDIX B ENCRYPTION RESULT OF TEXT FILES

B.1 The Text Files

Text2

300001,0,0,0,T,N,Red,Square,Lion,Canada,Piano,a5c276589,1ad744242,12e6161c9,46ae3059c,285771075,1,Master,LavaHot,1,A,RP,7,5300002,1,0,1,F,Y,Blue,Square,Dog,China,Piano,568550f04,1fe17a1fd,27d6df03f,b759e21f0,6f323c53f,2,Expert,Freezing,a,G,tP,1,12300003,0,0,1,Hot,b,Q,ke,2,3T,Y,Red,Star,d59d731b6

Text3

300006,0,0,0,T,Y,Green,Polygon,Cat,India,Oboe,dbfb714a4,788ba7aea,1c619215d,a6ae56854,d45567849,1,Contributor,Freezing,j,O,qP,4,9300007,0,0,0,T,N,Green,Trapezoid,Axolotl,Russia,Theremin,19db35594,d42f2b9ec,6b4d0cc44,56304bd77,985eabf13,3,Contributor,Freezing,j,A,KZ,3,1300008,0,1,1,T,N,Red,Square,Dog,China,Thereminmin,9bb7ea2da,b6972d6ec,a26bedd00,f0ca30ac1ac1,2,Contributor,BoilingHot,k,Q,aM,7,3

Text4

301070,0,0,1,T,Y,Green,Trapezoid,Hamster,Canada,Bassoon,3b5632a0c,cf8b12b4e,2c8ad6197,cfe0e3d59,73f000ff3,1,Novice,BoilingHot,j,U,YC,7,2301071,0,1,0,F,N,Red,Star,Snake,CostaRica,Bassoon,50f116bcf,6c90b0073,ba636104c,c1665c372,f26d7ddbd,1,Grandmaster,Cold,f,F,sD,1,3301072,0,0,1,T,N,Green,Trapezoid,Snake,China,Piano,e52fbf1c8,74e0be86d,7c033aaf1,8fe134687,996864a4f,1,Master,Freezing,g,I,kW,4,7301073,0,1,0,T,N,Blue,Trapezoid,Dog,Russia,Bassoon,1e6cb96e8,7e240024b,6206e88a7,5e2b7ec6

B.2 Text2 Ciphertext of the original PRESENT

701ad63b2c52aee568eab463ce037b35e63ce037b326a894a226a84b25fa640c3544a6c976114adf0568e682849904ab494a280215a54ac17df6eb22a8ddb374987fcf4c7b45ebd8682a923740b3947f946e8b63898a83465b856ed985683b936e59f8a6547b478d85fe895y6a874b74c36509826c03749b2084c2a84a6c5b63898a83y4ebaca280bd632673bad5462086b34987fcf4c7904ab463ce0352c4b29761145fe895y6a874b701ad63b2c58a83465b856ed1b5fa640c3544ebd8682a9237401ad63b2c52a8a83y4e349875fe547b

Text3 Ciphertext of the original PRESENT

59f8aa6406114adf4ac17d4c36349875fe547ba8a83y4e3ddb3d63b2c52a8a83y4ebaca4c7b45ebd5
6ede895y6b2c5252c40568e6d63b35e6f6eb22a8462086b34987fcf4c7904ab463ce0352c4b2976d
63b2c58a84b25fb2c524ab494a28086b349849875fe54d985683b63898a83y4ebaca280bd632673
bad57b478d3bad5462bd63267349875fe547bf6eb22a8086b3498826c03749b95ye895y6b468284
9900215a5f6eb22a8826c03749b74987fcf828499095y7b478d52c426a83ce032804ac17

Text4 Ciphertext of the original PRESENT

d1b5fa640c3544eb6114adfe03752c4d63b0568e63bad5462a8a83y4e3b4674987fcf349875fe547b8682a92
3743ce033bad5462d985683b0568e62c58a8a6c5be895y6bd632673b856ed63b2c52a8a83y4ed8682a8284
99074b701a0215a57401a6114adf856ebd632673b68ea92395yc354b35e6349875fe547b4ac17d4b25fab49
4a28280856e7b326086b34982806114adfc354b463caee5d63b2c52a8a83y4e52c43ce0359f8ae03
74a6c978682a923744ab494a2882849900215a585fe856edbacaf6eb22a856ed65bc354a6404b25f
a6c5b3bad54620b3947f946e8b85fe80

B.3 Text2 Ciphertext of the Enhanced PRESENT

d63b2c52a8a83y4e85fe81145f3465b8d63ad5462086b34ac17d4b25f7bebaca65b826c03749b936
eaee50b3947f946e8b086b349885fe87b478d0215a5856e85fe80568e628074b7d63b2c52a8a83y4
e4b25f49875fe540c3544eb936e59f8a4c362c58a826a8a640e037d8682a4ac17de895y67be0568e6
0c3544eb74987fcfc354f6eb22a8bd6326763898a834b46

Text3 Ciphertext of the Enhanced PRESENT

63898a83y4ebaca280bd632673bad57be3bad54625y6a87b478d462086b34987fcf4c7904ab463ce
0352c4b29769231145f0568e6d63b2c58a88682a923742c58a81b5fa64b2c5274b785fe84ab494a2
8b35e68284990856e7be0568e61145f5y6a80c3544ebb2c5252c43ce0374b7d985683b509c35482
6c03749b4b25ff6eb22a85y6a88682a92374701a4c3663898a834086b3498349875fe547bb463c1b
5fa64b29761145fe892084c2a84e895y674b701a68eab35e674b701ad8682a0b3947f946e8bb2976
1145fe89936e63898a834280462086b34987fcf4c7904ab463ce0352c4b2976c354d985683b50965
47401af6eb22a84b25f65b6114adf936ea6c5b74b701ad63b2c58a8826c03749b0c

Text4 Ciphertext of the Enhanced PRESENT

63898a8347bed985683b0b3947f946e8bbd632673bb4652c4462086b34987fcf4c7904ab463ce035
2c4b2976aee595yad5462086b32806114adf5y6a874b74a6c976a8bd632673b0215a5b29761145fe
89eba5y6a863898a834b29761145fe89349875fe547bd985683bad5462086b3d63b0568e6bd6326
78682a923747bed985683b74b76a8ca2803465b863898a834d634c3665bd63b0568e6462086b34
987fcf4c7904ab463ce0352c4b29767b478d7be63898a83y4ebaca280bd632673bad53465b874b70
1a92352c4b29761145fe8959f8ab463c6114adf2c58a856ed2084c2a84bd632673b63898a83y4eba
ca280bd632673bad546202a701aa894a282849900b3947f946e8b7b326a64074b701aad5462086b
3d8682a56e

APPENDIX C PCA IMPLEMENTATION AND FEATURE EXTRACTION

C.1 PCA IMPLEMENTATION SOURCE CODE

The PCA implementation source code can be found here:

https://www.dropbox.com/s/2n6lrqn6s0eciwd/PCA%20implementation%20code.txt?dl=0

C.2 Feature Extraction

Features are extracted from the face image files using PCA. Below are the images and the image template created.

Image02 of the Face Image Data

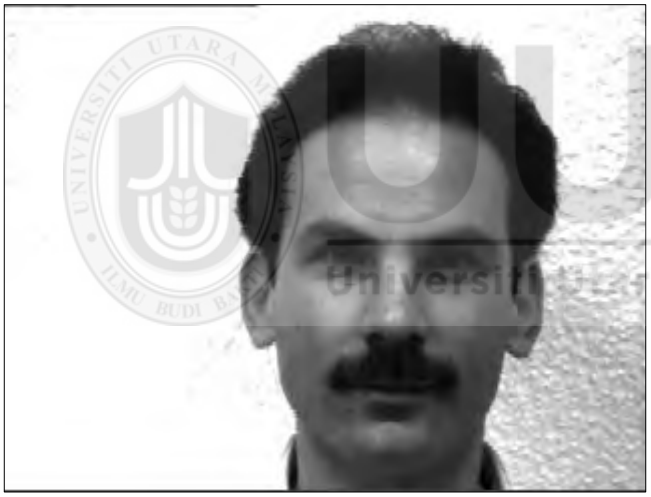


Image02 of Face Image Template

```
5.13040312e-02 3.39156477e-02 2.47893586e-02 2.27967054e-02 1.95632067e-02
1.82678428e-02 1.45655853e-02 1.38626271e-02 1.13318896e-02 1.07267786e-02
9.68365599e-03 9.17860717e-03 8.60995215e-03 8.21053028e-03 7.36580634e-03
7.01112888e-03
```

Image03 of Face Image Data

Image03 of Face Image Template

8.60995215e-03 8.21053028e-03 7.36580634e-03 7.01112888e-03 6.69450840e-03
6.40327943e-03 5.98295099e-03 5.49298705e-03 5.36083980e-03 4.99408106e-03
4.84854321e-03 4.77687371e-03 1.12203331e-04 1.11102187e-04 1.08901471e-04
1.06750318e-04

Image04 of Face Image Data

Image04 of Face Image Template

1.05732991e-04 1.01913786e-04 9.98164783e-05 9.85530209e-05 9.51582720e-05
8.95603083e-05 8.71638147e-05 8.44340263e-05 7.95894118e-05 7.77912922e-05
7.06467912e-05 6.77447444e-05 2.21225931e-3

APPENDIX D

ENCRYPTION RESULT OF FACE TEMPLATE

D.1: Original PRESENT Template Encryption

Image02 cipher template

24893eb7a9a8ed7432bcc9e9f73dfghijaaa41bd25fdfa1929bghija95dcb5d9697f746806f1f41df45
d95e39eghija9261da6cb4f1c021b6c81fec4b067d46432ce55ecea37a602fd7242e1fb44bb343f072
28cd0ghija5e78a0ghija412badaeghija73051f24ghija8ghija57677ghij

Image03 cipher template

1b25ghija63be0a428661a72ghijaa95f7aghijaa4a3118a1e9ghija44bf0003f02a53b4a80cc2aghijac
5ghijaghijaghija904d85e9d844147cc9ghijaa544ec21b62387f90afdec34244ghija48d059661ghija
446ac3922a7ghija2faghijab73da30416dd6eghija44cc26ghija2ghijac3dab05

Image04 cipher template

c0be2ghija30fd2dce59ghijabea26eaghija8049f65aghija3e6f8ccbb280ce024880f0dc4b3489bffde
bd3016b0257e1a20ghijaa84265ccc030a760ghijad5ad5bfghija6cghija3136ghijaaf6abd436b8e9c2
e119256b4ghijad5a96d241726d6eab58f64b65ff475abb008bf81dd2420ghija474c848ghija13ea4b
f0634bb34f0ghija38a8fb52711b0eghijacdfd02a275ghijaf

D.2 Enhanced PRESENT Template Encryption

Image02 cipher template

29fcdaghijaghija6fb3d5644fd2244b46506f710dd3a6bfa85eaghija605f43362ghijae9a1707aghijab
41e6712293cca8ghija170dea43f997076dc010b6e46a021533728ef1537c2e3750ghijaa044cac63a
dd5e039d834185d22fghijad85ghija1hijaghijac0d98121a2124218240f654fcghija729592181dbee
334638376b5c

Image03 cipher template

a94db35707c27ghijad384c387b58699dc00c6833dcghija4c626f82294dghijae82d84adfb4b747b8
cfe903468ghija2396bghija20b0dc26bghijabf26052103c3ghija958f7e860af06ecf19e76e4f5e4e52
039b447fghija514620cbe4287149461ghijaghijaghija9f2ghijab28d26d4d4e372ebghija0a318a2c8

Image04 cipher template

2ghija83201ghija8e9153ghija6b148028cab5ba7dcf4e82c4e1ghija64fe4b6df9ghija62f9ghijad552
65097ghija1797b1b2e6f64c2835f6214ghija62e4e46bb03d4ffee92233bd65a3eb30aec13e8d9c0df
a11c0b25b5cghija77ab0dghijaghija5473f214157c54cce7a808ghijaaf17f16f407dfghija3883ghija
2ghijaghija1ghijaghija3b880a795fc46784bcc92ghija139a3267ace2a5

APPENDIX E

FORMAL VERIFICATION OF THE PROTOCOL USING ProVerif

```
(*----FACE AND EMAIL LINK AUTHENTICATION SCHEME----*)

(*Secure Channel----//The Communication channels between CS,S, and UD---*)
free cCSS:channel [private].
free cSCS:channel [private].
free cUDCS:channel [private].
free cCSUD:channel [private].


(*entities---//The Identity of the entities used in communicating with the Functions-
--*)
free IdS:bitstring [private].
free IdCS:bitstring [private].
free IdU:bitstring [private].
free Fi:bitstring [private].
free IdUD:bitstring [private].
free Ft:bitstring [private].
free EL:bitstring [private].

(*Secret Key *)
free SK:bitstring [private].
(*Shared key*)
free SKudcs:bitstring [private].
free SKcss:bitstring [private].
free R:bitstring[private].

(*Functions*)
fun Concatenation(bitstring, bitstring):bitstring.
fun Hash(bitstring):bitstring.
fun PRESENT(bitstring):bitstring.
fun PRESENT2(bitstring,bitstring):bitstring.
fun PRESENT1(bitstring,bitstring):bitstring.

(*Events*)
event StartSetup(bitstring).
```

```
event EndSetup(bitstring).
event StartAuthenticationLogin(bitstring,bitstring,bitstring).
event SuccessfulAuthenticationLogin.
event UnSuccessfulAuthenticationLogin.
event GenerateEmailLink.
event FaceTemplate(bitstring).
event EndAuthenticationLogin(bitstring,bitstring,bitstring).
event StartUserProfileRecovery(bitstring,bitstring,bitstring,bitstring).
event UnSuccessfulUserProfileRecovery.
event UserProfileRecovery(bitstring).
event EndUserProfileRecovery(bitstring,bitstring,bitstring,bitstring).

(*Check for vulnerability in the data*)
query attacker(IdS).
query attacker(IdCS).
query attacker(SKS).
query attacker(SKcss).
query attacker(IdU).
query attacker(Fi).
query attacker(SKudcs).
query attacker(IdUD).
query attacker(Ft).
query attacker(EL).
query id:bitstring;inj-event(EndSetup(IdCS))==>inj-event(StartSetup(IdS)).
query id:bitstring;inj-event(EndSetup(IdUD))==>inj-event(StartSetup(IdCS)).
query id:bitstring;inj-event(EndAuthenticationLogin(IdU,Fi,IdUD))==>inj-
event(StartAuthenticationLogin(IdU,Fi,IdUD)).
query id:bitstring;inj-event(EndUserProfileRecovery (IdU,Fi,EL,Ft))==>inj-event(
StartUserProfileRecovery(IdU,Fi,EL,Ft)).
process
event StartSetup(IdS);
let KCSS=Hash(Concatenation(IdCS,SK)) in
let KUDCS=Hash(Concatenation(IdUD,SKudcs)) in
out(cSCS,KUDCS);
event EndSetup(IdCS);

event StartAuthenticationLogin(IdU,Fi,IdUD);
event StartUserProfileRecovery(IdU,Fi,EL,Ft);
new EFi:bitstring;
```

```
    new RId:bitstring;
    new T:bitstring;
    new DFi:bitstring;
    new Ael:bitstring;
    new T1:bitstring;
    new Ft:bitstring;
    new Ft1:bitstring;
    new Eft:bitstring;
    new Eft1:bitstring;
    new NEft:bitstring;
    new NEft1:bitstring;

    let EFi=PRESENT1(Fi,SKudcs) in
    out(cUDCS,(RId,T,EFi,IdUD));
    let DFi=PRESENT1(Fi,SKudcs) in
    if DFi=EFi then event GenerateEmailLink else event
UnSuccessfulAuthenticationLogin;
    let Ael=PRESENT1(EL,SKudcs) in
    out(cCSUD,(RId, T, Ael, IdCS));



    let NEft=Hash(Eft) in
    let NEft1=Hash(Concatenation(IdU,SK)) in

    if NEft=NEft1 then out(cUDCS,(RId,T,Ael))else event
UnSuccessfulUserProfileRecovery;
    out(cUDCS,(RId,T,Ael));
    event UserProfileRecovery(R);
    event EndUserProfileRecovery (IdU,Fi,EL,Ft);

    event FaceTemplate(Ft1);
    let EFt=PRESENT2(Ft,SKudcs) in
    let EFt1=PRESENT1(Ft,SKudcs) in

    if Eft1=Eft then out(cUDCS,(RId,T,IdU,IdUD))else event
UnSuccessfulAuthenticationLogin;
    if Eft1=Eft then out(cCSS,(IdUD,T,IdS))else event
UnSuccessfulAuthenticationLogin;
```

```
    if T<>T1 then event SuccessfulAuthenticationLogin else event
UnSuccessfulAuthenticationLogin;
    event EndAuthenticationLogin(IdU,Fi,IdUD);
0
```


APPENDIX F

INSTALLATION AND CONFIGURATION GUIDE OF AUTHENTICATION SCHEME TOOL

F.1 PI Configuration

Preparing SD Card and Raspbian Operating System

How to install an SD card-based operating system image on a Raspberry Pi is explained in this resource. To install the image, you will need a computer with an SD card reader. An SD Card with at least 4 GB, ideally 8/16 GB, is required. The operating system can be obtained by downloading it from https://www.Raspberrypi.org/downloads/. There are two choices for the OS. NOOBS, the easy installer and our easy installer for Raspbian, are the official operating systems for all Raspberry Pi models. Click on Raspbian to download Raspbian Buster with desktop and recommended software for installation with Raspbian.

Installing the OS into an SD Card

You will need to use an image writing tool to install the image you have downloaded on your SD card. balenaEtcher is a graphical SD card writing tool that works on Mac OS, Linux, and Windows, and is the easiest option for most users. balenaEtcher also supports writing images directly from the zip file, without any unzipping required. To write your image with balenaEtcher:

- Download the latest version of balenaEtcher (https://www.balena.io/etcher/) and install it.
- Connect an SD card reader with the SD card inside.
- Open balenaEtcher and select from your hard drive the Raspberry Pi .img or .zip file you wish to write to the SD card.
- Select the SD card on which you wish to write your image.

- Review your selections and click 'Flash!' to begin writing data to the SD card.

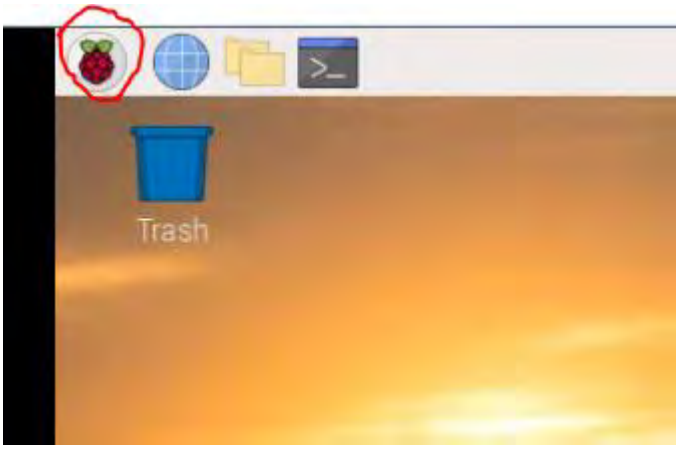
Note: for Linux users, zenity might need to be installed on your machine for balenaEtcher to be able to write the image on your SD card.

Running Raspberry PI for the first time

- After the OS has been written into the SD Card, insert the SD Card into Raspberry PI.
- Attach your HDMI or VGA to a display screen. **Note: This process is only done on the first configuration.**
- Power on the Raspberry PI
- Follow display screen instructions for the first-time setup
- Note your username and password if you change from the default.

Once you have access to Raspberry PI, configure the system.

Click on the red marked icon on the image below, select preferences, then Raspberry PI Configuration, click on interfaces, enable all interfaces, and click Ok.



Enable your Bluetooth

Access Raspberry using VNC viewer, SSH/Telnet.

First, insert your RJ45 Ethernet Cable between Raspberry PI and your computer, and connect your computer to WIFI.

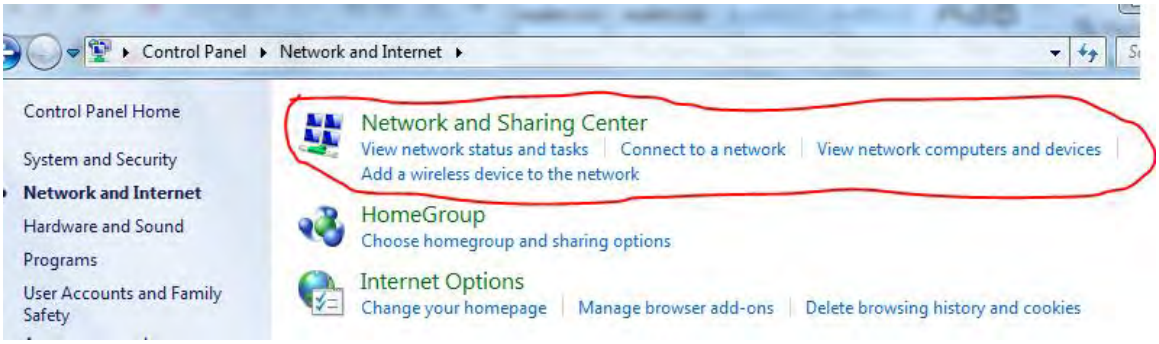
VNC Viewer access

- Download VNC viewer: https://www.realvnc.com/en/connect/download/viewer/
- To access Raspberry PI with VNC, you will need a Raspberry IP Address.

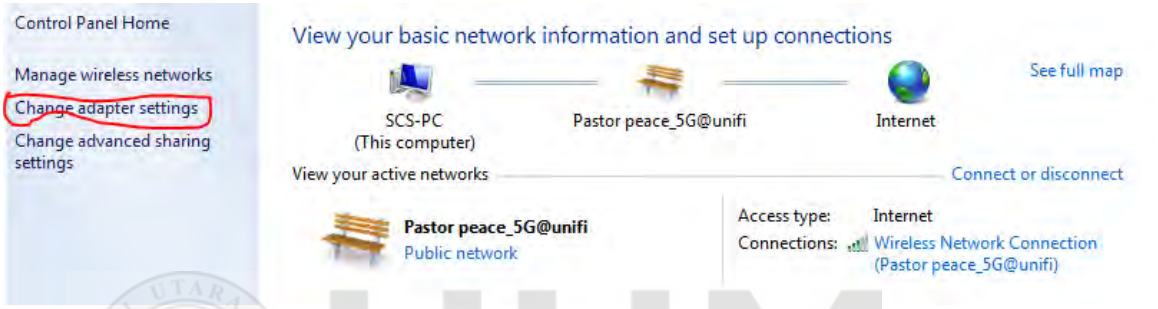
Use the following steps:

Select the red mark section from your control panel

Select Network and Sharing

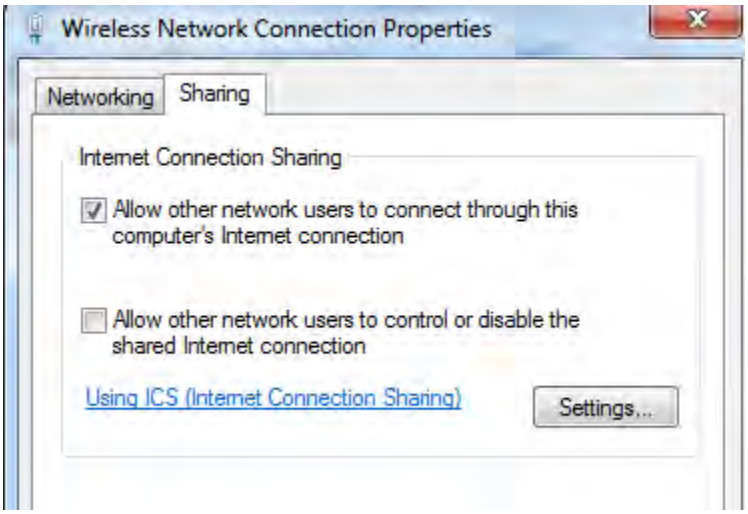


Select Change Adapter settings

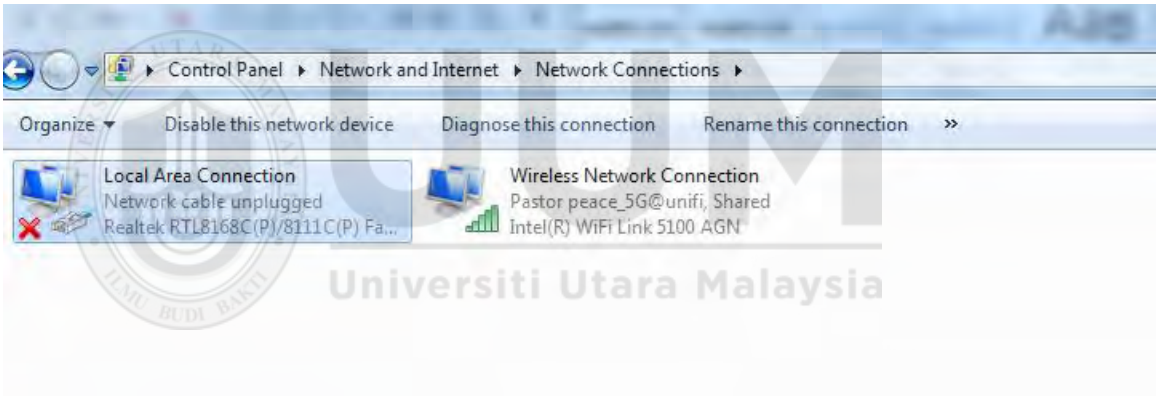


Right-click on Wireless Network Connection, and select properties

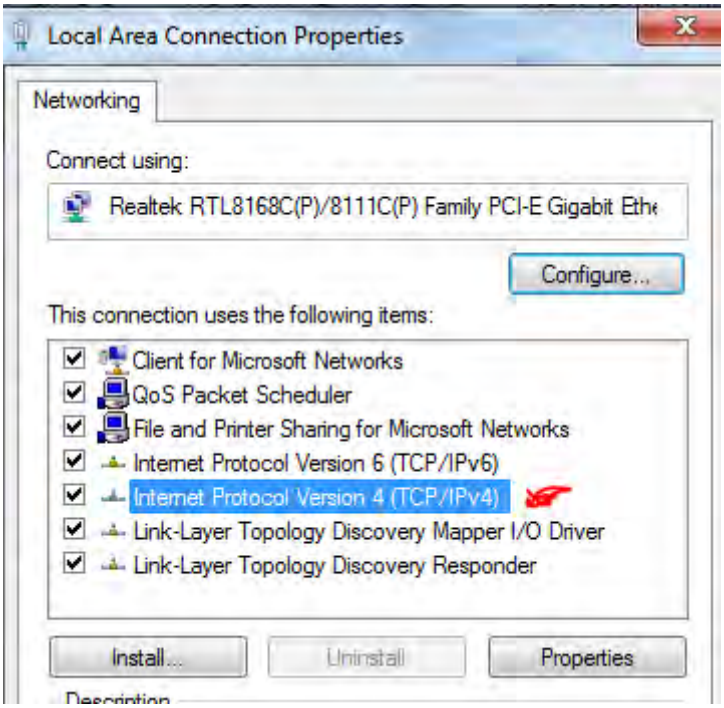
Select Sharing and checkbox allow other network users to connect through this computer internet connection and click OK and close the section.



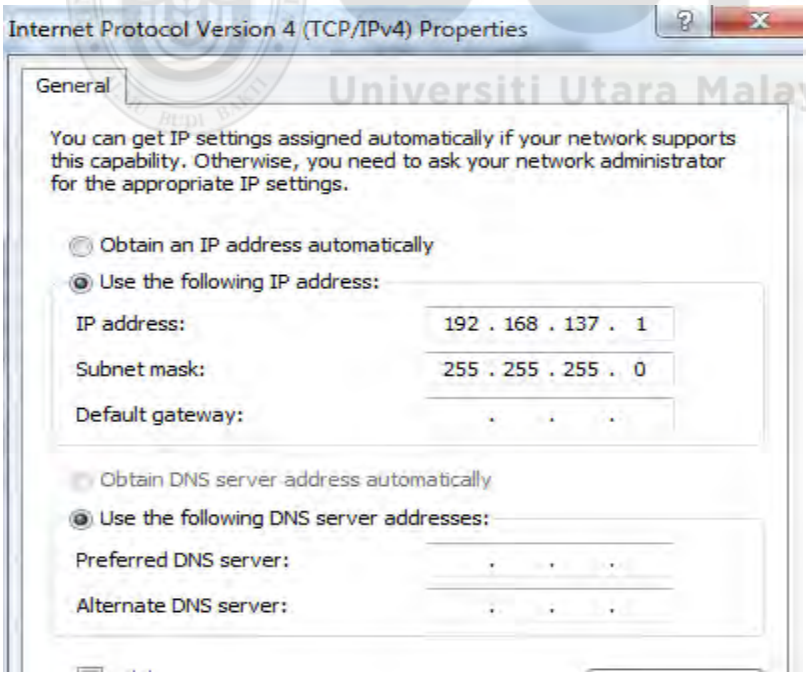
To identify the IP Subnet mask range of the Raspberry pi right-click on Local Area Connection



Double-click on TCP/IPv4



Select “Use the following IP address or Use Static IP address, and copy down the IP address that u see.



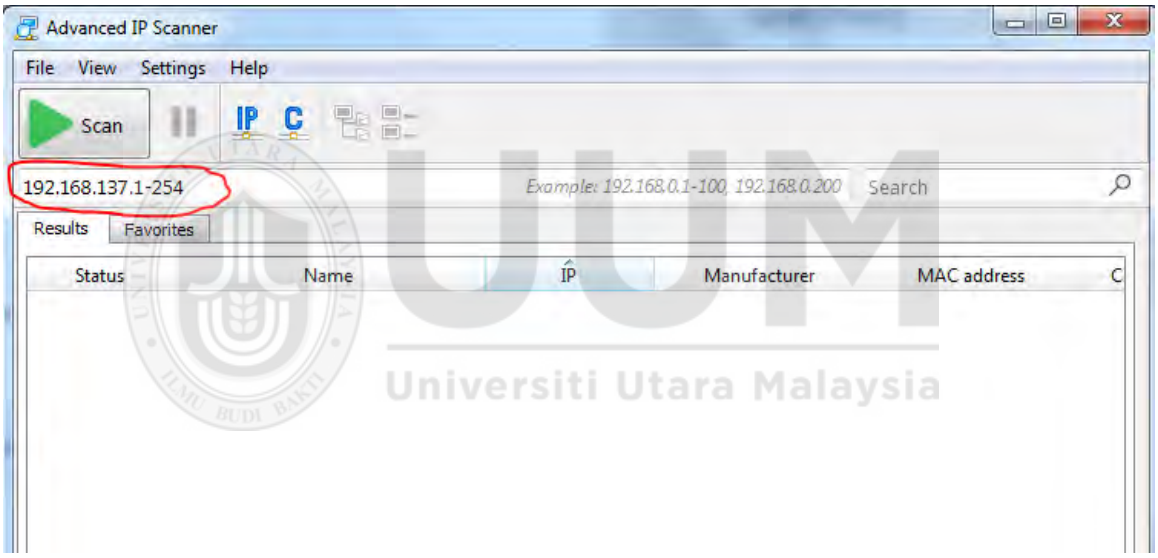
Having the IP Address found in mind, follow the next step:

Finding the IP Address of Raspberry PI

Download the advanced IP scanner (https://www.advanced-ip-scanner.com/) after downloading and opening the program.

Enter the IP address you copied and extend it to the range of 254. This will help you get the IP address of the Raspberry pi, then click scan, wait for some time, and you will see Raspberry with a name that looks like this: **Raspberrypi.mshome.net**, but it will be different if the name has been changed.

After you have identified the Ip address, Open the VNC viewer you downloaded.



Open the VNC viewer program, and key in the IP Address, and tap your enter button. It will connect to the Raspberry pi and ask for login details, and you have access to the Raspberry pi.

Default login

Userid: pi
Password: Raspberry

F.2 OPENCV CONFIGURATION AND INSTALLATION

To install and configure OpenCV in PI, the following script is executed.

```
sudo apt-get -y purge wolfram-engine

sudo apt-get -y purge libreoffice*

sudo apt-get -y clean

sudo apt-get -y autoremove

echo "OpenCV installation by learnOpenCV.com"
cvVersion="masrer"
```

clean build directories and create the installation directory

```
rm -rf opencv/build
rm -rf opencv_contrib/build
mkdir installation
mkdir installation/OpenCV-"$cvVersion"
```

APPENDIX G

IMPLEMENTATION OF THE DECENTRALIZED MULTI-FACTOR FACE IMAGE USER AUTHENTICATION SCHEME

G.1 Coding the Authentication Scheme

Enhanced PRESENT for Face Template Encryption

The source code for enhanced PRESENT for face template encryption can be found here: https://www.dropbox.com/s/88hialkwqyprt50/enhanced%20PRESENT%20for%20face%20template%20encryption%20code.txt?dl=0

ECC Encryption, Key Exchange, and Email Verification

The source code for ECC Encryption, Key Exchange, and Email Verification can be found here: https://www.dropbox.com/s/n34m608kdu12p6j/ECC%20Encryption%2C%20Key%20Exchange%2C%20and%20Email%20Verification%20code.txt?dl=0

Face Recognition Module

The source code for the face recognition module can be found here: https://www.dropbox.com/s/k704dr8o1mp2lb9/face%20recogintion%20module%20code.txt?dl=0

APPENDIX H

INSTALLATION AND CONFIGURATION OF REAL-LIFE SECURITY EVALUATION ENVIRONMENT

1. The first step is to download Kali Linux from the Kali Linux website https://www.kali.org/get-kali/
2. Launch the Kali Linux machine to get started.
3. Launch Ettercap
4. Set up the DNS config file in Ettercap

Set up the command terminal and change the DNS configuration of the Ettercap by typing the following syntax into the editor of your choice.

$ gedit /etc/ettercap/etter.dns

You will be displayed the DNS configuration file.

Next, you'll need to type your address in the terminal

>* a 10.0.2.15

Prepare the Apache server

Now fire up the Apache Server with the following command:

$ sudo service apache2 start

You'll see that the server has successfully launched.

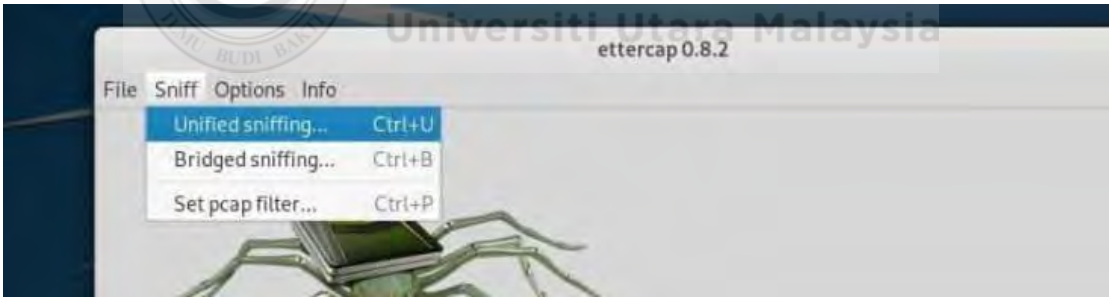
Spoofing with Ettercap addon

Now we'll see how Ettercap would come into play. We will be DNS spoofing with Ettercap. Launch the app by typing:

$ettercap -G

You can see that it's a GUI utility, which makes it much easier to navigate.

Once the addon has opened, you hit the 'sniff bottom' button and choose United sniffing



Select the network interface that's in your use at the moment:

With that set, click on the host tabs and choose one of the lists. If there's no appropriate host available, you may click the scan host to see more options.

Next, designate the victim to target 1 or 2. You can designate the victim by clicking on the target two-button and then on add to the target button.

Next, hit the mtbm tab and select ARP poisoning.

Now navigate to the Plugins tab and click on the "Manage the plugins" section and then activate DNS spoofing.

Catching the Https traffic with Wireshark

Launch Wireshark to attract the https traffic and try to retrieve web account details.

To launch Wireshark, summon a new terminal and enter Wireshark.