

Declaration

I hereby declare that the work presented in this thesis titled *Advanced Security Solutions for Large-scale and Highly Dynamic Internet of Vehicles (IoV)* submitted to the Indian Institute of Technology Jodhpur in partial fulfillment of the requirements for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work carried out under the supervision of Dr. Debasis Das (IIT Jodhpur, India). The contents of this thesis in full or in parts, have not been submitted to, and will not be submitted by me to any other Institute or University in India or abroad for the award of any degree or diploma.



Himani Sikarwar

P19CSE013

Computer Science and Engineering
Indian Institute of Technology Jodhpur

Certificate

This is to certify that the thesis titled *Advanced Security Solutions for Large-scale and Highly Dynamic Internet of Vehicles (IoV)*, submitted by Himani Sikarwar (P19CSE013) to the Indian Institute of Technology Jodhpur for the award of the degree of *Doctor of Philosophy*, is a bonafide record of the research work done by her under my supervision. To the best of my knowledge, the contents of this report, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.



Dr. Debasis Das
Ph.D. Thesis Supervisor
Computer Science and Engineering
Indian Institute of Technology Jodhpur

Abstract

The Internet of Vehicles (IoV) is a large-scale, highly dynamic network of heterogeneous communications. Maintaining a balance between authentication and privacy is crucial in such types of networks. Moreover, ensuring a high level of security through heterogeneous communication can result in significant computational overhead due to the numerous cryptographic operations required, which have higher execution times. Such trade-off between security and efficiency, are impractical in IoV networks, where the IoV devices have limited processing power and storage capacity. Furthermore, diverse communications generate substantial data that requires secure storage. Therefore, it is essential to minimize data storage and retrieval times to facilitate real-time communication in rapidly changing resource-constrained IoV network. These problems can be solved using lightweight security solutions that make sure users are authenticated without compromising their privacy. These solutions can also improve the trade-off between security and performance and make it easier to store and retrieve the large amounts of data that are created by different types of communication in the IoV network.

The research is conducted in two phases. The first phase proposes advanced security solutions for the aforementioned issues using Tamper-Proof Devices (TPD). The TPD, a type of Hardware Security Module (HSM), stores cryptographic keys along with secret parameters and performs cryptographic operations such as authentication, encryption, decryption, and so on within the device. Initially, a lightweight conditional-privacy preservation-based authentication mechanism is proposed, enhancing security through innovative key management mechanisms, such as Hard Key Update (HKU) and Soft Key Update (SKU). These mechanisms safeguard against key disclosure and ensure continuous protection even in the case of key compromise. The proposed solution significantly reduces computational and communication overhead using cryptographic techniques such as Message Authentication Codes (MACs), hash functions, and XOR operations. The research is further extended to mitigate the security-performance trade-off by implementing the idea of static and dynamic batch verification of multiple messages, leveraging lightweight cryptographic operations. The proposed method reduces computational overhead and ensures data integrity and confidentiality across the network. Additionally, it provides a solution for efficient and secure storage-retrieval of information while enhancing the responsiveness and efficiency of IoV services having dynamic and large-scale environment. The proposed approach reduces latency and prevents bottleneck issues in a centralized system by integrating edge computing with the Vehicular Cloud (V-Cloud).

Despite their robust design, TPDs can still be vulnerable to advanced physical attacks because of potential hardware flaws or inadequate protection against complex tampering techniques. Attackers can exploit these weaknesses to bypass security measures, potentially compromising the integrity of the device. This issue is resolved by introducing alternative approaches using Physical Unclonable Functions (PUF) devices. PUFs use hardware's inherent physical irregularities to generate cryptographic keys on demand, making them nearly impossible to clone and highly resistant to tampering, unlike TPDs, which require secure key storage. In the second phase, PUF devices are used as secure hardware modules to design a highly secure and lightweight authentication scheme using a Challenge-Response Pair (CRP) mechanism. Furthermore, the research provides an effective solution for enhancing security on resource-constrained devices, where efficient and secure data handling is crucial. The framework uses PUFs to generate dynamic nonce and keys to address nonce reuse issue, without imposing significant computational or energy demands. Additionally, implementing this framework on low-power hardware platforms demonstrates its suitability for systems that require high security with efficient power usage, making it an ideal choice for securing resource constrained IoV devices.

Comprehensive security analysis using BAN logic, Random Oracle Model (ROM), and the ProVerif tool validates the technical depth of the proposed solutions, making them highly effective in countering a wide variety of security threats prevalent in IoV scenarios. The proposed methods are also evaluated against existing techniques, demonstrating improvements in terms of computational overhead, communication overhead, energy consumption, latency, and scalability.

**To My Princess, *Kuhoo*,
My Caring Husband, *Abhishek*,
My Parents and In-laws.**

Acknowledgements

I am deeply grateful to my supervisor, Dr. Debasis Das, for his consistent support throughout my research. His guidance, advice, and feedback were crucial to completing this work. Dr. Das's encouragement and understanding, especially, for the challenges I faced during my pregnancy, provided me with the strength and motivation to persevere. His commitment to my academic and personal well-being has been to my success. I appreciate his patience and strong belief in my potential. Thank you, Dr. Das! I extend my heartfelt gratitude to my Student Research Committee (SRC) members, Dr. Suman Kundu, Dr. Angshuman Paul, and Dr. Nilkamal Hazra, for their guidance and valuable feedback throughout my research journey. They were always available to help me and provided valuable career advices.

I am also grateful to my best friends, Ankur Nahar and Lokendra Vishwakarma, for their constant support and companionship throughout my research. Their presence during the highs and lows of my research journey provided the encouragement I needed. Beyond academic support, their friendship has been key to my success. Thank you for believing in me and encouraging me every step of the way. I also want to thank my VANET lab members and friends, Monu Nagar, Ashish Bohra, Amritesh Kumar, Aarju Dixit, Nandini Saini, and K.K. Mondal, for their support and the joyful moments we shared. Your friendship made this journey enjoyable and memorable. Thank you for being there for both the work and the fun that lightened the load. Your friendship and support have been invaluable.

I am deeply thankful to my parents and in-laws for their exceptional support throughout this journey. My parents, despite their commitments, stayed with me to care for my daughter, allowing me to focus on my research. Their sacrifice has been invaluable. I am equally thankful to my in-laws for understanding my work demands and relieving me from household duties. Their support has enabled me to pursue my academic goals without distraction. My husband, Abhishek Fauzdar, has been a true gem, consistently motivating me and sharing responsibilities. His belief in my abilities, patience, and encouragement have helped me navigate challenging moments. Without his love and steadfast support, this journey would have been much more difficult. Thank you all for your love, care, and constant support.

Last but not least, I want to acknowledge my dear daughter, Kuhoo (Chhavishka). She has been a constant ray of hope, with her beautiful smile and sweet conversations always lifting my spirits. Even on the most stressful days, her cheerful presence makes me smile. Thank you, my princess, for bringing so much joy and love into my life. Your love and smiles have been a guiding light throughout this journey.

*Himani Sikarwar
P19CSE013
Computer Science and Engineering
Indian Institute of Technology Jodhpur*

Table of Contents

Declaration	I
Certificate	III
Abstract	V
Acknowledgments	IX
Table of Contents	XI
List of Figures	XV
List of Tables	XVII
1 Introduction	1
1.1 Background	1
1.1.1 Need of Internet of Vehicles	3
1.1.2 Security Requirements in Internet of Vehicles	4
1.2 Research Motivation	7
1.3 Research Objectives	9
1.4 Summary of Contributions	11
1.4.1 Tamper-Proof Device Based Solutions	11
1.4.2 Physical Unclonable Function Based Solutions	13
1.5 Preliminaries	14
1.5.1 Hardware Security Modules	14
1.5.2 Simulation Tools	17
1.5.3 Models for Security Analysis	19
1.6 Thesis Structure	21
2 Related Work	23
2.1 Based on Tamper-Proof Device	24
2.1.1 Authentication Schemes	24
2.1.2 Batch Verification Methods	26
2.1.3 Secure Data Handling	29
2.2 Based on Physical Unclonable Functions	32
2.2.1 Authentication Schemes	32
2.2.2 Secure Data Handling	35

3	Lightweight Authentication and Verification using Tamper-Proof Devices	41
3.1	Conditional Privacy Preservation and Lightweight Authentication	42
3.1.1	Network and Adversary Model	44
3.1.2	Proposed Scheme: NoMAS	46
3.1.3	Security Analysis	51
3.1.4	Performance Analysis and Simulation Results	57
3.1.5	Implementation Considerations in Diverse IoV Environments	62
3.2	Static Batch Verification	62
3.2.1	Proposed Scheme: Static Batch Verification	63
3.2.2	Security Analysis	68
3.2.3	Performance Analysis and Simulation Results	70
3.3	Dynamic Batch Verification	72
3.3.1	Network and Delay Model	73
3.3.2	Proposed Method: Dynamic Batch Verification (DyBatch)	75
3.3.3	Security Analysis	81
3.3.4	Performance Analysis and Simulation Results	83
3.4	Summary of the Work	87
4	Secure Data Handling using Tamper-Proof Devices	89
4.1	Proposed Hybrid Architecture for Internet of Vehicles	90
4.2	Proposed Scheme: <i>SecEdge</i>	91
4.3	Security Proof and Analysis	95
4.4	Performance Analysis And Simulation Results	102
4.5	Summary of the Work	105
5	Lightweight Authentication using Physical Unclonable Functions	107
5.1	PUF based Lightweight and Efficient Authentication by Integrating the Edge-computing	108
5.1.1	Network Model	109
5.1.2	Proposed Scheme: <i>PESPI</i>	110
5.1.3	Security Analysis	115
5.1.4	Performance Analysis and Simulation Results	118
5.2	PUF-based Lightweight Authentication in Drone-assisted Internet of Vehicles	122
5.2.1	Network Model	124
5.2.2	Proposed Scheme: <i>SECURE</i>	125
5.2.3	Performance Analysis and Simulation Results	130
5.3	Summary of the Work	133
6	Secure Data Handling using Physical Unclonable Functions	135
6.1	Proposed Scheme: PUF-AEAD	136
6.1.1	Security Enhancement Using PUFs	136
6.1.2	Modified AEAD algorithm using PUF	138
6.1.3	Proposed Cryptographic Hardware Accelerator	140
6.2	Security Analysis	143
6.3	Experimental Setup and Performance Analysis	145
6.4	Summary of the Work	149

7 Conclusion and Future Direction	151
7.1 Chapter 1: Introduction	151
7.2 Chapter 2: Related Work	151
7.3 Phase 1: TPD-based Security Solutions	152
7.3.1 Chapter 3: Lightweight Authentication and Verification:	152
7.3.2 Chapter 4: Secure Data Handling:	152
7.4 Phase 2: PUF-Based Security Solutions	152
7.4.1 Chapter 5: Lightweight Authentication using PUF:	153
7.4.2 Chapter 6: Secure Data Handling using PUF:	153
7.5 Limitations and Future Direction	154
Publications	155
References	157

List of Figures

1.1	A smart city scenario implementing the Internet of Vehicle (IoV) network	2
1.2	Heterogeneous communications in IoV network	3
1.3	Basic advantages of IoV including road safety, traffic management, environmental sustainability, infotainment services, and autonomous system	4
1.4	Security requirements for IoV communications	5
1.5	Primary security requirements in IoV: (a) Absence of authentication, (b) Absence of message integrity, (c) Absence of confidentiality, (d) Absence of network availability	6
1.6	Vulnerabilities and Attack Trends in Automotive Cybersecurity and IoV: (a) Cybersecurity issues in automotive industry, (b) Percentage of attacks by category in IoV	7
1.7	Primary research objectives that aim to balance authentication-privacy, to achieve high level of security having less overhead, and to securely handle the vast amount of IoV data	9
1.8	Contributions: Advance security solutions for large-scale and highly dynamic IoV	11
1.9	Internal working and the basic functioning of Tamper-Proof Device (TPD)	15
1.10	Unique characteristics of Physical Unclonable Functions (PUF)	16
1.11	ProVerif tool flowchart	18
2.1	Structural organization of the literature survey	24
3.1	The impact of conditional privacy preservation over fully privacy preservation	43
3.2	Network model for NoMAS	45
3.3	Various phases of the NoMAS scheme: (a) Network initialization and key generation stage, (b) User and vehicle registration stage, (c) Anonymous authentication of the user, (d) Secure communication and message verification between two vehicles	51
3.4	Process to create a session for authentication of vehicle	56
3.5	Comparison of NoMAS with state-of-the-art schemes in terms of: (a) Computation cost (Desktop), (b) Computation cost (Raspberry Pi), (c) Communication cost (bytes), (d) Energy consumption on Desktop (mJ)	58
3.6	Simulation results of NoMAS in terms of: (a) Physical layer overhead during message transmission, (b) Average one way delay (seconds), (c) Average throughput (bits/second)	60
3.7	Simulation results of NoMAS in terms of: (a) Packet delivery ratio for different cases (b) Packet loss ratio for different cases	61
3.8	Proposed layered architecture for the secure IoV	64
3.9	Comparison of computation cost (ms) between proposed scheme and state-of-the-art schemes	70
3.10	Network architecture of DyBatch for e-IoV networks	73

3.11	Performance evaluation of DyBatch: (a) Comparison of computation cost on different platforms, (b) The impact of the number of VPVs on the overall verification delay, (c) The variations in the number of optimal VPVs in case of increase in the number of SVs, (d) Comparison of verification delay in the case of verification done by EN only, and verification done by both EN and VPVs, (e) Number of verified BAMS for different schemes without re-batch formation, (f) Comparison between DyBatch and Ferng et al.'s scheme based on the number of verified BAMS in case of re-batch formation	86
3.12	Simulation results of DyBatch: (a) Packet delivery ratio v/s Packet loss ratio, (b) Latency analysis for 100 seconds, (c) Latency and Jitter comparison for every 10 seconds interval, (d) Throughput analysis	88
4.1	The proposed hybrid architecture for IoV leverages RSCN as highly capable nodes, structured into domains, and functioning as edge nodes	91
4.2	Performance evaluation and simulation results of <i>SecEdge</i> : (a) Energy consumption comparison of <i>SecEdge</i> with state-of-the-art schemes based on execution on Desktop and Raspberry Pi 4 systems, (b) Scalability of <i>SecEdge</i> scheme with respect to vehicle density (c) Data-rate of <i>SecEdge</i> scheme with respect to the vehicle density	104
5.1	PUF and edge-computing based three layered network model for proposed PESPI scheme	109
5.2	Registration process for smart vehicles and edge node using CRP mechanism	112
5.3	Anonymous mutual authentication	113
5.4	Performance evaluation of PESPI: (a) Scalability with respect to vehicle density, comparison of PESPI with state-of-the-art schemes in terms of: (b) computation cost (ms), and (c) communication cost (bytes)	119
5.5	Simulation results of PESPI: (a) Selecting MNIT Jaipur region, India using OpenStreetMap, (b) Data receiving rate for application packets, (c) Packet delivery ratio for application packets, (d) Data receiving rate for authentication packets, (e) Packet delivery ratio for authentication packets, and (f) Physical layer overhead during message transmission	121
5.6	Layers and DIoV components of <i>SECURE</i> protocol	123
5.7	Network model of <i>SECURE</i> considering RSCN and drones as edge devices	124
5.8	Requests handling process of RSCN and drone during authentication	127
5.9	Mutual authentication between drone and RSCN	128
5.10	Mutual authentication between vehicle and RSCN	129
5.11	Experimental setup for the execution of <i>SECURE</i> algorithm	131
5.12	Computation cost (ms) comparison of <i>SECURE</i> with state-of-the-art scheme	132
5.13	Performance comparison of <i>SECURE</i> with state-of-the-art in terms of (a) Energy consumption (mJ), and (b) Communication cost (bits)	133
6.1	Processing of PUF-AEAD: Nonce and key generation, authentication tag generation	139
6.2	Graphical representation of securing sensor data using PUF-based hardware encryption using RPP as PUF device and ESP32-D0WD as hardware accelerator	140
6.3	Experimental setup for proposed method using ESP32-D0WD micro-controller, RPP, MPU6050 sensor module and Linux-based OS having Arduino IDE	146
6.4	The impact of increased data size on encryption time (μs)	147
6.5	Execution times (ms) for nonce generation, HMAC, and encryption key generation	148
6.6	Network performance analysis in terms of signal strength, latency, single noise and packet loss	149

List of Tables

1.1	Burrow-Abadi-Needham (BAN) logic rules	19
2.1	State-of-the-art for TPD-based authentication schemes: Public key-based and Identity-based	25
2.2	State-of-the-art for TPD-based authentication schemes: Session key-based and MAC-based .	26
2.3	State-of-the-art static batch verification schemes for IoV	27
2.4	State-of-the-art dynamic batch verification schemes for IoV	28
2.5	State-of-the-art cloud computing schemes in IoV	30
2.6	State-of-the-art authentication and secure searching schemes in IoV	31
2.7	State-of-the-art PUF-based authentication schemes in vehicular networks	33
2.8	State-of-the-art authentication schemes in DIOV	34
2.9	State-of-the-art authenticated encryption schemes to achieve confidentiality and integrity . .	37
2.10	State-of-the-art PUF-based schemes for secure key generation and authentication	37
2.11	State-of-the-art hardware implementation schemes for authenticated encryption	39
3.1	Adversary model: Detailed representation of attack vectors, descriptions, and implications .	46
3.2	List of notations and their explanations	47
3.3	Detailed security analysis of NoMAS	52
3.4	Security comparison of NoMAS with state-of-the-art schemes	53
3.5	Truth table for proVerif tool	55
3.6	Confidentiality verification results using ProVerif tool	56
3.7	Authentication test results using ProVerif tool	56
3.8	Execution time of different cryptographic functions	57
3.9	Cryptographic equations having number of operations required for NoMAS and state-of-the-art schemes	58
3.10	Complexity comparison of NoMAS with state-of-the-art schemes	59
3.11	Configuration of the network	60
3.12	Notations used in batch verification scheme for IoV	65
3.13	Security analysis of the proposed scheme	68
3.14	Security comparison of proposed scheme with state-of-the-art schemes	69
3.15	Cryptographic equations for the proposed scheme and state-of-the-art schemes	70
3.16	Time complexity comparison	71
3.17	Transmission overhead comparison of proposed scheme with state-of-the-art schemes	71
3.18	Energy consumption (mJ) for different schemes	72
3.19	Variables used in DyBatch and their descriptions	78
3.20	Security comparison of DyBatch with the state-of-the-art schemes	81
3.21	Specifications of NVIDIA Jetson Nano 4 GB and Raspberry Pi 4 4 GB	84
3.22	Execution time (ms) of each cryptographic operation on different platforms	84
3.23	Comparison of DyBatch based on the computation cost	84
3.24	Network parameters and their values	86

3.25	Comparison of DyBatch with state-of-the-art schemes based on the different factors	87
4.1	Required symbols and their explanation	92
4.2	Edge E_j database	94
4.3	V-cloud database	94
4.4	Security analysis for different schemes including the proposed <i>SecEdge</i> scheme	99
4.5	Authentication, confidentiality verification, privacy-preservation results using ProVerif	102
4.6	Computation cost (ms) comparison of <i>SecEdge</i> with state-of-the-art schemes	103
4.7	Comparison of search time complexity between <i>SecEdge</i> and state-of-the-art schemes	103
4.8	Experiments and results to evaluate security effectiveness	105
5.1	Required notations and their definitions	110
5.2	Security comparison between different schemes	115
5.3	Execution time for each cryptographic operation	119
5.4	Required parameters for PESPI and other state of the art schemes	119
5.5	Comparison of computation and communication overhead	120
5.6	Complexity for different authentication schemes	120
5.7	Configuration of the network	121
5.8	Notations and their explanations	125
5.9	Hardware specifications of drone, smart vehicle, and RSCN	130
5.10	Execution time (ms) of each cryptographic operation on different platforms	131
5.11	Cryptographic equations of vehicle, drone, and RSCN	131
5.12	Comparison of <i>SECURE</i> with state-of-the-art schemes	132
6.1	Security comparison of PUF-AEAD with state-of-the-art methods based on different primitives	143
6.2	Hardware specifications for ESP32-D0WD and Raspberry Pi Pico devices	145
6.3	Performance analysis of the proposed scheme in terms of RAM utilization, current consumption, and energy consumption	147
6.4	Comparison of PUF-AEAD based on the key generation and PUF's statistical properties	148

Glossary

- ADAS** Advanced Driver Assistance Systems.
- AEAD** Authenticated Encryption with Associated Data.
- AES** Advanced Encryption Standard.
- AODV** Adhoc On-demand Distance Vector.
- ASIC** Application-Specific Integrated Circuits.
- BAN** Burrows-Abadi-Needham.
- BLE** Bluetooth Low Energy.
- CK** Canetti-Krawczyk.
- CRL** Certificate Revocation List.
- CRP** Challenge-Response Pair.
- CRT** Chinese Remainder Theorem.
- CTR** Counter Mode.
- DoS** Denial-of-Service.
- DSRC** Dedicated Short-Range Communications.
- ECC** Elliptic Curve Cryptography.
- FPGA** Field-Programmable Gate Array.
- GCM** Galois/Counter Mode.
- HKU** Hard Key Updates.
- HMAC** Hash-Based Message Authentication Code.
- HSM** Hardware Security Module.
- IoMT** Internet of Medical Things.
- IoT** Internet of Things.

IoV Internet of Vehicles.

ITS Intelligent Transportation Systems.

IV Initialization Vector.

LDR Light Dependent Resistor.

M2P Map-to-Point.

MAC Message Authentication Code.

MCU Micro-Controller Unit.

MPU Microprocessor Unit.

NoMAS Novel MAC-based Authentication Scheme.

NS-2 Network Simulator 2.

OBD On-Board Diagnostics.

OBU On-Board Unit.

PFS Perfect Forward Secrecy.

PKG Private Key Generator.

PKI Public Key Infrastructure.

ProVerif Protocol Verification Tool.

PUF Physical Unclonable Function.

RA Registration Authority.

ROM Random Oracle Model.

RPP Raspberry Pi Pico.

RSA Rivest-Shamir-Adleman.

RSCN Roadside Connecting Nodes.

RSU Road Side Unit.

SHA Secure Hash Algorithm.

SKU Soft Key Updates.

SSE Searchable Symmetric Encryption.

SUMO Simulation of Urban Mobility.

SV Smart Vehicle.

TA Trusted Authority.

TCP Transmission Control Protocol.

TPD Tamper-Proof Device.

UAV Unmanned Aerial Vehicle.

UDP User Datagram Protocol.

UWB Ultra-Wideband.

V2P Vehicle-to-Pedestrian.

VANET Vehicular Ad-hoc Network.

V-cloud Vehicular Cloud.

V2I Vehicle-to-Infrastructure.

V2V Vehicle-to-Vehicle.

V2X Vehicle-to-Everything.

VID Vehicle Identity.

VuCs VANET using Clouds.

WSN Wireless Sensor Network.

XOR Exclusive OR.