UNIVERSITI PUTRA MALAYSIA

EFFICIENT KERBEROS AUTHENTICATION SCHEME FOR CROSS-DOMAIN SYSTEMS IN INDUSTRIAL INTERNET OF THINGS USING ECC

HAQI KHALID ISMAIL

FK 2022 41

EFFICIENT KERBEROS AUTHENTICATION SCHEME FOR CROSS-DOMAIN SYSTEMS IN INDUSTRIAL INTERNET OF THINGS USING ECC

By

HAQI KHALID ISMAIL

Thesis Submitted to the School of Graduated Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

December 2021

DEDICATION

In the name of Allah, Most Gracious, Most Merciful
This thesis dedicated to:
My beloved and supportive father for supporting and encouraging me to believe in myself. It was his wish, thus I insisted to make it come true.
My cherished mother a strong and gentle soul who taught me to trust Allah, believe in hard work and that so much could be done with little.
To my friends who have supported me throughout the process. I will always appreciate all they have done for me.

Abstract of thesis presented to the Senate of the Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

EFFICIENT KERBEROS AUTHENTICATION SCHEME FOR CROSS-DOMAIN SYSTEMS IN INDUSTRIAL INTERNET OF THINGS USING ECC

By

HAQI KHALID ISMAIL

December 2021

Chairman : Professsor Shaiful Jahari bin Hashim, PhD
Faculty : Engineering

The advent of Industry 4.0 has propelled the Industrial Internet of Things (IIoT) as one of the essential enabling technologies for its successful adoption and implementation. IIoT links devices and enables connection and access to the Internet, providing various manufacturing and industrial practices services. These services are usually supplied with network and Internet security inside a cloud-based environment. Inter-connectivity capabilities make it possible for devices to work collaboratively to significantly improve efficiency and productivity with the assistance of automation. However, machines from different domains collaborate on the same data and task, raising security and privacy concerns about cross-domain communications. Many existing schemes have been proposed trying to meet the security and functionality of the cross-domain systems. These existing schemes, however, rely on different types of cryptographic methods that usually have high computation complexity. In addition, the communication between each participant via the public channel must be comprehensively secured against eavesdropping, altering, tampering, and impersonation attacks. Cybercriminals can take advantage of insecure communication to perform attacks that lead to compromises and intrusions. These cyberattacks against industrial entities, for common attacks examples, Trojan Horses, replay and man-in-the-middle, can lead to security compromises including espionage, sabotage, and ransomware. Solutions for these cyber security problems and threats are still not satisfactory.

Furthermore, most of the current authentication schemes designed for IIoT connected devices rely on reliable and continuous network connectivity. The users of the IIoT connected devices should be able to authenticate and communicate even when the Internet connections are intermittent and not available. A new multi-factor authentication scheme is designed using the AES-ECC algorithm based on Kerberos workflow to establish secure, efficient, and lightweight communication between the user and the targeted IIoT devices to avoid the issues. ECC encrypts and transfers the private keys as AES private keys in the proposed scheme, while AES encrypts the plain text (communication data). The design combined symmetric key encryption (AES) for the message encryption with the asymmetric key encryption (ECC). This combination provides a secure key management mechanism and data hiding to provide strong encryption and decryption standards. The multi-factor credentials are proposed for secure identification and authentication based on the combination of username/password (something you know), smartcard (something you have), and fingerprint (biometric which you possess). To prove that the proposed design is suitable for IIoT, a new scheme is proposed namely a secure, efficient, and lightweight multi-factor authentication scheme for cross-domain IIoT systems (SELAMAT). In addition, a proof of concept is constructed to validate the proposed multi-factor Kerberos authentication using Java programming language. As an extension to the scheme for enabling users to authenticate to the IIoT connected devices while Internet access is unavailable, a new offline multi-factor authentication scheme for the automotive industry is proposed. The offline scheme utilizes a Time-based One-Time Password (TOTP) algorithm to allow users to authenticate to the vehicle without needing an Internet connection once they have registered online when Internet access is available. Furthermore, the proposed scheme's performance and complexity are evaluated using the JPBC cryptographic library. The proposed schemes have been validated using informal and formal security verification to compare the achieved security features against various attacks. The formal verification is performed using BAN logic to prove the security and mutual authentications. The evaluation of the security of the proposed scheme is based on SVO logic to verify the security of the informal method. Likewise, the widely used standard verification simulation tool AVISPA is used to verify that the scheme is secure against passive and active attacks. Finally, the performance and functionality of the proposed schemes are evaluated in terms of computation and communication cost. The results show that the proposed schemes outperform the previous cross-domain authentication schemes by 53% of computation cost and 65% of communication cost.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

SKEMA PENGESAHAN KERBEROS CEKAP UNTUK SISTEM DOMAIN SILANG DALAM INTERNET PERKARA INDUSTRI MENGGUNAKAN ECC

Oleh

HAQI KHALID ISMAIL

Disember 2021

Pengerusi : Profesor Shaiful Jahari bin Hashim, PhD
Fakulti : Kejuruteraan

Kemunculan Industri 4.0 telah mendorong Industri Internet Perkara (IIoT) sebagai salah satu teknologi pemboleh yang penting untuk penggunaan dan pelaksanaannya yang berjaya. IIoT menghubung peranti dan membolehkan sambungan dan capaian kepada Internet, menyediakan pelbagai perkhidmatan pembuatan dan amalan perindustrian. Perkhidmatan ini biasanya dibekalkan dengan keselamatan rangkaian dan Internet dalam persekitaran berasaskan awan. Keupayaan antara ketersambungan membolehkan peranti berfungsi secara kerjasama untuk meningkatkan kecekapan dan produktiviti dengan ketara dengan bantuan automasi. Walau bagaimanapun, mesin daripada domain yang berbeza bekerjasama pada data dan tugas yang sama, menimbulkan kebimbangan keselamatan dan privasi tentang komunikasi domain silang. Banyak skema sedia ada telah dicadangkan cuba memenuhi keselamatan dan kefungsian sistem domain silang. Skema sedia ada ini, bagaimanapun, bergantung pada pelbagai jenis kaedah kriptografi yang biasanya mempunyai kerumitan pengiraan yang tinggi. Selain itu, komunikasi antara setiap peserta melalui saluran awam mesti dilindungi secara menyeluruh daripada penyadapan, pengubahan, gangguan dan serangan penyamaran. Penjenayah siber boleh mengambil kesempatan daripada komunikasi yang tidak selamat untuk melakukan serangan yang membawa kepada kompromi dan pencerobohan. Serangan siber ini terhadap entiti perindustrian, untuk contoh serangan biasa, Trojan Horses, main semula dan orang tengah, boleh membawa kepada kompromi keselamatan termasuk pengintipan, sabotaj dan perisian tebusan. Penyelesaian untuk masalah dan ancaman keselamatan siber ini masih belum memuaskan

Tambahan pula, kebanyakan skema pengesahan semasa yang direka untuk peranti bersambung IIoT bergantung pada sambungan rangkaian yang boleh diharap dan berterusan. Pengguna peranti yang disambungkan IIoT harus dapat mengesahkan dan berkomunikasi walaupun sambungan Internet terputus-putus dan tidak tersedia. Skema pengesahan berbilang faktor baharu direka bentuk menggunakan algoritma AES-ECC berdasarkan aliran kerja Kerberos untuk mewujudkan komunikasi yang selamat, cekap

dan ringan antara pengguna dan peranti IIoT yang disasarkan untuk mengelakkan isu. ECC menyulitkan dan memindahkan kunci persendirian sebagai kunci persendirian AES dalam skema yang dicadangkan, manakala AES menyulitkan teks biasa (data komunikasi). Reka bentuk ini menggabungkan penyulitan kunci simetri (AES) untuk penyulitan mesej dengan penyulitan kunci asimetri (ECC). Gabungan ini menyediakan mekanisme pengurusan kunci yang selamat dan penyembunyian data untuk menyediakan standard penyulitan dan penyahsulitan yang kukuh. Bukti kelayakan berbilang faktor dicadangkan untuk pengenalan dan pengesahan selamat berdasarkan gabungan nama pengguna/kata laluan (sesuatu yang anda tahu), kad pintar (sesuatu yang anda miliki) dan cap jari (biometrik yang anda miliki). Demi untuk membuktikan reka bentuk yang dicadangkan sesuai untuk IIoT, satu skema baharu dicadangkan iaitu skema pengesahan berbilang faktor yang selamat, cekap dan ringan untuk sistem IIoT domain silang (SELAMAT). Di samping itu, bukti konsep dibina untuk mengesahkan pengesahan Kerberos berbilang faktor yang dicadangkan menggunakan bahasa pengaturcaraan Java. Sebagai lanjutan kepada skema untuk membolehkan pengguna membuat pengesahan kepada peranti yang disambungkan IIoT semasa capaian Internet tidak tersedia, skema pengesahan berbilang faktor luar talian baharu untuk industri automotif dicadangkan. Skema luar talian menggunakan algoritma Kata Laluan Satu Masa (TOTP) berasaskan Masa untuk membolehkan pengguna mengesahkan kenderaan tanpa memerlukan sambungan Internet apabila mereka telah mendaftar dalam talian apabila capaian Internet tersedia. Tambahan pula, prestasi dan kerumitan skema yang dicadangkan dinilai menggunakan perpustakaan kriptografi JPBC. Skema yang dicadangkan telah disahkan menggunakan pengesahan keselamatan tidak formal dan formal untuk membandingkan ciri keselamatan yang dicapai terhadap pelbagai serangan. Pengesahan rasmi dilakukan menggunakan logik BAN untuk membuktikan keselamatan dan pengesahan bersama. Penilaian keselamatan skema yang dicadangkan adalah berdasarkan logik SVO untuk mengesahkan keselamatan kaedah tidak formal. Begitu juga, alat simulasi pengesahan piawai yang digunakan secara meluas AVISPA digunakan untuk mengesahkan bahawa skema selamat terhadap serangan pasif dan aktif. Akhir sekali, prestasi dan kefungsian skema yang dicadangkan dinilai dari segi pengiraan dan kos komunikasi. Keputusan menunjukkan bahawa skema yang dicadangkan mengatasi skema pengesahan domain silang sebelumnya sebanyak 53% daripada kos pengiraan dan 65% daripada kos komunikasi.

ACKNOWLEDGEMENTS

First and foremost, solemn praise and humble gratitude “to Allah, the Almighty, for bestowing His blessings on me throughout the research work to its successful completion.

I want to express my deep and sincere gratitude to my research supervisor, **Dr. Shaiful Jahari Hashim,** for allowing me to conduct research and providing invaluable guidance throughout the research. His dynamism, vision, sincerity, and motivation have deeply inspired me. He has taught me the methodology to carry out the research and present the research works as clearly as possible. It was a great privilege and honor to work and study under his guidance. I am incredibly grateful for what he has offered me. I would also like to thank him for his friendship, empathy, and great sense of humor.

Besides my advisor, I would like to thank the rest of my thesis committee: **Dr. Sharifah Mumtazah Syed Ahmad** and **Dr. Fazirulhisyam Hashim,** for their encouragement, insightful comments, and challenging questions that helped me a great deal in finalizing this project within a limited time frame, which also helped me in doing a lot of Research and I came to know about so many new things for which I am thankful to them. My sincere and special thanks go to **Dr. Muhammad Akmal Chaudhary** for his patience, motivation, enthusiasm, and immense knowledge.

Last but not least, I am incredibly grateful to my parents for their care, love, prayers, and sacrifices to educate and prepare me for my future. Also, I express my thanks to my sisters, brother, and friends for their support and valuable prayers."

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Shaiful Jahari bin Hashim, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Sharifah Mumtazah binti Syed Ahmad Abdul Rahman, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Fazirulhisyam bin Hashim, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Muhammad Akmal Chaudhary, PhD
Associate Professor
College of Engineering and Information Technology
Ajman University (UAE)
(Member)

____

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 February 2022

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:	
Name of Chairman of Supervisory Committee:	Professor Dr. Shaiful Jahari bin Hashim
Signature:	
Name of Member of Supervisory Committee:	Associate Professor Dr. Sharifah Mumtazah binti Syed Ahmad Abdul Rahman
Signature:	
Name of Member of Supervisory Committee:	Associate Professor Dr. Fazirulhisyam bin Hashim
Signature:	
Name of Chairman of Supervisory Committee:	Associate Professor Dr. Muhammad Akmal Chaudhary

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
AAL	Authenticator Assurance Level
AES	Advanced Encryption Standard
API	Application Programming Interface
AS	Authentication Service
ATM	Automated Teller Machine
AVISPA	Automated "Validation of Internet Protocols and Applications
AWS	Amazon Web Services
BAN Logic	Burrows–Abadi–Needham Logic
BCA	Bridge Certificate Authority
BCA	Bridge Certificate Authorities
BDHP	Bilinear Diffie-Hellman Problem
BGP	Border Gateway Protocol
BLE	Bluetooth Low Energy
CA	Central Authority
CAN	Control Area Network
CAP	Constrained Application Protocol
CBC	Cipher Block Chaining
CDHP	Computational Diffie-Hellman Problem
CDS	Cross-domain Systems
CFB	Cipher Feed Back
CL-AtSe	Constraint Logic based Attack Searcher
CM	Cloud Manufacturing
CN	Check number

CPS	Cloud Provider Server
CPSs	Cyber-Physical Systems
CS	Cross-Server
CSP	Credential service provider
CTR	Counter
DAP	Directory Access Protocol
DES	Data Encryption Standard
DH	Diffie-Hellman
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial-of-Service
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECS	Elastic Compute Service
FIDO	Fast Identity Online
FAL	Federation Assurance Level
FIPS	Federal Information Processing Standard
FN	Fog Node
GCM	Galois Counter Mode
GF	Finite field or Galois field

GPS	Global Positioning System
HABE	Homomorphic Attribute-Based Encryption
HLPSL	High Level Protocol Specification Language
HMAC	Hash-Based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IAL	Identity Assurance Level
IBC	Identity-Based Cryptography
IBE	Identity-based encryption
ID	Identity
IDAS	Inter-Domain Authentication Scheme
IdP	Identity provider
IETF	Internet Engineering Task Force
IF	Intermediate Format
IIoT	Industrial Internet of Things
IMRs	Industrial Mobile Robots
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
IV	Initialization Vector
JPBC	Java Pairing Based Cryptography
JWE	JSON Web Encryption
KDC	Key Distribution Center
KGC	Key Generation Center
LDAP	Lightweight Directory Access Protocol
LDAP	Lightweight Directory Access Protocol.

MACs	Message Authentication Codes.
MD	Mobile Device.
MD5	Message-Digest Algorithm
MFA	Multi-Factor Authentication
MITM	Man-in-the-Middle
NB-IoT	NarrowBand-Internet of Things
NFC	Near-field Communication
NGOs	Non-government Organizations
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OF	Output Format
OFB	Output Feed Back
OFMC	On-the-Fly Model-Checker
OT	Operational Technology
OTP	One-Time Password
PAKE	Password Authenticated Key Exchange
PBE	Password-based Encryption
PIN	Personal Identification Number
PKG	Private-Key Generator
PKI	Public key Infrastructure
PPT	Probabilistic Polynomial-Time
PRNG	Pseudo-random Number Generation
ProVerif	Protocols Verifier
QoS	Quality of Service
RBAC	Role-Based Access Control

RFC	Request for Comments
RFID	Radio-Frequency Identification
RP	Relying Party
RSA	Rivest–Shamir–Adleman
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SATMC	SAT-based Model-Checker
SC	Smartcard
SEAL	Software-optimized Encryption Algorithm
SELAMAT	Secure, Efficient and Lightweight Cross-domain Multi-factor Authentication for Internet of Things (IoT)
SFA	Single-Factor Authentication
SHA	Secure Hash Algorithms
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SP	Service Provider
SSL	Secure Sockets Layer
SSO	Single Sign-On
SVO	Syverson-van Oorschot Logic
TA	Trusted Authority
TA4SP	Tree Automata based on Automatic Approximations
TAN	Transaction Authentication Number
TGS	Ticket Granting Server
TKT	Ticket
TLS	Transport Layer Security
TOTP	Time-based One-Time Password

TS	Timestamp
U2F	Universal 2nd Factor
UDP	User Datagram Protocol
UML	Unified Modelling Language
USB	Universal Serial Bus
VCA	Virtual Code Authentication
VPN	Virtual Private Network
ZKP	Zero Knowledge Proof

CHAPTER 1

INTRODUCTION

1.1 Background

While some regard "Industry 4.0" as one of many flashy words, automation and data sharing in the industrial sector (and many other industries) are becoming ever more interconnected and integrated into our digitized world, this is enabled in part by the extension of IoT and business networks (Lin et al. 2018). Thus, security is a primary concern in an Industry 4.0 application, including the difficulty of detecting vulnerabilities implemented during manufacturing (e.g., hardware Trojans and backdoors) (Estrela et al. 2019). Furthermore, cross-domain authentication is the bedrock of and critical to securing connectivity between different domains in a cloud setting (Yanyan Yang et al. 2019). In a distributed “network environment, where businesses and organizations have their resources to share, to discourage unauthorized users from accessing these standard services, organizations or service providers establish an authentication server, a large separate confidential domain for authorized users. However, a single autonomous trust domain cannot offer multiple” resources, necessitating multiple domains by users (W. Wang, Hu, and Liu 2018).

The cross-domain system helps to collaborate with multiple organizations from different regions using the Internet to access their data. The data can be distributed among multiple organizations in different geographical environments (Kaur, Kumar, and Batra 2019). The global population generates enormous amounts of data in organizations/institutes and devices combined with rapid technology growth. These confidential data can be exchanged with different users in various areas, including experts and service providers in various settings (Salehi, Rudolph, and Grobler 2019). Currently, data are owned by independent organizations, and different policies and security methods are used to prevent malicious and unwanted data access by insiders and outsiders. cross-domain connectivity is limited to explicit information sharing systems. Approaches for more comprehensive connectivity are dependent on central storage or synchronized cross-domain policies (Salehi, Rudolph, and Grobler 2019).

Similarly, an entity has its security frameworks and policies to secure its local infrastructure, and different organizations must apply across a range of heterogeneous security domains. A security domain consists of operators (persons, computers, and services) licensed with designated authority and administered security processes and policies. Although the institutions and resources will participate in a highly complex and flexible collaboration mechanism, it is not to be concluded that each of the two partnering security sectors has a direct relationship. Meanwhile, zero trust technologies claimed to solve perimeter security issues. The perimeter security concept assumes that information systems within a company's internal network are trustworthy, but those outside the organization are not. The zero-trust architecture avoids these weaknesses by not trusting any entity, inside or outside the organization's perimeter (Microsoft 2019;

Rose et al. 2020). A potential solution to this problem is finding some intermediate realms that act as authentication paths between the two different realms to collaborate (D. Zhang, Xu, and Li 2007).

1.2 Research Problem

In the cross-domain system, two institutions/industries authenticate using an authentication mechanism. Recently, cross-domain systems authentication has been quite attracted by researchers and scientists to establish secure communication between domains located in different locations with different security policy settings. Some of the issues are described below:

- Integrating"multiple platforms enable users to access multiple edge devices in different geographical locations. For example, In the public sector, the government has taken various initiatives to increase collaboration among government agencies and non-government organizations (NGOs) to provide better public service to citizens. So, practically, secure communication is still not established between domains located in different locations with different security policy settings results in high vulnerability to attacks (e.g., impersonation attack, DoS attacks, password guessing attack, and modification attack). Also, leakage of the user information could lead to tracking user transmission and may allow the opportunity to compute the session key to break into the system (Yang Yang et al. 2018),(Shen et al. 2020),(Xudong Jia et al. 2020). For example, Microsoft's implementations of the Kerberos protocol may allow an attacker to obtain that secret key and bypass the authentication system, as reported in (Australian Cyber Security Centre (ACSC) 2020). A second primary class of attack on the Kerberos protocols involves an intruder recording login dialogs to mount a password-guessing assault. When a user requests a ticket-granting ticket, the reply is returned encrypted with the key, a key derived by a publicly known algorithm from the user's password. A guess at the user's password can be confirmed by calculating key and using it to decrypt the recorded message. An intruder who has recorded the login dialogs has the probability of finding several new passwords; empirically, users do not pick strong passwords unless forced to (Merco, Biron, and Pisu 2018). Cross-domain systems deal with many resource-constrained devices, and the traditional Kerberos protocol is highly suffering from high computation costs in the central authority, which leads to delay in the authentication requests. Additionally, IIoT devices cannot perform extensive computation due to the computation capabilities of IIoT devices. Furthermore, some cryptographic algorithms used in existing schemes, such as bilinear pairing, PKI, and IBC, require high computation that is not suitable to the IIoT environment (Xudong Jia et al. 2020) (Quanxin Zhang et al. 2018).

- Connected vehicles are another revolution of the automotive industry, "and car-sharing applications are an example. However, connectivity shortcoming in areas with no network availability makes vehicle sharing or any IoT-connected device undesirable. For example, the Guardian journalist Kari Paul turned into a cautionary tale about the IoT-connected car. Paul had rented a car through a local car-sharing service called GIG Car Share and planned to spend the weekend in a more rural part of the state about three hours north of Oakland. But on Sunday, she was left stranded on an unpaved road when the car's telematics system lost its cell signal. The rented car refused to move (Gitlin 2020) (Kumar et al. 2020). Therefore, accessing the vehicle in such network connectivity shortcoming makes developing IoT-connected vehicles undesirable. However, offline authentication—used for in-person transactions where access is inaccessible or unnecessary—must provide a way of checking that the person claiming their identity is whom they claim to be without reference to other systems (e.g., remote identity databases and online services) and, if possible, that the credentials they present are genuine.

”On the other hand, “vulnerability scanning interference, network eavesdropping, attacks, service system, and database attacks could all be used by adversaries to disrupt networks, posing a threat to the entire industry. Replay attacks are one of the many steppingstones for car hacking. Replay attacks, in general, are when a malicious user “sniffs” out a signal between two parties. The receiver will verify the sender as a legitimate user; while this exchange is safe, this is where the malicious user comes into play.” The malicious user uses the “sniffed” signal and mimics the signal to the original receiver. In turn, it makes the receiver think that this is the original sender, but the malicious user gains access to unauthorized information using the “replay” of the authenticated user’s signal (Dibaei et al., 2019; Merco, Biron, and Pisu 2018). Also, if the adversary successfully computed the session key, they would get into the targeted server to alter or modify the data and make the service undesirable.”

1.3 Research Significance and Objectives

This research offers the reader a deeper insight into the authentication schemes in cross-domain and appropriate solutions for their needs and requirements. Also, if the research goals are achieved, this work will hopefully benefit several different parties/healthcare institutions and industries. However, experts, industries, and factories will benefit from this work. It also offers an efficient way to share resources/services among cross-domain, such as physicians, workers, and nurses, ensures confidentiality, and protects data integrity. The proposed multi-factor authentication scheme will provide secure exchanging services and robust security workflow for cross-domain entities. The proposed scheme will be suitable for industry 4.0 entities (healthcare institutions, financial institutions, companies, and factories).

1. Propose a multi-factor authentication scheme based-Kerberos workflow using the AES-ECC algorithm to cross-domain the fog computing system in Industrial IoT.
2. Propose an online and offline authentication scheme using Time-based One-Time Password (TOTP) for cross-domain systems in the automotive industry.

1.4 Research Contributions

1. **A cross-domain multi-factor authentication scheme for fog computing in industrial IoT:** This contribution integrates the proposed design into the fog computing environment for cross-domain communication. The scheme intends to improve security and establish secure communication between edge devices and fog nodes. The SELAMAT scheme uses the AES-ECC algorithm to design an efficient key management system. AES (Symmetric Key Encryption Scheme) for the ECC Message Encryption (Asymmetric Key Encryption Scheme) for the Secure Key Management mechanism is combined with data hiding to provide strong encryption and decryption requirements by using the advantages of both the cryptographic schemes. With the proposed MFA, three types of factors are used: Username/Password (something you know), smart card (something you have), and biometric (fingerprint you possess)."

   The proposed MFA secures the user information from password guessing attacks, session attacks, and impersonation attacks. It provides layered security, making accessing the fog node more difficult for unauthorized users to a target such as the physical location, device, network, application, or database. So, ECC provides the efficient key management mechanism at the beginning of the session establishment for the communication process to start; hence, for the AES key encrypted by ECC and transmitted for data communication, there is no need to send private information secret key before communication." Symmetrical encryption algorithm AES encryption speed is fast and can be suited for encryption of long plaintext. The ECC encrypts the messages using the ECC key to avoid unauthorized users decrypting the messages. ECC creates a public and private key to encrypt the messages. ECC proves to be a better solution as compared to other encryption algorithms. It is used to create smaller, faster, and more efficient cryptographic keys. ECC is more suitable for cross-domain systems where the data is more confidential. It uses a minor key size and low computational system requirements. "By reducing the size of the key involved, the computational efficiency can be improved. The security of the proposed contribution was analysed and verified using the AVISPA tool against passive and active attacks. Also, the BAN logic is used to verify the secure mutual authentication between the edge-user and the fog node server." Finally, the performance of the proposed scheme is evaluated using the computation cost and communication cost."

2. **An online and offline cross-domain multi-factor authentication for IoT applications in the automotive industry:** To improve the efficiency of the industrial IoT, the first contribution is extended to propose an authentication scheme using the combination of AES-ECC algorithm due to the adequate performance of the algorithm itself to improve the automotive industry. IoT-connected cars have been widely introduced to the community with a new development of the industrial IoT in this environment. Therefore, IIoT connected cars are resource-constrained devices with low power and computing capacity. Also, the current development of these cars is produced with continuous network connection requirements, which must always be

there for Internet services. The Internet service cannot be available in certain places since the cars need a continuous network connection.

Therefore, we propose an online and offline multi-factor authentication scheme for the IIoT application in the automotive industry. The scheme also utilizes the AES-ECC algorithm based on Kerberos workflow for secure cross-domain online booking. To enable the user to authenticate to the vehicle in offline mode, the Time one-time password (TOTP) algorithm is used by adding an offline phase between the user and the vehicle using a mobile phone. The authentication scheme comprises five phases, i.e., setup, vehicle registration, server registration, booking, and offline authentication. The user in this scheme must enter a username, password, and TOTP using their mobile phone with biometric recognition support (Fingerprint). First, the user and the server must be registered with a central authority. Later, if the user wants to book the vehicle, they will apply for the booking. After successful booking, the user will authenticate to the vehicle without an Internet connection since the user will be provided with TOTP. The proposed contribution shows a lightweight performance due to the AES-ECC advantages in terms of complexity. It also enables the user to authenticate to the vehicle offline, which means that there is no need for Internet when the network connection is unavailable. “However, the proposed scheme security is analysed against attacks using the well-known AVISPA tool. Also, SVO logic is used for formal security verification to verify the security of the proposed scheme. Finally, the scheme's complexity in terms of computation and communication cost will be evaluated against other authentication schemes.”

1.5 Research Scope

The research mainly focuses on the environment of industry 4.0 in general and industrial IoT while excluding the other subtopics of “Industry 4.0, such as cyber-physical systems or the IIoT as the only field.” The thesis focuses on the security and privacy of industrial IoT authentication. The study provides security against various known attacks such as replay attacks, impersonation attacks, known key attacks, offline guessing attacks, MiTM attacks, insider attacks, and DoS attacks. Also, part of the study was the privacy features like anonymity, forward secrecy, untraceability, confidentiality, and integrity. This thesis addressed these issues and proposed a secure authentication scheme that meets the stated requirements. This study has selected cross-domain authentication as the main scope of the study. The authentication of cross-domain systems was categorized as centralized and decentralized to achieve different security goals and functions.

Hence, it focuses on the need to research the centralized authentication methods construction due to the industrial platforms for achieving trustworthiness between two entities they never met before. Researchers designed many authentication methods with different structures of user-related information such as single-factor authentication, two-factor authentications. The third type of authentication is multi-factor authentication which is the scope of this study. The multi-factor authentication enables the developers to use various identifications related to the user to increase the security robustness. This research uses four types of identifications; three contributions are already stated previously. However, this research proposes a multi-factor authentication scheme for cross-domain systems located in different geographical locations. Three types of factors are used in this research: password/username, smartcard, and fingerprint as user biometric. The purpose, in general, is to increase security strength and establish trust and secure communication between entities with different security policies and locations. The research further focuses on reducing the communication and computation costs by utilizing the AES-ECC method. In addition, to improve the efficiency of the industrial IoT environment, the study also aimed to propose an online and offline multi-factor authentication for secure communication and enable the users to authenticate with industrial IoT vehicles in offline mode. This scheme can work offline when the Internet services are unavailable by using mobile phones and TOTP generated by the vehicle. Finally, better security and efficiency performance is expected. The scope mapping of the research is illustrated in Figure 1.1."

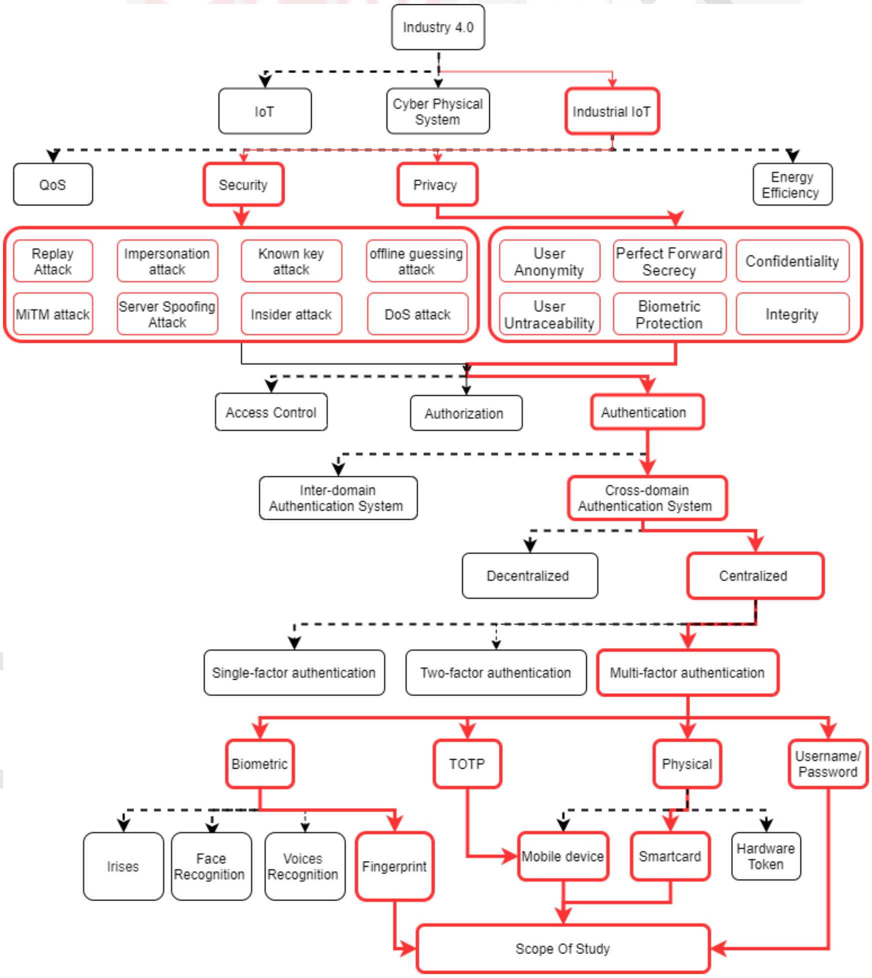

Figure 1.1 : The Scope of the Research

1.6 Thesis Organization

In Figure 1.2., the organization of the thesis is shown and is described in this section. The background of the study and the research problem is stated in this chapter. Also, the chapter outlines the objectives and the significance of the study. Subsequently, the main contributions and the scope of the study are highlighted as well. Chapter 2 outlines the background on the IIoT and industrial IoT environment. Additionally, a complete description of the cross-domain authentication systems and authentication structure types are shown. The chapter also reviews and analyses the previous studies on cross-domain authentication systems to identify the issues and the lessons learned from the analysis.

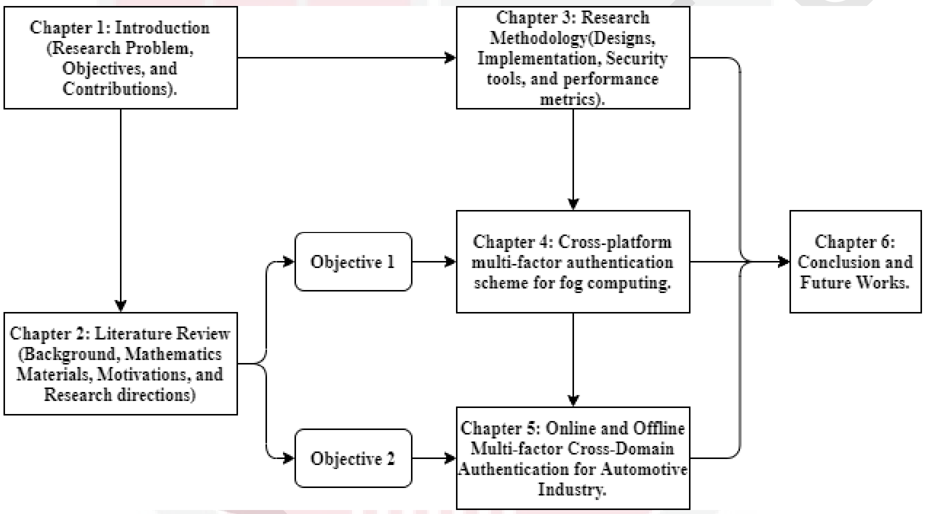

Figure 1.2 : Thesis Organization Chart

Chapter 3. presents the methodology of the research designs and the problem formulation. The proposed designs and their implementation and the security and verification tools are highlighted in the chapter. Likewise, the performance metrics used to evaluate the authentication schemes are described. Chapter 4 Introduced the study's first objective and an in-depth discussion on the proposed scheme. Also, the security analysis of the scheme was verified informally and formally to discuss the prevention of attacks. The performance evaluation of the scheme is compared against other schemes. Chapter 5., the second objective is presented, and the scheme's design is highlighted. Also, the methodology design, the scheme description, and its security analysis and verification are illustrated. The performance evaluation of the scheme is also outlined. Finally, the research and the future works for further improvement in industry 4.0 are highlighted.

REFERENCES

Abdelghaffar, Hossam M., Maha Elouni, Youssef Bichiou, and Hesham A. Rakha. 2020. "Development of a Connected Vehicle Dynamic Freeway Variable Speed Controller." *IEEE Access* 8: 99219–26. https://doi.org/10.1109/ACCESS.2020.2995552.

Abu Talib, Manar, Sohail Abbas, Qassim Nasir, and Mohamad Fouzi Mowakeh. 2018. "Systematic Literature Review on Internet-of-Vehicles Communication Security." *International Journal of Distributed Sensor Networks* 14 (12). https://doi.org/10.1177/1550147718815054.

Addobea, Abigail Akosua, Jun Hou, and Qianmu Li. 2020. "MHCOOS: An Offline-Online Certificateless Signature Scheme for M-Health Devices." *Security and Communication Networks* 2020. https://doi.org/10.1155/2020/7085623.

Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic. 2018. "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams." *IEEE Transactions on Dependable and Secure Computing* 15 (5): 840–52. https://doi.org/10.1109/TDSC.2016.2616861.

Akram, Muhammad Arslan, Zahid Ghaffar, Khalid Mahmood, Saru Kumari, Kadambri Agarwal, and Chien Ming Chen. 2020. "An Anonymous Authenticated Key-Agreement Scheme for Multi-Server Infrastructure." *Human-Centric Computing and Information Sciences* 10 (1). https://doi.org/10.1186/s13673-020-00227-9.

Alessandro Armando, David Basin, Jorge Cuellar, Michael Rusinowitch and Luca Viganò. 2001. "The High Level Protocol Specification Language Deliverable Details." *AVISPA*.

Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Borhanuddin M Ali. 2014. "An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks." *IEEE Region Symposium*, 502–7.

Almuhaideb, Abdullah, Bala Srinivasan, Phu Dung Le, Campbell Wilson, and Vishv Malhotra. 2012. "Analysis of Mobile Authentication Protocols by SVO Logic." *ACM International Conference Proceeding Series*, 126–34. https://doi.org/10.1145/2490428.2490446.

Altigani, Abdelrahman, Muawia Abdelmagid, and Bazara Barry. 2016. "Analyzing the Performance of the Advanced Encryption Standard Block Cipher Modes of Operation: Highlighting the National Institute of Standards and Technology Recommendations." *Indian Journal of Science and Technology* 9 (28). https://doi.org/10.17485/ijst/2016/v9i28/97795.

Arena, Fabio, Giovanni Pau, and Alessandro Severino. 2020. “A Review on IEEE 802.11p for Intelligent Transportation Systems.” *Journal of Sensor and Actuator Networks* 9 (2): 1–11. https://doi.org/10.3390/jsan9020022.

Arias-Cabarcos, Patricia, Christian Krupitzer, and Christian Becker. 2019. “A Survey on Adaptive Authentication.” *ACM Computing Surveys* 52 (4). https://doi.org/10.1145/3336117.

Aslam, Muhammad Umair, Abdelouahid Derhab, Kashif Saleem, Haider Abbas, Mehmet Orgun, Waseem Iqbal, and Baber Aslam. 2017. “A Survey of Authentication Schemes in Telecare Medicine Information Systems.” *Journal of Medical Systems* 41 (1). https://doi.org/10.1007/s10916-016-0658-3.

Australlian Cyber Security Centre (ACSC). 2020. Fundamentals of Cross-domain Solutions.

Azeez, Nureni Ayofe, and Charles Van der Vyver. 2019. “Security and Privacy Issues in E-Health Cloud-Based System: A Comprehensive Content Analysis.” *Egyptian Informatics Journal* 20 (2): 97–108. https://doi.org/10.1016/j.eij.2018.12.001.

B, Veronika Kuchta, Gaurav Sharma, and Rajeev Anand Sahu. 2018. “Multi-Party (Leveled) Homomorphic Encryption on Identity-Based and Attribute-Based Settings.” In *International Conference on Information Security and Cryptology*, 10779:71–92. Springer International Publishing. https://doi.org/10.1007/978-3-319-78556-1.

Bagga, Palak, Ashok Kumar Das, Mohammad Wazid, Joel J.P.C. Rodrigues, and Youngho Park. 2020. “Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges.” *IEEE Access* 8: 54314–44. https://doi.org/10.1109/ACCESS.2020.2981397.

Bajpai, Durgesh, Manu Vardhan, Sachin Gupta, Ravinder Kumar, and Dharmender Singh Kushwaha. 2012. “Security Service Level Agreements Based Authentication and Authorization Model for Accessing Cloud Services.” *Advances in Intelligent Systems and Computing* 176 AISC (VOL. 1): 719–28. https://doi.org/10.1007/978-3-642-31513-8_73.

Bandyopadhyay, Debasis, and Jaydip Sen. 2011. “Internet of Things: Applications and Challenges in Technology and Standardization.” *Wireless Personal Communications* 58 (1): 49–69. https://doi.org/10.1007/s11277-011-0288-5.

Barbero, Ángela I., Eirik Rosnes, Guang Yang, and Øyvind Ytrehus. 2014. “Near-Field Passive RFID Communication: Channel Model and Code Design.” *IEEE Transactions on Communications* 62 (5): 1716–27. https://doi.org/10.1109/TCOMM.2014.032314.130723.

Bellare, Mihir, Joe Kilian, and Phillip Rogaway. 1994. “The Security of Cipher Block Chaining.” In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 839 LNCS:341–58. https://doi.org/10.1007/3-540-48658-5_32.

Bhuiyan, Md Zakirul Alam, Sy Yen Kuo, Jiannong Cao, and Guojun Wang. 2020. “Guest Editorial: Trustworthiness in Industrial Internet of Things Systems and Applications.” *IEEE Transactions on Industrial Informatics* 16 (9): 6079–82. https://doi.org/10.1109/TII.2020.2983387.

Blanchet, Bruno. 2016. “Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif.” *Foundations and Trends® in Privacy and Security* 1 (1–2): 1–135. https://doi.org/10.1561/3300000004.

Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. 2019. “A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues.” *Telematics and Informatics* 36 (May 2018): 55–81. https://doi.org/10.1016/j.tele.2018.11.006.

Castiglione, Aniello, Francesco Palmieri, Chin Ling Chen, and Yao Chung Chang. 2016. “A Blind Signature-Based Approach for Cross-domain Authentication in the Cloud Environment.” *International Journal of Data Warehousing and Mining* 12 (1): 34–48. https://doi.org/10.4018/IJDWM.2016010103.

Chellappan, V., and K. M. Sivalingam. 2016. *Security and Privacy in the Internet of Things*. *Internet of Things: Principles and Paradigms*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-805395-9.00010-1.

Chen, Chien Ming, Yanyu Huang, King Hang Wang, Saru Kumari, and Mu En Wu. 2020. “A Secure Authenticated and Key Exchange Scheme for Fog Computing.” *Enterprise Information Systems* 7575. https://doi.org/10.1080/17517575.2020.1712746.

Chen, Chien Ming, Bin Xiang, Yining Liu, and King Hang Wang. 2019a. “A Secure Authentication Protocol for Internet of Vehicles.” *IEEE Access* 7 (c): 12047–57. https://doi.org/10.1109/ACCESS.2019.2891105.

Chen, Chien Ming, Bin Xiang, Yining Liu, and King Hang Wang. 2019b. “A Secure Authentication Protocol for Internet of Vehicles.” *IEEE Access* 7: 12047–57. https://doi.org/10.1109/ACCESS.2019.2891105.

Chen, Liqun, Hoon Wei Lim, and Guomin Yang. 2013a. “Cross-domain Password-Based Authenticated Key Exchange.” In *IEEE International Conference on Computer Communications (INFOCOM)*, 1–31.

Chen, Liqun, Hoon Wei Lim, and Guomin Yang. 2013b. “Cross-domain Password-Based Authenticated Key Exchange Revisited.” In *Proceedings - IEEE INFOCOM*. https://doi.org/10.1109/INFCOM.2013.6566895.

Chevalier, Y, L Compagna, J Cuellar, and J Mantovani. 2004. "A High-Level Protocol Specification Language for Industrial Security-Sensitive Protocols ∗." *Proc. SAPS'04*, no. May 2014.

Choudhary, Karanjeet, Gurjot Singh Gaba, Ismail Butun, and Pardeep Kumar. 2020. "Make-It—a Lightweight Mutual Authentication and Key Exchange Protocol for Industrial Internet of Things." *Sensors (Switzerland)* 20 (18): 1–21. https://doi.org/10.3390/s20185166.

Cigoj, Primož, and Borka Jerman Blažič. 2015. "An Authentication and Authorization Solution for a Multiplatform Cloud Environment." *Information Security Journal* 24 (4–6): 146–56. https://doi.org/10.1080/19393555.2015.1078424.

D. M'Raihi, S. Machani, M. Pei, J. Rydell. 2011. "TOTP: Time-Based One-Time Password Algorithm." Internet Engineering Task Force (IETF).

Darrel, R, and A Scott. 2004. *Guide to Elliptic Curve Cryptography*. *Guide to Elliptic Curve Cryptography*. Springer Science \& Business Media. https://doi.org/10.1007/b97644.

Delvaux, Jeroen, Roel Peeters, Dawu Gu, and Ingrid Verbauwhede. 2015. "A Survey on Lightweight Entity Authentication with Strong PUFs." *ACM Computing Surveys*. https://doi.org/10.1145/2818186.

Dhillon, Parwinder Kaur, and Sheetal Kalra. 2017. "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, Parwinder Kaur and Sheetal Kalra. 2018. "Multi-Factor User Authentication Scheme for IoT-Based Healthcare Services." *Journal of Reliable Intelligent Environments*. https://doi.org/10.1007/s40860-018-0062-5.

Dhillon, Parwinder Kaur and Sheetal Kalra. 2019. "A Secure Multi-Factor ECC Based Authentication Scheme for Cloud-IoT Based Healthcare Services." *Journal of Ambient Intelligence and Smart Environments* 11 (2): 149–64. https://doi.org/10.3233/AIS-190516.

Dibaei, Mahdi, Xi Zheng, Kun Jiang, Sasa Maric, Robert Abbas, Shigang Liu, Yuexin Zhang, et al. 2019. "An Overview of Attacks and Defences on Intelligent Connected Vehicles." *ArXiv*, 1–36.

Dmitrienko, Alexandra, and Christian Plappert. 2017. "Secure Free-Floating Car Sharing for Offline Cars." In *CODASPY 2017 - Proceedings of the 7th ACM Conference on Data and Application Security and Privacy*, 349–60. https://doi.org/10.1145/3029806.3029807.

Dmitrienko, Alexandra, Ahmad-reza Sadeghi, Sandeep Tamrakar, and Christian Wachsmann. 2012. "SmartTokens : Delegable Access Control With." In *International Conference on Trust and Trustworthy Computing (TRUST)*, 1–23.

Dong, Guishan, Jian Bai, Yuxiang Chen, Peng Zhang, Jia Fan, and Feng Li. 2019. "Anonymous Cross-domain Authentication Scheme for Medical PKI System." *ACM International Conference Proceeding Series*, no. 30. https://doi.org/10.1145/3321408.3321574.

Dunne, J Paul, and Ron P Smith. 2010. "The OAuth 1.0 Protocol OAuth." *Internet Engineering Task Force (IETF)*.

Edward, Schwartzman. 2018. "Your World. My BMW. The New-Generation App for BMW Customers. Now Available in 30 European Markets, China and Korea." BMW Press and Public Relations. 2018. https://doi.org/10.4324/9781315126630-8.

El-Hajj, Mohammed, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. 2019. "A Survey of Internet of Things (IoT) Authentication Schemes." *Sensors (Switzerland)* 19 (5): 1–43. https://doi.org/10.3390/s19051141.

Estrela, Vania Vieira, Universidade Federal Fluminense, Ana Carolina, Borges Monteiro, and Khelassi Abdeldjalil. 2019. "Health 4.0 as an Application of Industry 4.0 in Healthcare Services and Management." *Medical Technologies Journal* 2 (January): 262–76. https://doi.org/10.26415/2572-004X-vol2iss1p262-276.

Evans, Brandon. 2020. "Information Security Reading Room Firebase : Google Cloud ' s Evil Twin." Firebase: Google Cloud's Evil Twin - Excerpt. 2020. https://www.sans.org/blog/firebase-google-cloud-s-evil-twin-condensed/.

Ferdous, Md Sadek, and Ron Poet. 2015. "Managing Dynamic Identity Federations Using Security Assertion Markup Language." *Journal of Theoretical and Applied Electronic Commerce Research* 10 (2): 53–76. https://doi.org/10.4067/S0718-18762015000200005.

Ferrag, Mohamed Amine, Leandros A. Maglaras, Helge Janicke, Jianmin Jiang, and Lei Shu. 2017. "Authentication Protocols for Internet of Things: A Comprehensive Survey." *Security and Communication Networks* 2017. https://doi.org/10.1155/2017/6562953.

Fraga-Lamas, Paula, Tiago M. Fernández-Caramés, and Luis Castedo. 2017. "Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways." *Sensors (Switzerland)* 17 (6). https://doi.org/10.3390/s17061457.

Fu, Chenglong, Tassadit Kezmane, Xiaojiang Du, Yat Fu, and Colin Morrisseau. 2018. "An Location-Aware Authentication Scheme for Cross-domain Internet of Thing Systems." *2018 International Conference on Computing, Networking and Communications, ICNC 2018*, 452–56. https://doi.org/10.1109/ICCNC.2018.8390312.

Ganesh, Anirudh Ramaswamy, P. Naveen Manikandan, S. Pl Sethu, R. Sundararajan, and K. Pargunarajan. 2011. "An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity Based Wireless Sensor Networks." In *International Conference on Recent Trends in Information Technology, ICRTIT 2011*, 1209–14. https://doi.org/10.1109/ICRTIT.2011.5972351.

Gitlin, Jonathan M. 2020. "Driver Stranded after Connected Rental Car Can't Call Home." *The Guardian*, 2020. https://arstechnica.com/cars/2020/02/driver-stranded-after-connected-rental-car-cant-call-home/.

Grassi, Paul A., Michael E. Garcia, and James L. Fenton. 2017. "Digital Identity Guidelines." *National Institute of Standards and Technology Special Publication* 800 (63): 75.

Greenberg, Andy. 2020. "How 30 Lines of Code Blew Up a 27-Ton Generator." WIRED. 2020. https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.

Gueron, Shay, Simon Johnson, and Jesse Walker. 2011. "Sha-512/256." In *Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011*, 354–58. https://doi.org/10.1109/ITNG.2011.69.

Guo, Cong, Zijian Zhang, Liehuang Zhu, Yu an Tan, and Zhen Yang. 2015. "Scalable Protocol for Cross-domain Group Password-Based Authenticated Key Exchange." *Frontiers of Computer Science* 9 (1): 157–69. https://doi.org/10.1007/s11704-014-4124-4.

Gupta, Daya Sagar, S. K. Hafizul Islam, Mohammad S Obaidat, Pandi Vijayakumar, Neeraj Kumar, and Yohan Park. 2019. "A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for IIoT Environments." *Security and Communication Networks* 2019: 1–10. https://doi.org/10.1155/2019/7871067.

Haas, Sarah, Andreas Wallner, Ronald Toegl, Thomas Ulz, and Christian Steger. 2017. "A Secured Offline Authentication Approach for Industrial Mobile Robots." In *IEEE International Conference on Automation Science and Engineering*, 2017-Augus:308–13. https://doi.org/10.1109/COASE.2017.8256121.

Habib, Sheikh Mahbub, Sebastian Ries, and M Max. 2014. "A Virtual Bridge Certificate Authority-Based Cross- Domain Authentication Mechanism for Distributed Collaborative Manufacturing Systems." *Security and Communication Networks*, 1–18. https://doi.org/10.1002/sec.

Hamzah F. Zmezm, Shaiful Jahari Hashim, Aduwati Sali, Kamal Ali Alezabi. 2015. "Pre-Authentication Design for Seamless and Secure Handover in Mobile WiMAX." *International Review on Computers and Software* 10 (7).

Han, Daoqi, Yueming Lu, Xiaofeng Du, and Jiefu Gan. 2018. "Offline Authentication Scheme Based on Blockchain Technology for Smart Lock." In *ACM International Conference Proceeding Series*, 384–90. https://doi.org/10.1145/3291842.3291893.

Hao, Shen Gang, Li Zhang, and Ghulam Muhammad. 2013. "A Union Authentication Protocol of Cross-domain Based on Bilinear Pairing." *Journal of Software* 8 (5): 1094–1100. https://doi.org/10.4304/jsw.8.5.1094-1100.

Hardjono, Thomas. 2019. "A Federated Authorization Framework for Distributed Personal Data & Digital Identity." *The Computing Research Repository (CoRR)*, 1–15.

Hathaliya, Jigna J., Sudeep Tanwar, Sudhanshu Tyagi, and Neeraj Kumar. 2019. "Securing Electronics Healthcare Records in Healthcare 4.0: A Biometric-Based Approach." *Computers and Electrical Engineering* 76: 398–410. https://doi.org/10.1016/j.compeleceng.2019.04.017.

He, Debiao, Neeraj Kumar, Huaqun Wang, Lina Wang, Kim Kwang Raymond Choo, and Alexey Vinel. 2018. "A Provably-Secure Cross-domain Handshake Scheme with Symptoms-Matching for Mobile Healthcare Social Network." *IEEE Transactions on Dependable and Secure Computing* 15 (4): 633–45. https://doi.org/10.1109/TDSC.2016.2596286.

He, Wu, and Lida Xu. 2015. "A State-of-the-Art Survey of Cloud Manufacturing." *International Journal of Computer Integrated Manufacturing* 28 (3): 239–50. https://doi.org/10.1080/0951192X.2013.874595.

Heys, Howard M. 2003. "Analysis of the Statistical Cipher Feedback Mode of Block Ciphers." *IEEE Transactions on Computers* 52 (1): 77–92. https://doi.org/10.1109/TC.2003.1159755.

Hirsch, Frederick, Rob Philpott, R S A Security, John Hughes, Atos Origin, Hal Lockhart, B E A Systems, et al. 2005. "Security and Privacy Considerations for the OASIS Security Assertion Markup." *OASIS Security Services (SAML) TC*, no. March: 1–33.

Hou, Jia Li, and Kuo Hui Yeh. 2015. "Novel Authentication Schemes for IoT Based Healthcare Systems." *International Journal of Distributed Sensor Networks* 2015 (ii). https://doi.org/10.1155/2015/183659.

Hu, Junyan, Parijat Bhowmick, Farshad Arvin, Alexander Lanzon, and Barry Lennox. 2020. "Cooperative Control of Heterogeneous Connected Vehicle Platoons: An Adaptive Leader-Following Approach." *IEEE Robotics and Automation Letters* 5 (2): 977–84. https://doi.org/10.1109/LRA.2020.2966412.

Ibrahim, Maged Hamada. 2016. "Octopus: An Edge-Fog Mutual Authentication Scheme." *International Journal of Network Security* 18 (6): 1089–1101.

Iorga, Michaela, Larry Feldman, Robert Barton, Michael J. Martin, Nedim Goren, and Charif Mahmoudi. 2011. "Fog Computing Conceptual Model." *NIST Special Publication 500-325*. Vol. 1. https://doi.org/10.2174/2210677411101020169.

Iovino, Angelo {De Caro} and Vincenzo. 2011. "JPBC: Java Pairing Based Cryptography." In *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*, 850–55. IEEE.

Jia, Xiaoying, Debiao He, Neeraj Kumar, and Kim Kwang Raymond Choo. 2019. "Authenticated Key Agreement Scheme for Fog-Driven IoT Healthcare System." *Wireless Networks* 25 (8): 4737–50. https://doi.org/10.1007/s11276-018-1759-3.

Jia, Xudong, Ning Hu, Shen Su, Shi Yin, Yan Zhao, Xinda Cheng, and Chi Zhang. 2020. "IRBA: An Identity-Based Cross-domain Authentication Scheme for the Internet of Things." *Mdpi Electronics*.

Jiang, Qi, Ning Zhang, Jianbing Ni, Jianfeng Ma, Xindi Ma, and Kim Kwang Raymond Choo. 2020. "Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles." *IEEE Transactions on Vehicular Technology* 69 (9): 9390–9401. https://doi.org/10.1109/TVT.2020.2971254.

Jonnada, Srikanth, Ram Dantu, Pradhumna Shrestha, Ishan Ranasinghe, and Logan Widick. 2018. "An Oauth-Based Authorization Framework for Access Control in Remote Collaboration Systems." *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, 38–44. https://doi.org/10.1109/NCS.2018.00011.

Karuppiah, Marimuthu, and R. Saravanan. 2015. "A Secure Authentication Scheme with User Anonymity for Roaming Service in Global Mobility Networks." *Wireless Personal Communications* 84 (3): 2055–78. https://doi.org/10.1007/s11277-015-2524-x.

Katsikas, Sokratis, and Vasileios Gkioulos. 2020. "Security, Privacy, and Trustworthiness of Sensor Networks and Internet of Things." *Sensors (Switzerland)* 20 (14): 1–5. https://doi.org/10.3390/s20143846.

Kaur, Harmanjeet, Neeraj Kumar, and Shalini Batra. 2019. "ClaMPP : A Cloud-Based Multi-Party Privacy Preserving Classification Scheme for Distributed Applications." *The Journal of Supercomputing* 75 (6): 3046–75. https://doi.org/10.1007/s11227-018-2691-0.

Khalid, Haqi, Shaiful Jahari Hashim, Sharifah Mumtazah Syed Ahmad, Fazirulhisyam Hashim, and Muhammad Akmal Chaudhary. 2020a. "Cybersecurity in Industry 4.0 Context: Background, Issues, and Future Directions." In *The Nine Pillars of Technologies for Industry 4.0*, 263–307. IET Digital Library. https://doi.org/library.theiet.org/content/books/10.1049/pbte088e_ch14.

Khalid, Haqi, Shaiful Jahari Hashim, Sharifah Mumtazah Syed Ahmad, Fazirulhisyam Hashim, and Muhammad Akmal Chaudhary. 2020b. "Security and Safety of Industrial Cyber-Physical System : Systematic Literature Review." *PalArch's Journal of Archaeology of Egypt / Egyptology* 17 (9): 1592–1620.

Khalid, Haqi, Kweh Yeah Lun, Mohamed Othman, and Idawaty Ahmad. 2017. "Authentication Groups with Privacy-Protection of Machine-to- Machine in LTE/LTE-A Networks." *Journal of Theoretical & Applied Information Technology* 95 (13).

Khan, Minhaj Ahmad, and Khaled Salah. 2018. "IoT Security: Review, Blockchain Solutions, and Open Challenges." *Future Generation Computer Systems* 82: 395–411. https://doi.org/10.1016/j.future.2017.11.022.

Khan, W. Z., M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah. 2020. "Industrial Internet of Things: Recent Advances, Enabling Technologies and Open Challenges." *Computers and Electrical Engineering* 81: 106522. https://doi.org/10.1016/j.compeleceng.2019.106522.

Kumar, Vinod, Musheer Ahmad, Dheerendra Mishra, Saru Kumari, and Muhammad Khurram Khan. 2020. "RSEAP: RFID Based Secure and Efficient Authentication Protocol for Vehicular Cloud Computing." *Vehicular Communications* 22: 100213. https://doi.org/10.1016/j.vehcom.2019.100213.

Kwon, Sungmoon, Jaehan Jeong, and Taeshik Shon. 2018. "Toward Security Enhanced Provisioning in Industrial IoT Systems." *Sensors (Switzerland)* 18 (12): 1–18. https://doi.org/10.3390/s18124372.

Lee, In. 2016. "An Exploratory Study of the Impact of the Internet of Things (IoT) on Business Model Innovation." *International Journal of Information Systems and Social Change* 7 (3): 1–15. https://doi.org/10.4018/ijissc.2016070101.

Li, Chunlei, Qian Wu, Hewu Li, and Jun Liu. 2019. "Trustroam : A Novel Blockchain-Based Cross-domain Authentication Scheme for Wi-Fi Access." In *International Conference on Wireless Algorithms, Systems, and Applications*, 2:149–61. Springer International Publishing. https://doi.org/10.1007/978-3-030-23597-0.

Li, Fagen, and Pan Xiong. 2013. "Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things." *IEEE Sensors Journal* 13 (10): 3677–84. https://doi.org/10.1109/JSEN.2013.2262271.

Li, Yanping, Weifeng Chen, Zhiping Cai, and Yuguang Fang. 2016. "CAKA: A Novel Certificateless-Based Cross-domain Authenticated Key Agreement Protocol for Wireless Mesh Networks." *Wireless Networks* 22 (8): 2523–35. https://doi.org/10.1007/s11276-015-1109-7.

Li, Yuting, Qingfeng Cheng, and Wenbo Shi. 2021. "Security Analysis of a Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for IIoT Environments." *Security and Communication Networks* 2021. https://doi.org/10.1155/2021/5573886.

Lim, Anthony. 2020. "Mercedes Me Connect Service Introduced in Malaysia – Mercedes Me Adapter Available for Older Cars." Mercedes Me Connect: The next-Generation. 2020. https://www.automotiveworld.com/news-releases/mercedes-me-connect-the-next-generation/.

Lin, Chao, Debiao He, Xinyi Huang, Kim Kwang Raymond Choo, and Athanasios V. Vasilakos. 2018. "BSeIn: A Blockchain-Based Secure Mutual Authentication with Fine-Grained Access Control System for Industry 4.0." *Journal of Network and Computer Applications* 116 (May): 42–52. https://doi.org/10.1016/j.jnca.2018.05.005.

Liu, Dan, Shun Zhang, Hong Zhong, Runhua Shi, and Yimin Wang. 2017. "An Efficient Identity-Based Online/Offline Signature Scheme without Key Escrow." *International Journal of Network Security* 19 (1): 127–37. https://doi.org/10.6633/IJNS.201701.19(1).14.

Liu, Xiaoxue, and Wenping Ma. 2018. "CDAKA: A Provably-Secure Heterogeneous Cross-domain Authenticated Key Agreement Protocol with Symptoms-Matching in TMIS." *Journal of Medical Systems* 42 (8). https://doi.org/10.1007/s10916-018-0985-7.

Lohachab, Ankur, and Karambir. 2019. "ECC Based Inter-Device Authentication and Authorization Scheme Using MQTT for IoT Networks." *Journal of Information Security and Applications* 46: 1–12. https://doi.org/10.1016/j.jisa.2019.02.005.

Lupascu, Cristian, Alexandru Lupascu, and Ion Bica. 2020. "DLT Based Authentication Framework for Industrial IoT Devices." *Sensors (Switzerland)* 20 (9). https://doi.org/10.3390/s20092621.

Masdari, Mohammad, and Safiyyeh Ahmadzadeh. 2017. "A Survey and Taxonomy of the Authentication Schemes in Telecare Medicine Information Systems." *Journal of Network and Computer Applications* 87 (August 2016): 1–19. https://doi.org/10.1016/j.jnca.2017.03.003.

Menezes, Alfred. 2009. *An Introduction to Pairing-Based Cryptography*. *Recent Trends in Cryptography*. Vol. 477. AMS-RSME.

Merco, Roberto, Zoleikha Abdollahi Biron, and Pierluigi Pisu. 2018. "Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control." In *Proceedings of the American Control Conference*, 2018-June:5582–87. https://doi.org/10.23919/ACC.2018.8431538.

Miao, Feng Man, and Qiu Yu Zhang. 2010. "Cross-domain Authentication Model Based on Lattice." *Proceedings - 2010 WASE International Conference on Information Engineering, ICIE 2010* 1: 115–18. https://doi.org/10.1109/ICIE.2010.35.

Microsoft. 2019. "Zero Trust Maturity Model." *Microsoft Security*. https://go.microsoft.com/fwlink/p/?linkid=2109181.

Mohamed, Nur Nabila, Yusnani Mohd Yussoff, Mohammed Ahmed Saleh, and Habibah Hashim. 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.

Mohd Aman, Azana Hafizah, Elaheh Yadegaridehkordi, Zainab Senan Attarbashi, Rosilah Hassan, and Yong Jin Park. 2020. "A Survey on Trend and Classification of Internet of Things Reviews." *IEEE Access* 8: 111763–82. https://doi.org/10.1109/ACCESS.2020.3002932.

Moosavi, Sanaz Rahimi, Tuan Nguyen Gia, Amir Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, and Hannu Tenhunen. 2015. "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways." *Procedia Computer Science* 52 (1): 452–59. https://doi.org/10.1016/j.procs.2015.05.013.

Mrabet, Nadia El, and Marc Joye. 2017. *Guide to Pairing-Based Cryptography*. *CRC Press*. https://doi.org/10.1201/9781315370170.

Munir, Kashif, and Lawan A. Mohammed. 2018. "Biometric Smartcard Authentication for Fog Computing." *International Journal of Network Security & Its Applications* 10 (6): 35–45. https://doi.org/10.5121/ijnsa.2018.10604.

Nguyen, Thi Ai Thao, and Tran Khanh Dang. 2017. "Protecting Biometrics Using Fuzzy Extractor and Non-Invertible Transformation Methods in Kerberos Authentication Protocol." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10140 LNCS: 47–66. https://doi.org/10.1007/978-3-662-54173-9_3.

Ni, Jianbing, Kuan Zhang, Xiaodong Lin, and Xuemin Sherman Shen. 2018. "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions." *IEEE Communications Surveys and Tutorials* 20 (1): 601–28. https://doi.org/10.1109/COMST.2017.2762345.

Ninan, Simon, Bharath Gangula, Matthias von Alten, and Brenna Sniderman. 2021. "Who Owns the Road? The IoT-Connected Car of Today—and Tomorrow." The Internet of Things in Automotive. 2021. https://www2.deloitte.com/us/en/insights/focus/internet-of-things/iot-in-automotive-industry.html.

NIST. 2017. "Special Publication- Digital Identity Guidelines." Https://Pages.Nist. Gov/800-63-3/. 2017.

O'Donovan, P., K. Leahy, K. Bruton, and D. T.J. O'Sullivan. 2015. "An Industrial Big Data Pipeline for Data-Driven Analytics Maintenance Applications in Large-Scale Smart Manufacturing Facilities." *Journal of Big Data* 2 (1): 1–26. https://doi.org/10.1186/s40537-015-0034-z.

Obimbo, Charlie, and Benjamin Ferriman. 2011. "Vulnerabilities of LDAP As An Authentication Service." *Journal of Information Security* 02 (04): 151–57. https://doi.org/10.4236/jis.2011.24015.

Oliver, J. 2013. *Encyclopedia of Cryptography and Security*. *Journal of Chemical Information and Modeling*. Vol. 53. https://doi.org/10.1017/CBO9781107415324.004.

Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. "Multi-Factor Authentication: A Survey." *Cryptography* 2 (1): 1. https://doi.org/10.3390/cryptography2010001.

Othmane, Lotfi Ben, Harold Weffers, Mohd Murtadha Mohamad, and Marko Wolf. 2015. "A Survey of Security and Privacy in Connected Vehicles." *Wireless Sensor and Mobile Ad-Hoc Networks Vehicular and Space Applications*, 217–47. https://doi.org/10.1007/978-1-4939-2468-4_10.

Palattella, Maria Rita, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. 2016. "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models." *IEEE Journal on Selected Areas in Communications* 34 (3): 510–27. https://doi.org/10.1109/JSAC.2016.2525418.

Patel, Sudha, Dhiren R. Patel, and Ankit P. Navik. 2016. "Energy Efficient Integrated Authentication and Access Control Mechanisms for Internet of Things." *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 304–9. https://doi.org/10.1109/IOTA.2016.7562742.

Pease, Sarogini Grace, Russell Trueman, Callum Davies, Jude Grosberg, Kai Hin Yau, Navjot Kaur, Paul Conway, and Andrew West. 2018. "An Intelligent Real-Time Cyber-Physical Toolset for Energy and Process Prediction and Optimisation in the Future Industrial Internet of Things." *Future Generation Computer Systems* 79: 815–29. https://doi.org/10.1016/j.future.2017.09.026.

Pelzl, Jan, and Christof Paar. 2016. "The Advanced Encryption Standard (AES)." In *Understanding Cryptography*, 103–41. Springer. https://doi.org/10.1007/978-3-662-49297-0_4.

Peng, Liu, Zong Rui, and Liu Sizuo. 2008. "A New Model for Authentication and Authorization across Heterogeneous Trust-Domain." *Proceedings - International Conference on Computer Science and Software Engineering, CSSE 2008* 3: 789–92. https://doi.org/10.1109/CSSE.2008.1152.

Permanasari, Yurika, and Erwin Harahap. 2006. "Algoritma Data Encryption St Andard (Des) Pada Electronic Code Book (Ecb)." *{Matematika: Jurnal Teori Dan Terapan Matematika* 6 (1): 77–84.

Punithavathi, P., S. Geetha, Marimuthu Karuppiah, SK Hafizul Islam, Mohammad Mehedi Hassan, and Kim Kwang Raymond Choo. 2019. "A Lightweight Machine Learning-Based Authentication Framework for Smart IoT Devices." *Information Sciences* 484: 255–68. https://doi.org/10.1016/j.ins.2019.01.073.

Qu, T., S. P. Lei, Z. Z. Wang, D. X. Nie, X. Chen, and George Q. Huang. 2016. "IoT-Based Real-Time Production Logistics Synchronization System under Smart Cloud Manufacturing." *International Journal of Advanced Manufacturing Technology* 84 (1–4): 147–64. https://doi.org/10.1007/s00170-015-7220-1.

Rahim, Md Abdur, Md Arafatur Rahman, M. M. Rahman, A. Taufiq Asyhari, Md Zakirul Alam Bhuiyan, and D. Ramasamy. 2021. "Evolution of IoT-Enabled Connectivity and Applications in Automotive Industry: A Review." *Vehicular Communications* 27: 100285. https://doi.org/10.1016/j.vehcom.2020.100285.

Rahman, Gohar, and Chuah Chai Wen. 2019. "Mutual Authentication Security Scheme in Fog Computing." *International Journal of Advanced Computer Science and Applications* 10 (11): 443–51. https://doi.org/10.14569/IJACSA.2019.0101161.

Rech, Alexander, Markus Pistauer, and Christian Steger. 2019. "A Novel Embedded Platform for Secure and Privacy-Concerned Cross-domain Service Access." *2019 IEEE Intelligent Vehicles Symposium (IV),* no. Iv: 1961–67. https://doi.org/10.1109/ivs.2019.8814123.

Rose, Scott, Borchert Oliver, Stu Mitchell, and Sean Connelly. 2020. "[NIST SP 800-207] Zero Trust Architecture." *National Institute of Standards and Technology Special Publication,* 49. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf.

S. Hartman. 2011. "A Generalized Framework for Kerberos Pre-Authentication." *Internet Engineering Task Force (IETF),* 24. http://ridum.umanizales.edu.co:8080/jspui/bitstream/6789/377/4/Mu�oz_Zapata_Adriana_Patricia_Art�culo_2011.pdf.

Saeed, Mutaz Elradi S., Qingyin Liu, Gui Yun Tian, Bin Gao, and Fagen Li. 2018. "HOOSC: Heterogeneous Online/Offline Signcryption for the Internet of Things." *Wireless Networks* 24 (8): 3141–60. https://doi.org/10.1007/s11276-017-1524-z.

Safkhani, Masoumeh, Carmen Camara, Pedro Peris-Lopez, and Nasour Bagheri. 2021. "RSEAP2: An Enhanced Version of RSEAP, an RFID Based Authentication Protocol for Vehicular Cloud Computing." *Vehicular Communications* 28: 100311. https://doi.org/10.1016/j.vehcom.2020.100311.

Salehi, Ahmad, Carsten Rudolph, and Marthie Grobler. 2019. "A Dynamic Cross-domain Access Control Model for Collaborative Healthcare Application." *2019 IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019*, 643–48.

Sandhu, Ravi, and Pierangela Samarati. 1996. "Authentication, Access Control, and Audit." *ACM Computing Surveys* 28 (1): 241–43. https://doi.org/10.1145/234313.234412.

Sargent, R. G. 2013. "Verification and Validation of Simulation Models." *Journal of Simulation* 7 (1): 12–24. https://doi.org/10.1057/jos.2012.20.

Sari, Alparslan, Alexios Lekidis, and Ismail Butun. 2017. "Industrial Networks and IIoT: Now and Future Trends." In *Industrial IoT*, 3–55.

Sengupta, Jayasree, Sushmita Ruj, and Sipra Das Bit. 2020. "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT." *Journal of Network and Computer Applications* 149: 102481. https://doi.org/10.1016/j.jnca.2019.102481.

Shah, Ghayoor, Md Saifuddin, Yaser P. Fallah, and Somak Datta Gupta. 2020. "RVE-CV2X: A Scalable Emulation Framework for Real-Time Evaluation of CV2X-Based Connected Vehicle Applications." *IEEE Vehicular Networking Conference, VNC* 2020-Decem: 0–7. https://doi.org/10.1109/VNC51378.2020.9318345.

Shakil, Kashish A, Farhana J Zareen, Mansaf Alam, and Suraiya Jabin. 2017. "BAMHealthCloud : A Biometric Authentication and Data Management System for Healthcare Data in Cloud." *Journal of King Saud University - Computer and Information Sciences,* 0–7. https://doi.org/10.1016/j.jksuci.2017.07.001.

Shamir, Adi, and Yael Tauman. 2001. "Improved Online / Offline Signature Schemes." In *Advances in Cryptology-CRYPTO 2001*, 2139:355–67.

Shen, Meng, Huisen Liu, Liehuang Zhu, Ke Xu, Hongbo Yu, Xiaojiang Du, and Mohsen Guizani. 2020. "Blockchain-Assisted Secure Device Authentication for Cross-domain Industrial IoT." *IEEE Journal on Selected Areas in Communications* 8716 (c): 1–1. https://doi.org/10.1109/jsac.2020.2980916.

Somma, Giorgia. 2021. "A Viable Replacement to the Existing CA-Based PKI for IoT Devices." https://cyberstartupobservatory.com/a-viable-replacement-to-the-existing-ca-based-pki-for-iot-devices/.

Sun, Jinyuan, and Yuguang Fang. 2010. "Cross-domain Data Sharing in Distributed Electronic Health Record Systems." *IEEE Transactions on Parallel and Distributed Systems* 21 (6): 754–64. https://doi.org/10.1109/TPDS.2009.124.

Sun, Xiaoqiang, F. Richard Yu, and Peng Zhang. 2021. "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)." *IEEE Transactions on Intelligent Transportation Systems,* 1–20. https://doi.org/10.1109/tits.2021.3085297.

Sutrala, Anil Kumar, Palak Bagga, Ashok Kumar Das, Neeraj Kumar, Joel J.P.C. Rodrigues, and Pascal Lorenz. 2020. "On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment." *IEEE Transactions on Vehicular Technology* 69 (5): 5535–48. https://doi.org/10.1109/TVT.2020.2981934.

Symeonidis, Iraklis, Abdelrahaman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe, and Bart Preneel. 2017. "SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision." In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* 10493 LNCS:475–93. https://doi.org/10.1007/978-3-319-66399-9_26.

Syverson, Paul, and Iliano Cervesato. 2001. "The Logic of Authentication Protocols." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 2171 LNCS (September 2000): 63–137. https://doi.org/10.1007/3-540-45608-2_2.

Syverson, Paul F, and Paul C Van Oorschot. 1996. "A Unified Cryptographic Protocol Logic." *NRL CHAOS Report*, no. October 2001: 5540–227.

Szymanski, Ted H. 2016. "Supporting Consumer Services in a Deterministic Industrial Internet Core Network." *IEEE Communications Magazine* 54 (6): 110–17. https://doi.org/10.1109/MCOM.2016.7498096.

Tan, Haowen, and Shichang Xuan. 2020. "HCDA : Efficient Pairing-Free Homographic Key Management for Dynamic Cross-domain Authentication in VANETs." *Symmetry* 12 (6): 1003. https://doi.org/10.3390/sym12061003.

Tang, Shaohua, Sunan Shen, and Ke Xue. n.d. "SAML-BASED FEDERATED AUTHENTICATION AND AUTHORIZATION."

Tat, P. Yu and S. R. 2005. ""Online/Offline Signature Schemes for Devices with Limited Computing Capabilities." In *In 4e Cryptographers' Track at the RSA Conference 2008 (CT-RSA 2008),*. Vol. 3457. San Francisco, CA, USA.

The, Unlocking, and Cloud Operating. n.d. “Unlocking the Cloud Operating Model,” 1–9.

Tsague, Aline Z, Elie T Fute, Adnen E L Amraoui, and Emmanuel Tonye. 2018. “DS-NIZKP : A ZKP-Based Strong Authentication Using Digital Signature for Distributed Systems.” *International Journal of Computer Science and Information Security (IJCSIS),* no. April 2019.

Tuttle, Steven, and Michael Storrs. n.d. “Understanding LDAP Design and Implementation LDAP Concepts and Architecture for Directory.” *International Technical Support Organization*.

Venčkauskas, Algimantas, Nerijus Morkevicius, Vaidas Jukavičius, Robertas Damaševičius, Jevgenijus Toldinas, and Šarūnas Grigaliūnas. 2019. “An Edge-Fog Secure Self-Authenticable Data Transfer Protocol.” *Sensors (Switzerland)* 19 (16): 1–19. https://doi.org/10.3390/s19163612.

Viganò, Luca. 2006. “Automated Security Protocol Analysis With the AVISPA Tool.” *Electronic Notes in Theoretical Computer Science* 155 (1 SPEC. ISS.): 61–86. https://doi.org/10.1016/j.entcs.2005.11.052.

Vinoth, R., Lazarus Jegatha Deborah, Pandi Vijayakumar, and Neeraj Kumar. 2020. “Secure Multi-Factor Authenticated Key Agreement Scheme for Industrial IoT.” *IEEE Internet of Things Journal* 8 (5): 1–1. https://doi.org/10.1109/jiot.2020.3024703.

Wagner, Helger Lipmaa and Phillip Rogaway and David. 2000. “Comments to NIST Concerning AES Modes of Operations: CTR-Mode Encryption.” In *National Institute of Standards and Technologies*, 1–4.

Wang, Caifen, Chao Liu, Shufen Niu, Li Chen, and Xu Wang. 2017. “An Authenticated Key Agreement Protocol for Cross-domain Based on Heterogeneous Signcryption Scheme.” *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017,* 723–28. https://doi.org/10.1109/IWCMC.2017.7986374.

Wang, Huaqun. 2018. “Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record.” *IEEE Access* 6: 27818–26. https://doi.org/10.1109/ACCESS.2018.2838095.

Wang, Lin, Haonan An, and Zhuo Chang. 2020. “Security Enhancement on a Lightweight Authentication Scheme with Anonymity Fog Computing Architecture.” *IEEE Access* 8: 97267–78. https://doi.org/10.1109/ACCESS.2020.2996264.

Wang, Wentong, Ning Hu, and Xin Liu. 2018. “BlockCAM: A Blockchain-Based Cross-domain Authentication Model.” *Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018*, 896–901. https://doi.org/10.1109/DSC.2018.00143.

Wang, Yu, and Yong Li Wang. 2015. “A Heterogeneous Cross-domain Authentication Model Based on Access Tickets in Virtual Cable Television Network.” *Applied Mechanics and Materials* 742: 717–20. https://doi.org/10.4028/www.scientific.net/amm.742.717.

Wazid, Mohammad, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel J.P.C. Rodrigues. 2019. “Authentication in Cloud-Driven IoT-Based Big Data Environment: Survey and Outlook.” *Journal of Systems Architecture* 97: 185–96. https://doi.org/10.1016/j.sysarc.2018.12.005.

Wazid, Mohammad, Ashok Kumar Das, Neeraj Kumar, and Athanasios V. Vasilakos. 2019. “Design of Secure Key Management and User Authentication Scheme for Fog Computing Services.” *Future Generation Computer Systems* 91: 475–92. https://doi.org/10.1016/j.future.2018.09.017.

Wazid, Mohammad, Ashok Kumar, and Jong-hyouk Lee. 2019. “User Authentication in a Tactile Internet Based Remote Surgery Environment : Security Issues , Challenges , and Future Research Directions.” *Pervasive and Mobile Computing* 54: 71–85. https://doi.org/10.1016/j.pmcj.2019.02.004.

Wei, Fushan, Sherali Zeadally, Pandi Vijayakumar, Neeraj Kumar, and Debiao He. 2020. “An Intelligent Terminal Based Privacy-Preserving Multi-Modal Implicit Authentication Protocol for Internet of Connected Vehicles.” *IEEE Transactions on Intelligent Transportation Systems,* 1–13. https://doi.org/10.1109/tits.2020.2998775.

Wen, Yamin, Fangguo Zhang, Huaxiong Wang, Zheng Gong, and Yinbin Miao. 2020. “A New Secret Handshake Scheme with Multi-Symptom Intersection for Mobile Healthcare Social Networks.” *Information Sciences* 520: 142–54. https://doi.org/10.1016/j.ins.2020.02.007.

Wollschlaeger, Martin, Thilo Sauter, and Juergen Jasperneite. 2017. “The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0.” *IEEE Industrial Electronics Magazine* 11 (1): 17–27. https://doi.org/10.1109/MIE.2017.2649104.

Wong, Ford Long, and Hoon Wei Lim. 2007. “Identity-Based and Inter-Domain Password Authenticated Key Exchange for Lightweight Clients.” *Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW’07* 2: 544–50. https://doi.org/10.1109/AINAW.2007.203.

Wu, Fan, Lili Xu, Saru Kumari, Xiong Li, Ashok Kumar Das, and Jian Shen. 2018. “A Lightweight and Anonymous RFID Tag Authentication Protocol with Cloud Assistance for E-Healthcare Applications.” *Journal of Ambient Intelligence and Humanized Computing* 9 (4): 919–30. https://doi.org/10.1007/s12652-017-0485-5.

Wu, Jun, Mianxiong Dong, Kaoru Ota, Jianhua Li, and Bei Pei. 2014. "A Fine-Grained Cross-domain Access Control Mechanism for Social Internet of Things." *Proceedings - 2014 IEEE International Conference on Ubiquitous Intelligence and Computing, 2014 IEEE International Conference on Autonomic and Trusted Computing, 2014 IEEE International Conference on Scalable Computing and Communications and Associated Sy*, 666–71. https://doi.org/10.1109/UIC-ATC-ScalCom.2014.140.

Wu, Jun, Mianxiong Dong, Kaoru Ota, Muhammad Tariq, and Longhua Guo. 2015. "Cross-domain Fine-Grained Data Usage Control Service for Industrial Wireless Sensor Networks." *IEEE Access* 3: 2939–49. https://doi.org/10.1109/ACCESS.2015.2504541.

Wu, Tzong Sun, Yih Sen Chen, and Kong Yi Lin. 2010. "ID-Based Online/Offline Signature from Pairings." In *ICS 2010 - International Computer Symposium*, 198–203. IEEE. https://doi.org/10.1109/COMPSYM.2010.5685518.

Xu, Li Da, Wu He, and Shancang Li. 2014. "Internet of Things in Industries: A Survey." *IEEE Transactions on Industrial Informatics* 10 (4): 2233–43. https://doi.org/10.1109/TII.2014.2300753.

Yang, Yang, Xianghan Zheng, Ximeng Liu, Shangping Zhong, and Victor Chang. 2018. "Cross-domain Dynamic Anonymous Authenticated Group Key Management with Symptom-Matching for e-Health Social System." *Future Generation Computer Systems* 84: 160–76. https://doi.org/10.1016/j.future.2017.06.025.

Yang, Yanyan, Mingsheng Hu, Shan Kong, Bei Gong, and Xinxin Liu. 2019. "Scheme on Cross-domain Identity Authentication Based on Group Signature for Cloud Computing." *Wuhan University Journal of Natural Sciences* 24 (2): 134–40. https://doi.org/10.1007/s11859-019-1378-6.

Yao, Lin, Lei Wang, Xiangwei Kong, Guowei Wu, and Feng Xia. 2010. "An Inter-Domain Authentication Scheme for Pervasive Computing Environment." *Computers and Mathematics with Applications* 60 (2): 234–44. https://doi.org/10.1016/j.camwa.2010.01.010.

Yao, Yingying, Xiaolin Chang, Jelena Misic, Vojislav B. Misic, and Lin Li. 2019. "BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services." *IEEE Internet of Things Journal* 6 (2): 3775–84. https://doi.org/10.1109/JIOT.2019.2892009.

Yuan, Chao, Wenfang Zhang, and Xiaomin Wang. 2017. "EIMAKP: Heterogeneous Cross-domain Authenticated Key Agreement Protocols in the EIM System." *Arabian Journal for Science and Engineering* 42 (8): 3275–87. https://doi.org/10.1007/s13369-017-2447-9.

Zantalis, Fotios, Grigorios Koulouras, Sotiris Karabetsos, and Dionisis Kandris. 2019. "A Review of Machine Learning and IoT in Smart Transportation." *Future Internet* 11 (4): 1–23. https://doi.org/10.3390/FI11040094.

Zhang, Dacheng, Jie Xu, and Xianxian Li. 2007. "Dynamic Cross-Realm Authentication for Multi-Party Service Interactions." *Proceedings of the International Conference on Dependable Systems and Networks,* 440–49. https://doi.org/10.1109/DSN.2007.36.

Zhang, Hui, Muhammad Babar, Muhammad Usman Tariq, Mian Ahmad Jan, Varun G. Menon, and Xingwang Li. 2020. "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning." *IEEE Access* 8: 145256–67. https://doi.org/10.1109/ACCESS.2020.3014622.

Zhang, Qikun, Jun Zheng, Yuan Tan, Ruifang Wang, and Yuanzhang Li. 2011. "Cross-domain Authentication Alliance Protocol Based on Isomorphic Groups." *Journal of Computers* 6 (4): 650–56. https://doi.org/10.4304/jcp.6.4.650-656.

Zhang, Quanxin, Qikun Zhang, Yong Gan, Ruifang Wang, and Yu An Tan. 2018. "A Dynamic and Cross-domain Authentication Asymmetric Group Key Agreement in Telemedicine Application." *IEEE Access* 6: 24064–74. https://doi.org/10.1109/ACCESS.2018.2799007.

Zhang, Qui Yu, Wen Tao Jiang, and Guang Bin Bao. 2011. "Route Choice Options Based on Lattice Alliance Certification in Wireless Networks." *Key Engineering Materials* 474–476: 183–88. https://doi.org/10.4028/www.scientific.net/KEM.474-476.183.

Zheng, Jiamin, Yu'an Tan, Xiaosong Zhang, Qikun Zhang, Quanxin Zhang, and Changyou Zhang. 2018. "Multi-Domain Lightweight Asymmetric Group Key Agreement." *Chinese Journal of Electronics* 27 (5): 1085–91. https://doi.org/10.1049/cje.2018.07.002.

Zhou, J., and Z. Cao. 2012. "PSCPA: Patient Self-Controllable Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Systems." *Cryptology EPrint Archive*, 44.

Zhu, Liehuang, Cong Guo, Zijian Zhang, Wei Fu, and Rixin Xu. 2017. "A Novel Contributory Cross-domain Group Password-Based Authenticated Key Exchange Protocol with Adaptive Security." *Proceedings - 2017 IEEE 2nd International Conference on Data Science in Cyberspace, DSC 2017*, 213–22. https://doi.org/10.1109/DSC.2017.89.

Zkik, Karim, Ghizlane Orhanou, and Said El Hajji. 2017. "Secure Mobile Multi Cloud Architecture for Authentication and Data Storage." *International Journal of Cloud Applications and Computing* 7 (2): 62–76. https://doi.org/10.4018/ijcac.2017040105.