LIGHTWEIGHT MUTUAL AUTHENTICATION SCHEME BASED ON ELLIPTIC CURVE DEFFIE-HELLMAN KEY EXCHANGE IN MACHINE-TO-MACHINE COMMUNICATION NETWORK

SHAFI ULLAH

A report submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Faculty of Computing
Universiti Teknologi Malaysia

OCTOBER 2021

ACKNOWLEDGEMENT

First and foremost, all praise and thanks are due to ALLAH, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him). Next, I wish to convey my heartfelt gratitude to my main supervisor, Dr. Raja Zahilah for the kind reassurance, kind guidance and support that enabled me to grasp several research opportunities that groomed me very much for the world of research ahead. I am also very thankful to my co-supervisor Madam Rashidah Kadir for her patience and consideration.

In organizing this thesis, I was in contact with many fellow researchers, academicians, and practitioners who contributed towards my understanding and grooming in the world of research. My most humble appreciation also extends to all my UTM postgraduate colleagues for their support and encouragement.

Finally, I am grateful to all my family members for their support and patience in the hard days of Covid-19 lockdowns. I especially thank my wife and children who stood with me in completing this journey. Moreover, I would like to thank my wonderful friends for their much-appreciated council, patience, and love without which, this journey would not have been possible.

ABSTRACT

Machine-to-Machine communication today is increasing with the help of powerful computing capabilities remotely operated through the advancement in automation devices and the Internet of Things (IoT), known as machine-type communication (MTC) devices. MTC devices consist of small and cheap onboard computers that can execute few tasks due to limited computational, memory and energy capabilities. These devices are used for autonomous monitoring, storing sensory data, and controlling actuators based on shared data. Moreover, these resource-constrained MTC devices are utilized in remote environments and places where human intervention is either unfeasible or immensely complicated. Due to the sensitivity of the data and dynamic topology of MTC devices, it is challenging to trust and rely on autonomous and remote devices in a shared network. Additionally, the data sharing procedures must endure several basic and modern security features such as securing mutual authentication, confidentiality, computationally affordable encryption, key agreeing techniques and effective handling strategies during communication failures. The schemes developed to provide robust security lack performance efficiencies to overcome modern security attacks due to operational costs and computational unaffordability. With inefficient performance and inadequate security, resource-constrained MTC devices face various types of modern Man-in-the-Middle (MiTM), data spoofing, and enforced data leakage-related security attacks. Moreover, most schemes ignore enforced data leakage and communication failure scenarios. Therefore, this research was designed to develop a machine-to-machine physical layer lightweight mutual authentication scheme for 8-bit MTC devices that could withstand modern security attacks and achieve all basic security features, including an anti-communication failure strategy. The scheme consists of three major sections. First, a curve25519 driven lightweight end-to-end encryption which efficiently provided data transmission security to resource-constrained MTC devices. Second, an elliptic-curve Diffie-hellman-based effective mutual authentication with lightweight, encrypted keys enabled the 8-bit devices to achieve authentication, anonymity, and confidentiality. Third, the inclusion of data availability where anti communication failure strategy enabled MTC devices to execute their basic functionality during communication disruption. With offloaded computation, curve25519 driven end-to-end encryption technique produced heavy keys at low cost. Moreover, the lightweight mutual authentication produced comparatively lower network and computational overheads. Additionally, the anti communication failure strategy completely prevented circumstantial and enforced data losses. The results showed that the scheme lost no data during communication failures. Furthermore, the end-to-end encryption achieved 192-bit security with minimum resources, and the mutual authentication in machine-to-machine communication networks produced comparatively lesser network and computation overheads.

ABSTRAK

Komunikasi Mesin-ke-Mesin hari ini meningkat dengan bantuan keupayaan pengkomputeran berkuasa yang dikendalikan dari jauh melalui kemajuan dalam peranti automasi dan Internet of Things (IoT), yang dikenali sebagai peranti komunikasi jenis mesin (MTC). Peranti MTC terdiri daripada komputer onboard yang kecil dan murah yang boleh melaksanakan beberapa tugas kerana keupayaan pengiraan, ingatan dan tenaga yang terhad. Peranti ini digunakan untuk pemantauan autonomi, menyimpan data deria, dan mengawal penggerak berdasarkan data yang dikongsi. Selain itu, peranti MTC yang dikekang oleh sumber ini digunakan dalam persekitaran terpencil dan tempat di mana campur tangan manusia sama ada tidak boleh dilaksanakan atau sangat rumit. Disebabkan oleh sensitivti data dan topologi dinamik peranti MTC, adalah satu cabaran untuk dipercayai dan bergantung pada peranti autonomi dan jauh dalam rangkaian kongsi. Selain itu, prosedur perkongsian data mesti menanggung beberapa ciri keselamatan asas dan moden seperti mendapatkan pengesahan, kerahsiaan, penyulitan berpatutan secara pengiraan, Teknik persetujuan utama dan strategi pengendalian yang berkesan semasa kegagalan komunikasi. Skim dibangunkan untuk menyediakan keselamatan yang teguh, kekurangan kecekapan prestasi untuk mengatasi serangan keselamatan moden disebabkan oleh kos operasi dan ketidakmampuan pengiraan. Dengan prestasi yang tidak cekap dan keselamatan yang tidak berkesan, peranti MTC yang dikekang oleh sumber menghadapi pelbagai jenis Man-in-theMiddle (MiTM) moden, pemalsuan data dan serangan keselamatan berkaitan kebocoran data yang dikuatkuasakan. Selain itu, kebanyakan skim mengabaikan kebocoran data yang dikuatkuasakan dan senario kegagalan komunikasi. Oleh itu, penyelidikan ini direka bentuk untuk membangunkan skim pengesahan bersama ringan lapisan fizikal mesin ke mesin untuk peranti MTC 8-bit yang boleh menahan serangan keselamatan moden dan mencapai semua ciri keselamatan asas, termasuk anti-strategi kegagalan komunikasi. Skim ini terdiri daripada tiga bahagian utama. Pertama, penyulitan hujung ke hujung ringan didorong lengkung25519 yang menyediakan data keselamatan penghantaran dengan cekap kepada peranti MTC yang dikekang sumber. Kedua, pengesahan bersama berkesan berasaskan lengkung eliptik Diffie-hellman dengan kekunci yang ringan dan disulitkan membolehkan peranti 8-bit mencapai pengesahan, tidak dikenali dan kerahsiaan. Ketiga, kemasukan ketersediaan data di mana strategi kegagalan anti komunikasi membolehkan peranti MTC melaksanakan fungsi asasnya semasa gangguan komunikasi. Dengan pengiraan yang dilepaskan, teknik penyulitan hujung ke hujung dipacu lengkung25519 menghasilkan kunci berat pada kos yang rendah. Selain itu, pengesahan bersama yang ringan menghasilkan overhed rangkaian dan pengiraan yang agak rendah. Selain itu, strategi kegagalan anti-komunikasi menghalang sepenuhnya kehilangan data mengikut keadaan dan dikuatkuasakan. Keputusan menunjukkan bahawa skim itu tidak kehilangan data semasa kegagalan komunikasi. Tambahan pula, penyulitan hujung ke hujung mencapai keselamatan 192-bit dengan sumber minimum, dan pengesahan bersama dalam rangkaian komunikasi mesin-ke mesin menghasilkan overhed rangkaian dan pengiraan yang lebih rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3DES	-	Triple Data Encryption System
3GPP	-	3rd Generation Partnership Project
6LoWPAN	-	IPv6 over Low-Power Wireless Personal Area Networks
ABE	-	Attribute Based Encryption
AES	-	Advance Encryption Standard
AIBCwKE	-	Authentication via Identity-Based Cryptography without Key Escrow
AKA	-	Authentication Key Agreeing
AKAES	-	Authentication and Key Agreeing Encrypted System
ANSI	-	American National Standards Institute
API	-	Application Programmable Interface
AVISPA	-	Automated Validation of Internet Security Protocols and
	-	Applications
BAN	-	Body Area Network
CDMA	-	Code-Division Multiple Access
CL-AtSe	-	Constraint-Logic-based Attack Searcher
CP-ABE	-	Cipher-Text Policy Attribute Based Encryption
CRC	-	Cyclic Redundancy Check
DBMS	-	Database Management System
DK	-	Dynamic Key
DoS	-	Denial of Service
DTLS	-	Datagram Transport Layer Security
DY	-	Dolev-Yao (model)
ECC	-	Elliptic Curve Cryptography
ECDH	-	Elliptic Curve Deffie-Hellman
ECDLP	-	Elliptic Curve Discrete Logarithm Problem
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECIES	-	Elliptic Curve Integrated Encryption Scheme
ECMQV	-	Elliptic Curve Menezes-Qu-Vanstone
ECDSA	-	Edwards-curve Digital Signature Algorithm
ECDLP	-	Elliptic Curve Discrete Logarithm
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECMQV	-	Elliptic Curve Menezes-Qu-Vanstone
GW	-	Gateway

HLSPL	-	High−Level Protocol Specification Language
HSS		Home Subscriber Server
IBE	-	Identity Based Encryption
IPI-PRNG	-	Inter Pulse Intervals-Pseudo Random Number Generator
KGC	-	Key Generation Centre
LT	-	Lagrange Time
MAC	-	Machine Access Code
MME	-	Mobile Management Entity
M2M	-	Machine-to-Machine
MTC	-	Machine Type Communication
NTESA	-	New Tiny Symmetric Encryption Algorithm
PKC	-	Public Key Cryptography
PKs	-	Private Keys
PLS	-	Physical Layer Security
PUF	-	Physically Unclonable Function
RSA	-	Rivest Shamir Adelman
RFID	-	Radio Frequency Identification
SATMC	-	Satisfiability-based Model-Checker
SK	-	Secret Key
SoC	-	System on Chip
SPAN	-	Security Protocol Animator
SSK	-	Secret Shared Key
TA4SP	-	Tree Automata based on Automatic Approximations for the Analysis of Security Protocols
TEA	-	Tiny Encryption Algorithm
TSTP	-	Trustful Space-Time Protocol
TTP	-	Trusted Third Party
WBAN		Wireless Body Area Network
WSN	-	Wireless Sensor Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Kevin Ashton (Ashton, 2009) introduced the world to interconnected devices called as Internet of Things (IoT). Network of tiny ubiquitous computational devices connected together called “Internet of Things” processing information and data, creating and sharing new data with machines and users (Singh *et al.*, 2014). It brought immense revolution and enabling human race to technologically enter to a new era of advancements. With the help of industrial developments, a big sized expensive computer is now very tiny and cheap. With the passage of time, sensors were developed that enabled these computers to translate the physical world into digital. Very soon, the computers were able to measure pressure, humidity, temperature, distance, light and proximity(Aman *et al.*, 2018). When the sensors got more advanced, the computers were able to measure complex and tiny physical objects and particles like the amount of carbon dioxide in air, viscosity of liquid, heartbeat of human and voices were recognized. With the help of computer vision, computers can now see and recognized objects, and to some extent understand human behaviors all with the help of advancements in IoTs.

Network of small computational devices called microcontrollers and microprocessors which are capable of processing small information with the ability to work remotely, requiring less internal memory and power compared to the standard personal computers. These devices are then connected to small sensors, keyboards, small Liquid Crystal Displays (LCDs) and Radio-Frequency Identifications (RFIDs) devices etc. to mimic a functional computer. These IoT devices work autonomously in remote areas and do not necessarily require human intervention.

With the development of Industrial revolution 4.0, These Machine-Type Communication (MTC) devices are used in almost all type of new industries. It has been vastly used in medical care where patients are equipped with devices that monitor heartbeat, temperature, and blood sugar level. The devices store the data and share it online with the concerned doctor and patient. Similarly, smart homes are controlled through such IoT devices. Network of microcontrollers is spread in home controlling doors, water supply, providing security through surveillance, buzz alarms and store all the activity within home. The same happens in a computer vision equipped with MTC device through which the devices can identify human behavior and act accordingly. In industries, these devices are responsible for automation such as maintain optimal temperature of the factory through smart ventilation, provide sensory data to robots and many more. These devices form a machine-to-machine networks where several MTC devices communication with each other autonomously. The applications of M2M communication directly connect the people with everyday security to strengthen human security awareness and norms of human behavior (Jing *et al.*, 2014).

Machine-Type communication refer to communication between tiny and low-cost resource constrained independent IoT devices that operate where human involvement is either not needed or possible due to the nature of operation. As discussed in previous chapters, according to Cisco's survey reports in, 48% of world population is using internet (Aspects, 2012) with more than 5 billion such devices connected to WSN and the amount is to reach 50 billion by 2025. We discussed End-to-End encryption feature in this chapter, but only encryption cannot guarantee secure communication because of the heterogeneous nature of M2M communication protocols.

The functionality of MTC devices generally consists upon four levels. Figure 1.1 shows a four level architecture of these resource constained MTC devices.

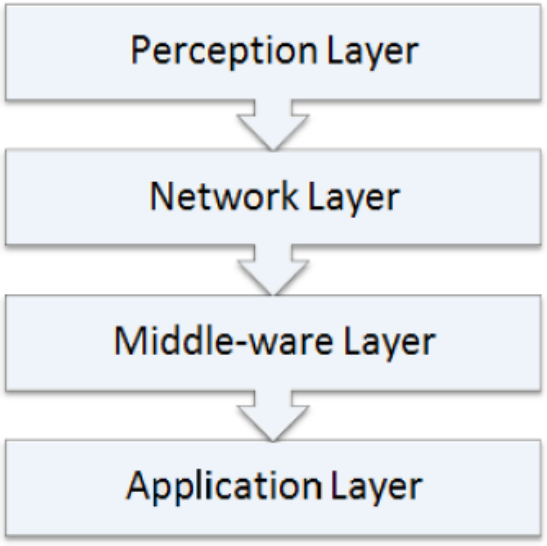

Figure 1.1 : Generic Architecture of M2M communication network

(a) The First layer is called a perception layer that contains several sensors such as Temperature, humidity, RFID, barcode readers, gyro, motion and heartbeat and is responsible for collection of data from real world using these sensors (Zhang, 2011). The data in generated from sensors in this layer, can be transmitted to the attached devices through RFID Readers, Bluetooth, Wi-fi ZigBee and radio frequency transmission medias.

(b) Second layer is called Network layer which is responsible to transmit the received and collected data to any information processing mechanism devised in existing communication networks for instance the internet, via Bluetooth or any other network (Yang *et al.*, 2012).

(c) Third layer “Middle-ware Layer” is consisted upon information processing mechanisms used to automate the flow of actions based on received data. This layer also links the mechanism with the database for storage purposes. The layer has extra work of ensuring the protocols on both sides of transmitter and receiver are same (Khan *et al.*, 2012).

(d) The fourth layer is called an application layer which has many purposes from a representation of the collected data to a good graphical interface to automating the framework for which devices are being used. This layer translates the collected data and converts the whole mechanism into a smart home, smart business, smart industry and smart environment (Yan-rong and Tao, 2013).

M2M communication idea reflects in making more immersive and pervasive internet by allowing variety of MTC devices such as smart home appliances, monitoring sensors, smart visual displays, automated actuators and motors, cameras and even vehicles to communicate with one another thus making a vast network of heterogeneous devices which generates enormous data. This data is further used for predicting market behaviours, data analysis services to citizens including individuals, companies, industries, private and public administrations (Zanella *et al.*, 2014). However, for a heterogeneous network of remote MTC devices, it is a huge challenge in making the distinguishing proof of security of all MTC devices fit for satisfying the prerequisites of all conceivable applications. This challenge has prompted the expansion of various and, some of the time, incongruent solutions for the applicable acknowledgment of M2M frameworks. In this regard, from a framework point of view, the acknowledgment of an M2M framework, together with the required additional servers and gateways still comes up short on real-time applications because of its complexity and uniqueness. Hence, the reception of the M2M communication is additionally obstructed by the absence of an unmistakable and generally acknowledged security scheme that can put such advance organizations in ventures (Laya *et al.*, 2013). One of the reason is that there lacks a sophisticated security scheme in M2M has not yet been given any monitoring polices or standards of interconnected heterogeneous individual M2M networks (Zanella *et al.*, 2014).

1.2 Problem background

In an M2M network where almost everything is connected and exchange data with one another, there arises several security issues. Cyber criminals exploit these

issues. Because of less computational power and memory, standard security protocols and traditional cryptographic techniques cannot be applied on these resource constrained MTC devices since the standard protocols and techniques are not sufficient enough or not available, and a need for a new infrastructure is required by M2M communication networks with optimum security level (Mukherjee, 2015). As there are no security standards to the network of such heterogamous devices, the developer has to self-secure the data exchanged by MTC devices. It was concluded that there are numerous designing options for M2M communication infrastructure that standardized protocols usage cannot be put into consideration rather a topology specific solutions might envision the solutions (Mahmoud *et al.*, 2015) .

This research is based on security provision to tackle security issues afflicted in the perception layer of MTC devices thus relating to the

Figure 1.1 as perception layer faces many challenges. The security provision is developed for an M2M communication network driven resource constrained autonomous MTC (Machine Type Communication) devices which are mainly unsupervised by the user or cloud. Such MTC devices face several security issues, especially in perceptual layer communication (Mukherjee, 2015).

In an M2M communication network consisting of several unsupervised MTC devices by user or cloud, few of which might transmit data remotely, it is very vital to recognize that the data is being transferred from the right sender or data is not tempered during the transmitting as M2M communication is primarily based on exchanging the data. This points to data integrity which imposes a feature of End-to-End encryption during the communication. Even if the data traffic is controlled via strict usage of firewalls and security protocols, the perception layer security of such devices could not be fully guaranteed (Mahmoud *et al.*, 2015).

Due to numerous devices in a strict network, MTC devices are vulnerable to data mutation by attacker through replacing the device with another device that sends tempered data to affect the next in-line set of instruction. It is common troubleshooting solution where the technician would replace any device that is either sending wrong or corrupt data to the network or the device malfunctions and needs to be replaces with a new one. However, the similar device behavior can also be via attacker. This points to another trust issues between MTC devices within the M2M communication network in which finding a tempered device could be a lot of work where several heterogeneous devices generate data simultaneously. Hence, the researchers adopted an easier way in which every device must authenticate itself to be marked as a trusted device.

However, the procedure of authenticating all devices in M2M network costs CPU performance, memory usage, produce network overheads and consume more power. Moreover, the process face security robustness challenges. The topology of an M2M network could be such that several MTC devices are dependent on a central gateway device. Sometimes, task of several devices, is to collect and send the data to a central device (gateway) which is responsible to send the data over the network. In a topology where a master device controls several slave devices, attacking the master device usually disrupts the slaves as well. Thus, the slave devices must not cease to function even if the master device (gateway) is under attack and the devices must not get failed rather keep executing basic tasks until the gateway is restored.

Furthermore, three main challenges with the IoT are protection for users, classification of business applications and device anonymity (Lai *et al.*, 2016b). It is recognized that in the IoT framework, there are four interconnected, collaborating sections (i.e., users, devices, software, and network) that communicate over open and untrusted networks. These will undoubtedly be vulnerable to security protection and open trust issues. In this manner, issues mentioned in (Li *et al.*, 2017a) concerning central gateways, users and outsider attacks must be tended to. In circumstances where security can be characterized as a composed system comprising of encryption

algorithms, security schemes, network standards, device topologies, and overall protocols must be focused to ensure plausible resilience of either a specific framework or general framework in against any unexpected risk. Every one of these associations should be anchored to guarantee data security and trustable devices, provisioning of every single noteworthy vulnerability and limit risk occurrences that might impact the whole network as statistical attacks can reclaim data from the system without affecting its executions. In this regard, vulnerabilities are encountered due to certain risk and attacks applied on M2M communication network. Therefore, M2M network now faces different statistical and dynamic attacks that may effortlessly upset its usefulness and invalidate the advantages of utilizing its purpose.

Data in perception layer, can be transmitted over a wired network, WSN however the challenge lies in both wired and wireless sensor networks. The challenge is not receiving accurate data from sensors but to transmit the received data from sensor accurately, at the perception layer. Figure 1.2 shows the IoT security architecture.

Intruder’s perceptive model is one of the distinctive kinds of threat to the IoT network. A Dolev-Yao (DY) sort of intruder which is a result of the system and may block all or any message at any point transmitted between MTC devices and gateways. Nevertheless, its abilities are marginally unrealistic, "attacks just improve, they never deteriorate" said by “Bruce Schneider in (Srilaya and Velampalli, 2020)”. Similarly, security will be a lot more grounded if our M2M communication is intended to be DY interloper versatile. Be that as it may, the DY interloper needs one ability that common interlopers may have which is a physical trade off. In this way, carefully designed devices are additionally extraordinarily alluring. This objective is unattainable, yet obstruction for physical modification in devices, is in any case an essential objective, which, together with alter recognition abilities might be an adequate first-line resistance.

Physical attacks are kind of attacks that alters devices' data or hardware. Due to the unattended and circulated nature of IoT, most devices ordinarily work in outside situations, which are exceptionally helpless to physical attacks (Mosenia and Jha, 2017). Attacks on security is common since the M2M makes huge volumes of data effectively accessible through remote access components, security assurance in the network, is moved toward becoming progressively testing. The enemy is not required to be physically present to complete observation, however data collected should generally be safe. The most well-known attacks on client protection are as per the following (Burhan *et al.*, 2018) are spying and detached checking which is most normal and simplest type of assault on information protection. If messages are not ensured by cryptographic systems, a foe could without much of a stretch comprehend the substance. Moreover, traffic investigation requests to adequately assault, security and listening are joined with traffic investigation. Through viable traffic investigation, an enemy can recognize certain data with exceptional jobs and exercises in IoT devices and information. Additionally, the information mining empowers aggressors to find data that is unforeseen in specific databases. This could

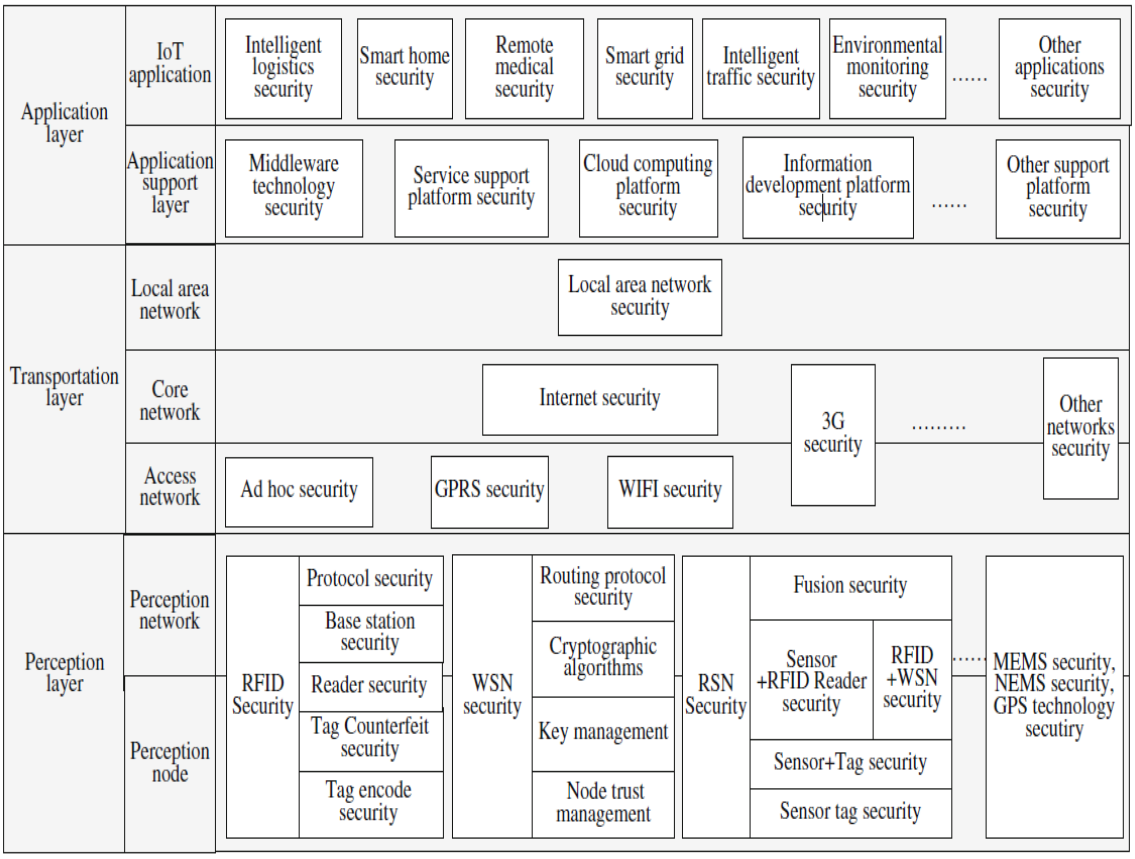

Figure 1.2: IoT security architecture adopted from (Hansch *et al.*, 2019)

be a security and protection issue in M2M communication, and if data is made accessible it will leak all the data (Farooq *et al.*, 2015).

1.2.1 Security features in perception layer of machine type communication devices

According to (Mahmoud *et al.*, 2015) , the security features are divided into two categories; technological and security challenges. The technological challenge is due to dynamic topologies of connected devices and ubiquitous nature of M2M communication. Technological challenges mainly focuses on energy, power and distributed nature of the devices while security challenges primarily focuses on the ability of devices to ensure authentication, scalability, confidentiality, end-to-end security and data integrity (Mahalle *et al.*, 2013). Our research remains in the area of security challenges primarily with the inclusion of integrity, confidentiality, authentication and availability. Main features are as follows.

1.2.1.1 Data integrity

It is based on the accuracy of the data being exchanged between various heterogeneous devices. Since the main purpose of numerous MTC devices is to collect data and share with neighboring devices, store the data, or take prescribed action against it. That is why it is very important for the data to be accurate, and sender of the data must be cleared from intended or unintended interference during transmission. This feature is mostly imposed by lightweight end-to-end cryptography.

1.2.1.2 Data availability

Purpose of MTC devices is to serve the user with the constant flow of data in all circumstances. This feature emphasizes on constant flow of data no matter what happens to the network which mainly points to the scenarios where performance of these devices must not affect the assigned tasks, even if the communication is either disrupted or attacked that can result in functionality and loss of critical data

1.2.1.3 Confidentiality

Device's privacy must be protected in all case primarily because the data being transmitted is very sensitive to the end user that is why data must be kept encrypted even from the unauthorized nodes in the same network. To achieve this feature, many researchers have proposed encryption techniques. Confidentiality is generally achieved with the combination of the authentication of devices and encrypting the transmission processing.

1.2.1.4 Authentication

Due to heterogeneity and numerous devices working autonomously within an M2M network, the MTC devices can be easily duplicated or captured, and data can be tempered and transmitted over the network. Which is why all the devices in the network must be trusted and authentication must be carried out between the exchanges of messages. Device must know who it is sending and receiving data from.

1.2.2 Integrity and confidentiality of data in Machine-to- Machine communication network

M2M Communication network faces challenges in data confidentiality and integrity as mentioned in previous sections. In a heterogeneous network of numerous connected resource constrained MTC devices, sharing and perceiving information from neighboring devices, there comes an issue in trusting the incoming data. While in process of communication, data or information could be modified by the cybercriminals or then again could be influenced by different elements that are beyond human control including the server crash or an electromagnetic disruption (Yang *et al.*, 2017). Data Integrity points to the safety of valuable information from the cybercriminals or the outer interference during transmission and reception with some basic following strategies, so the data cannot be altered without endangering the framework (Farooq *et al.*, 2015). The techniques to guarantee the accuracy and originality of data incorporates strategies like checksum and cyclic redundancy check (CRC), which are common error detection mechanism for a segment of data. Moreover, persistent adjusting of the data for reinforcement purposes and the feature such as version control. Version control keeps a record of the document changes in a framework to reestablish the record on the off chance that of accidental erasure of data can likewise guarantee the respectability of data with the end goal that the data on IoT based devices is in its unique frame when gotten to by the allowed clients. While data confidentiality refers to the data being monitored by unauthorized users or external interference. It mainly points to the ability of confidence the user faces for sharing sensitive data. Security mechanism for provision and assurance of data confidentiality is achieved in many security mechanisms by researcher mainly in terms of encryption techniques (Farooq *et al.*, 2015) (which is not enough). This could be achieved by the combination of authentication of MTC devices with encryption technique to stay anonymous from neighboring devices. Researchers have found many ways for data encryption i.e. random hash lock protocols also known as hash functions, hash chain mechanisms and infinite extraction key channels (Jing *et al.*, 2014). That is why, to secure transmission confidentiality within nodes, encrypting the data seems extremely necessary. Encryption requires great consumption of resources i.e., computational power and memory both of which the resource constrained MTC devices lack in general. That is why, lightweight

cryptography techniques are the best solutions to be adopted that includes algorithms related lightweight cryptographies (Aman *et al.*, 2018).

Typically, the symmetric encryption calculation is utilized to encode information for classification. Advance Encryption Standard (AES) block Cipher; Asymmetric algorithms is regularly used to digital signatures and key transport, more often used algorithm is the Rivest Shamir Adelman (RSA); the Diffie-Hellman (DH) Asymmetric key agreement algorithm is utilized to key manipulation and agreement; and the SHA-1 and SHA-256 secure hash algorithms will be connected for integrality. However, implementing these algorithms will require processor speed and memory. In this regard, elliptic curve cryptography (ECC) is noteworthy asymmetric algorithm that can deliver affordable security by utilization of shorter length keys.

1.2.3 Authentication of machine type communication devices in Machine-to-Machine communication network

Based on tight security requirements in autonomous and data sensitive industrial application, hundreds of MTC devices interconnect with one another and share data. It is very difficult to monitor all the devices personally, as many works remotely or in places where human intervention is either very risky, costly, or extremely difficult. Such security challenges are worsened by the steep number of devices and the normal barriers in user interfaces. Among others, certain security angles such as authorization and data protection require creative methodologies. As of authentication, there is a need to characterize an object validation component to guarantee that as it remained accepted and can access certain segments of data exchanged within M2M communication network. In such environment, all the devices need to validate one another and in order to establish the trust through authentication where every device will authenticate itself the first time connected to the network. The process is known as identity authentication.

Identity authentication can assess the data transmission between both sides i.e., transmitter and receiver; and can confirm each side's identity. This mechanism can help prevent disguised threats and outsider attacks to ensure authenticity and validity of data. Many identity authentication techniques in wired and wires sensory networks have been proposed. As IoT devices consists of low computational power and memory with very open environment and dynamic topology, an authentication mechanism must surpass these limitations. Most of the recent research such as (Lai *et al.*, 2016a), (Li *et al.*, 2018b) and (Parne *et al.*, 2018) has been based on MD5 and SHA hash functions with public key authentication features. Since public key cryptography needs much more computation and memory, the mechanism has been ineffective. (Li *et al.*, 2018b) imposed that (Shi and Gong, 2013) , (Choi *et al.*, 2014) and (Shi and Gong, 2013) techniques lack password guessing and changing attacks and aren't suitable IoT environment due to messages directly being exchange with nodes. Rather (Li *et al.*, 2018b) worked on mutual three factor authentication between user, device and gateway while (Lin *et al.*, 2018b) presented Local authentication modes; imposing further weakness in user-less network, data spoofing and Eavesdropping attacking techniques.

1.2.4 Data availability of devices during disrupted Machine-to- Machine communication network

Availability is one the main feature of a robust IoT or M2M communication network mentioned in (Farooq *et al.*, 2015) which points to a scenario when data transmission is either attacked or malfunctions then the devices must not cease to function. In other words, the devices must not malfunction even if transmission lines or media malfunctions (Hossain *et al.*, 2015a). For instance, a device connected to a terminal being responsible for granting access to doors to different users while also recording the user information and sending it to another device. In this case, if the data sending process has been compromised then the device should keep granting access to the recent users, brought up by (Hussain *et al.*, 2017). Data availability has been highlighted by (Aman *et al.*, 2018). Moreover, the scenario in which a master device controls several slave devices which then perform their own specified tasks,

connect via I^2C communication or SPI configuration also known as mode of communication (Chen *et al.*, 2016) where the types of communication takes place includes one to one, one to many and many to many. In general cases, the slave device will also malfunction if the master device stops working or the communication media malfunctions. Feature of data availability must ensure the non-malfunctioning of slave devices, rather the devices should keep working as far as it can rather malfunctioning(Hussain, 2016). Whereas the collection of data is not the only purpose of M2M communication in IoT; devices and services must be accessible and available when required in a timely fashion to achieve for uninterrupted smooth operations of IoT (Kamble and Bhutad, 2018).

Similarly, attacks such as sinkhole attack, black hole attack , wormholes attack , sybil attack , hello flood attacks and desynchronization attacks; attack the sensor nodes or any part of the M2M network and end up influencing the survivability of the entire network (Burhanuddin *et al.*, 2018). Therefore, the data availability requirement is vital for maintaining the operational services of M2M communication network and likewise in maintaining the whole network throughout its life cycle. In addition, the severity of data loss and services mainly depend on the type of operation driven by the overall network application; ignoring such feature pose a major security threat and is considered a security risk that provides an open ground to the adversary to carry away any desired attack on the IoT network. In this regard, researchers such as (Hossain *et al.*, 2015b), (Ali and Awad, 2018) , (Ahanger and Aljumah, 2018) and (Gupta *et al.*, 2018) have addressed such threat by inducing a feature in basic security architecture of IoT network known as data availability. It has been recognized as one of the main four security provisions that an IoT network must endure, especially in remotely operated IoT applications. However, data availability feature has been widely neglected in recent developments on IoT driven applications. This is because of either predicting high communication system reliability or insensitive data. Despite the consideration of data insensitivity, it is a huge security vulnerability.

1.3 Problem statement

In M2M communication, resource constrained autonomous MTC devices in current security schemes lack in countering modern attacks such as DoS, MiTM and data spoofing efficiently in terms of computational cost and memory consumptions. Adoption of end-to-end encryption gained data integrity but did not address confidentiality. Whereas, mutual authentication schemes gained data confidentiality at unaffordable cost of computation, network overheads and memory consumption. In addition, almost all the recent schemes do not address data availability that emphasizes on robustness and survivability of devices and the network during enforced communication disruption and enforced data loss. Which is why, a communication failure resilient lightweight security scheme is required that can effectively counter modern attacks with affordable computational, network and memory costs. In addition, the scheme must also address all basic four basic perception layer security features i.e., data integrity, authentication, confidentiality, and data availability. A lightweight end-to-end encryption can help in achieving data integrity and privacy efficiently while a cost-effective ECDH based mutual authentication will achieve confidentiality and trust between the devices with affordable computation. To achieve data availability, an anti-failure strategy is required that enables devices to function during communication disruption.

1.4 Research questions

(a) How to achieve lightweight End-to-End encryption feature to effectively counter MiTM, data spoofing and other modern security threats in perception layer?

(b) How to establish secure lightweight mutual authentication between the resource constrained MTC devices efficiently, in terms of affordable computational cost and memory overheads?

(c) How to make MTC device function during communication failures to minimize data loss and improve device survivability?

(d) How to device a comprehensive authentication scheme that contains all basic security features in perception layer of MTC devices.

1.5 Research goal

The research aims to introduce a robust security scheme that focuses on integrity of data and mutual authentication of devices during machine-to-machine communication regardless of the user and cloud with an inclusion of anti-communication failure strategy to avoid data loss in case the communication between the MTC devices is disturbed so that devices will not cease to function.

1.5.1 Research objectives

(a) To develop ECC based lightweight end-to-end encryption for resource constrained MTC devices in protection against modern MiTM and data spoofing attacks to ensure integrity of data.

(b) To devise pre-shared keys driven lightweight ECDH (Elliptic Curve Diffie Hellman) authentication key exchange protocol during mutual authentication using a lightweight novel hash function in public key asymmetric cryptosystem to developed trust between resource constrained MTC devices.

(c) To add anti-communication failure strategy as a secondary function in MTC devices in case of communication disruption and enforced data loss so that the basic function of MTC such as data generating, controlling, and monitoring is not disturbed, to achieve data availability feature.

1.6 Research contributions

(a) Addition of anti-communication failure strategy as a secondary function allocated to MTC devices addresses data availability for the first time. The strategy introduced thorough protection against enforced data loss attacks and minimized losses during enforce communication disruptions.

(b) An ECDH based mutual authentication via lightweight key exchange function will improve power and storage consumptions. Moreover, the use of small sized pre-shared keys (authentication frames) will reduce the transmission overheads significantly. It will ensure authentication and privacy for M2M communication networks.

(c) An elliptic curve based lightweight end-to-end encryption will ensure random and robust encrypted keys. Moreover, use of proper light and robust curve results in affordable computation for resource constrained MTC devices in ensuring data integrity and confidentiality and protection against modern MiTM, data spoofing and other related attacks.

1.7 Research scope/assumptions

(a) The research does not include wired and wireless data transmission protocols such as TCP/IP, Wi-Fi, Bluetooth, and ZigBee. Rather, the perception layer prepares a block (MAC) which can be transmitted over any medium through serial communication protocol.

(b) The study mainly focuses on end-to-end serial communication between perception layers in MTC devices. However, the communication can also be extended to work with SPI and I^2C communication.

(c) The machine-to-machine communication network is assumed static, hierarchical and can suffer communication disruption. Furthermore, the nodes (devices) are homogeneous, and time synchronized.

(d) MTC devices are resource constrained, equipped with extremely limited internal memory capacity i.e., 4Kbytes RAM and less computational power i.e., 8-bit CPU.

(e) MTC devices have constant supply of power during communication disruption.

(f) The ECC based keys are small sized and pre-shared. The encryption and decryption processes support limited ASCII characters so that the least possible internal memory is occupied.

REFERENCES

Ab Manan, J.-L., Mubarak, M. F., Isa, M. a. M. and Khattak, Z. A. (2011). Security, Trust and Privacy–a New Direction for Pervasive Computing. *Information Security***,** 56-60.

Abdelhalim, M., El-Mahallawy, M., Ayyad, M. and Elhennawy, A. (2012). Design and Implementation of an Encryption Algorithm for Use in Rfid System. *International Journal of RFID Security and Cryptography (IJRFIDSC),* 1(1/2)**,** 15-22.

Abdullah, D., Rahim, R., Siahaan, A. P. U., Ulva, A. F., Fitri, Z., Malahayati, M. and Harun, H. (Year) Published. Super-Encryption Cryptography with Idea and Wake Algorithm. Journal of Physics: Conference Series, 2018. IOP Publishing, 012039.

Adnan, S. F. S., Isa, M. a. M. and Hashim, H. (Year) Published. Timing Analysis of the Lightweight Aaβ Encryption Scheme on Embedded Linux for Internet of Things. 2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2016. IEEE, 113-116.

Ahanger, T. A. and Aljumah, A. (2018). Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. *IEEE Access,* 7**,** 11020-11028.

Aigner, H., Bock, H., Hütter, M. and Wolkerstorfer, J. (Year) Published. A Low-Cost Ecc Coprocessor for Smartcards. International Workshop on Cryptographic Hardware and Embedded Systems, 2004. Springer, 107-118.

Akitaya, T., Asano, S. and Saba, T. (Year) Published. Time-Domain Artificial Noise Generation Technique Using Time-Domain and Frequency-Domain Processing for Physical Layer Security in Mimo-Ofdm Systems. Communications Workshops (ICC), 2014 IEEE International Conference on, 2014. IEEE, 807-812.

Ali, B. and Awad, A. I. (2018). Cyber and Physical Security Vulnerability Assessment for Iot-Based Smart Homes. *sensors,* 18(3)**,** 817.

Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing,* 21(2)**,** 34-42.

Altop, D. K., Levi, A. and Tuzcu, V. (Year) Published. Towards Using Physiological Signals as Cryptographic Keys in Body Area Networks. 2015 9th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2015. IEEE, 92-99.

Aman, M. N., Sikdar, B., Chua, K. C. and Ali, A. (2018). Low Power Data Integrity in Iot Systems. *IEEE Internet of Things journal*.

Aranha, D. F., Dahab, R., López, J. and Oliveira, L. B. (2010). Efficient Implementation of Elliptic Curve Cryptography in Wireless Sensors. *Adv. in Math. of Comm.,* 4(2)**,** 169-187.

Armando, A., Basin, D., Cuellar, J., Rusinowitch, M. and Viganò, L. (2006). Avispa: Automated Validation of Internet Security Protocols and Applications. *ERCIM News,* 64(January).

Ashton, K. (2009). That Internet of Things Thing.
Aspects, T. S. G. S. a. S. (2012). 3gpp System Architecture Evolution (Sae); Security Aspects of Non-3gpp Accesses. 11(4.0).
Association, K. T. T. (2013). 128 Bit Light Weight Block Cipher Lea. *Information Telecommunication Organization Standard (Korean Standard)*.
Ayub, M. F., Mahmood, K., Kumari, S. and Sangaiah, A. K. (2020). Lightweight Authentication Protocol for E-Health Clouds in Iot Based Applications through 5g Technology. *Digital Communications and Networks*.
Babar, S., Stango, A., Prasad, N., Sen, J. and Prasad, R. (Year) Published. Proposed Embedded Security Framework for Internet of Things (Iot). Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, 2011. IEEE, 1-5.
Bala, D. Q., Maity, S. and Jena, S. K. (Year) Published. Mutual Authentication for Iot Smart Environment Using Certificate-Less Public Key Cryptography. 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), 2017. IEEE, 29-34.
Barki, A., Bouabdallah, A., Gharout, S. and Traore, J. (2016). M2m Security: Challenges and Solutions. *IEEE Communications Surveys & Tutorials*, 18(2)**,** 1241-1254.
Benenson, Z., Gedicke, N. and Raivio, O. (2005). Realizing Robust User Authentication in Sensor Networks. *Real-World Wireless Sensor Networks (REALWSN)*, 14**,** 52.
Bernstein, D. J. (Year) Published. Curve25519: New Diffie-Hellman Speed Records. International Workshop on Public Key Cryptography, 2006. Springer, 207-228.
Bhasin, S. and Regazzoni, F. (Year) Published. A Survey on Hardware Trojan Detection Techniques. Circuits and Systems (ISCAS), 2015 IEEE International Symposium on, 2015. IEEE, 2021-2024.
Bhunia, S., Abramovici, M., Agrawal, D., Bradley, P., Hsiao, M. S., Plusquellic, J. and Tehranipoor, M. (2013). Protection against Hardware Trojan Attacks: Towards a Comprehensive Solution. *IEEE Design & Test*, 30(3)**,** 6-17.
Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., Seurin, Y. and Vikkelsoe, C. (Year) Published. Present: An Ultra-Lightweight Block Cipher. International workshop on cryptographic hardware and embedded systems, 2007. Springer, 450-466.
Boneh, D., Gentry, C., Lynn, B. and Shacham, H. (Year) Published. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. International Conference on the Theory and Applications of Cryptographic Techniques, 2003. Springer, 416-432.
Brandt, A., Buron, J. and Porcu, G. (2010). Home Automation Routing Requirements in Low-Power and Lossy Networks.
Burhan, M., Rehman, R., Khan, B. and Kim, B.-S. (2018). Iot Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, 18(9)**,** 2796.
Burhanuddin, M., Mohammed, A. a.-J., Ismail, R., Hameed, M. E., Kareem, A. N. and Basiron, H. (2018). A Review on Security Challenges and Features in Wireless Sensor Networks: Iot Perspective. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 10(1-7)**,** 17-21.

Cao, J., Ma, M. and Li, H. (2015). Gbaam: Group-Based Access Authentication for Mtc in Lte Networks. *Security and communication networks,* 8(17)**,** 3282-3299.

Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y. and Sastry, S. (Year) Published. Attacks against Process Control Systems: Risk Assessment, Detection, and Response. Proceedings of the 6th ACM symposium on information, computer and communications security, 2011. ACM, 355-366.

Carracedo, J. M., Milliken, M., Chouhan, P. K., Scotney, B., Lin, Z., Sajjad, A. and Shackleton, M. (Year) Published. Cryptography for Security in Iot. 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, 2018. IEEE, 23-30.

Chanal, P. M. and Kakkasageri, M. S. (2020). Security and Privacy in Iot: A Survey. *Wireless Personal Communications,* 115(2)**,** 1667-1693.

Chen, S., Ma, M. and Luo, Z. (2016). An Authentication Scheme with Identity-Based Cryptography for M2m Security in Cyber-Physical Systems. *Security and Communication Networks,* 9(10)**,** 1146-1157.

Chen, Y.-W., Wang, J.-T., Chi, K.-H. and Tseng, C.-C. (2012). Group-Based Authentication and Key Agreement. *Wireless Personal Communications,* 62(4)**,** 965-979.

Chim, T. W., Yiu, S.-M., Li, V. O., Hui, L. C. and Zhong, J. (2015). Prga: Privacy-Preserving Recording & Gateway-Assisted Authentication of Power Usage Information for Smart Grid. *IEEE Transactions on Dependable and Secure Computing,* 12(1)**,** 85-97.

Choi, D., Choi, H.-K. and Lee, S.-Y. (2015). A Group-Based Security Protocol for Machine-Type Communications in Lte-Advanced. *Wireless networks,* 21(2)**,** 405-419.

Choi, K.-C. and Jun, M.-S. (2016). A Design of Key Agreement Scheme between Lightweight Devices in Iot Environment. *Advances in Computer Science and Ubiquitous Computing.* (pp. 224-229). Springer.

Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J. and Won, D. (2014). Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors,* 14(6)**,** 10081-10106.

Chou, T. (Year) Published. Sandy2x: New Curve25519 Speed Records. International Conference on Selected Areas in Cryptography, 2015. Springer, 145-160.

Chu, D., Großschädl, J., Liu, Z., Müller, V. and Zhang, Y. (Year) Published. Twisted Edwards-Form Elliptic Curve Cryptography for 8-Bit Avr-Based Sensor Nodes. Proceedings of the first ACM workshop on Asia public-key cryptography, 2013. ACM, 39-44.

Das, A. K., Zeadally, S. and He, D. (2018). Taxonomy and Analysis of Security Protocols for Internet of Things. *Future Generation Computer Systems,* 89**,** 110-125.

Das, M. L. (2009). Two-Factor User Authentication in Wireless Sensor Networks. *IEEE transactions on wireless communications,* 8(3)**,** 1086-1090.

De Clercq, R., Uhsadel, L., Van Herrewege, A. and Verbauwhede, I. (Year) Published. Ultra Low-Power Implementation of Ecc on the Arm Cortex-M0+. 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), 2014. IEEE, 1-6.

De Santis, F. and Sigl, G. (2016). Towards Side-Channel Protected X25519 on Arm Cortex-M4 Processors. *Proceedings of Software performance enhancement*

*for encryption and decryption, and benchmarking, Utrecht, The Netherlands***,** 19-21.
Devi, G. U., Balan, E. V., Priyan, M. and Gokulnath, C. (2015). Mutual Authentication Scheme for Iot Application. *Indian Journal of Science and Technology,* 8(26).
Ding, L., Jin, C., Guan, J. and Wang, Q. (2014). Cryptanalysis of Lightweight Wg-8 Stream Cipher. *IEEE Transactions on Information Forensics and Security,* 9(4)**,** 645-652.
Ding, S., Li, C. and Li, H. (2018). A Novel Efficient Pairing-Free Cp-Abe Based on Elliptic Curve Cryptography for Iot. *IEEE Access,* 6**,** 27336-27345.
Dolev, D. and Yao, A. (1983). On the Security of Public Key Protocols. *IEEE Transactions on information theory,* 29(2)**,** 198-208.
Dong, J., Zheng, F., Cheng, J., Lin, J., Pan, W. and Wang, Z. (Year) Published. Towards High-Performance X25519/448 Key Agreement in General Purpose Gpus. 2018 IEEE Conference on Communications and Network Security (CNS), 2018. IEEE, 1-9.
Du, X., Xiao, Y., Guizani, M. and Chen, H.-H. (2007). An Effective Key Management Scheme for Heterogeneous Sensor Networks. *Ad Hoc Networks,* 5(1)**,** 24-34.
Düll, M., Haase, B., Hinterwälder, G., Hutter, M., Paar, C., Sánchez, A. H. and Schwabe, P. (2015). High-Speed Curve25519 on 8-Bit, 16-Bit, and 32-Bit Microcontrollers. *Designs, Codes and Cryptography,* 77(2-3)**,** 493-514.
El-Hajj, M., Fadlallah, A., Chamoun, M. and Serhrouchni, A. (2019). A Survey of Internet of Things (Iot) Authentication Schemes. *Sensors,* 19(5)**,** 1141.
Electronic Industries, A. and Engineering, D. (1969). *Interface between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange.* [Washington], Electronic Industries Association, Engineering Dept.
Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O. M., Shawkat, S. A., Arunkumar, N. and Farouk, A. (2018). Secure Medical Data Transmission Model for Iot-Based Healthcare Systems. *IEEE Access,* 6**,** 20596-20608.
Farooq, M. U., Waseem, M., Khairi, A. and Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (Iot). *International Journal of Computer Applications,* 111(7).
Faz-Hernández, A., López, J. and Dahab, R. (2019). High-Performance Implementation of Elliptic Curve Cryptography Using Vector Instructions. *ACM Transactions on Mathematical Software (TOMS),* 45(3)**,** 1-35.
Fröhlich, A. A., Scheffel, R. M., Kozhaya, D. and Veríssimo, P. E. (2018). Byzantine Resilient Protocol for the Iot. *IEEE Internet of Things Journal,* 6(2)**,** 2506-2517.
Frustaci, M., Pace, P., Aloi, G. and Fortino, G. (2018). Evaluating Critical Security Issues of the Iot World: Present and Future Challenges. *IEEE Internet of Things journal,* 5(4)**,** 2483-2495.
Fu, A., Song, J., Li, S., Zhang, G. and Zhang, Y. (2016). A Privacy-Preserving Group Authentication Protocol for Machine-Type Communication in Lte/Lte-a Networks. *Security and Communication Networks,* 9(13)**,** 2002-2014.
Fujii, H. and Aranha, D. F. (Year) Published. Efficient Curve25519 Implementation for Arm Microcontrollers. Anais Estendidos do XVIII Simpósio Brasileiro

em Segurança da Informação e de Sistemas Computacionais, 2018. SBC, 57-64.
Gentry, C. and Waters, B. (Year) Published. Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts). Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2009. Springer, 171-188.
Glouche, Y., Genet, T., Heen, O. and Courtay, O. (Year) Published. A Security Protocol Animator Tool for Avispa. ARTIST2 workshop on security specification and verification of embedded systems, Pisa, 2006.
Gouvêa, C. P., Oliveira, L. B. and López, J. (2012). Efficient Software Implementation of Public-Key Cryptography on Sensor Networks Using the Msp430x Microcontroller. *Journal of Cryptographic Engineering,* 2(1)**,** 19-29.
Goyal, V., Pandey, O., Sahai, A. and Waters, B. (Year) Published. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Proceedings of the 13th ACM conference on Computer and communications security, 2006. Acm, 89-98.
Grindrod, K., Khan, H., Hengartner, U., Ong, S., Logan, A. G., Vogel, D., Gebotys, R. and Yang, J. (2018). Evaluating Authentication Options for Mobile Health Applications in Younger and Older Adults. *PloS one,* 13(1)**,** e0189048.
Gupta, S., Parne, B. L. and Chaudhari, N. S. (2018). Dgbes: Dynamic Group Based Efficient and Secure Authentication and Key Agreement Protocol for Mtc in Lte/Lte-a Networks. *Wireless Personal Communications,* 98(3)**,** 2867-2899.
Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S. C. (Year) Published. Comparing Elliptic Curve Cryptography and Rsa on 8-Bit Cpus. International workshop on cryptographic hardware and embedded systems, 2004. Springer, 119-132.
Hammoudi, S., Aliouat, Z. and Harous, S. (Year) Published. A New Infrastructure as a Service for Iot-Cloud. 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018. IEEE, 786-792.
Hankerson, D., Menezes, A. J. and Vanstone, S. (2005). Guide to Elliptic Curve Cryptography. *Computing Reviews,* 46(1)**,** 13.
Hanley, N. and Oneill, M. (Year) Published. Hardware Comparison of the Iso/Iec 29192-2 Block Ciphers. 2012 IEEE Computer Society Annual Symposium on VLSI, 2012. IEEE, 57-62.
Hansch, G., Schneider, P., Fischer, K. and Böttinger, K. (Year) Published. A Unified Architecture for Industrial Iot Security Requirements in Open Platform Communications. 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019. IEEE, 325-332.
Hassan, H. a. H., Pelov, A. and Nuaymi, L. (2015). Integrating Cellular Networks, Smart Grid, and Renewable Energy: Analysis, Architecture, and Challenges. *IEEE access,* 3**,** 2755-2770.
Hayajneh, T., Doomun, R., Al-Mashaqbeh, G. and Mohd, B. J. (2014). An Energy-Efficient and Security Aware Route Selection Protocol for Wireless Sensor Networks. *Security and Communication Networks,* 7(11)**,** 2015-2038.
He, D., Bu, J., Zhu, S., Chan, S. and Chen, C. (2011). Distributed Access Control with Privacy Support in Wireless Sensor Networks. *IEEE Transactions on wireless communications,* 10(10)**,** 3472-3481.

He, D., Chan, S. and Guizani, M. (2015a). Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications,* 14(1)**,** 389-398.
He, D., Gao, Y., Chan, S., Chen, C. and Bu, J. (2010). An Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks. *Ad hoc & sensor wireless networks,* 10(4)**,** 361-371.
He, D., Kumar, N. and Chilamkurti, N. (2015b). A Secure Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme with Pseudo Identity for Wireless Sensor Networks. *Information Sciences,* 321**,** 263-277.
Hernandez, G., Arias, O., Buentello, D. and Jin, Y. (2014). Smart Nest Thermostat: A Smart Spy in Your Home. *Black Hat USA*.
Hinterwälder, G., Moradi, A., Hutter, M., Schwabe, P. and Paar, C. (Year) Published. Full-Size High-Security Ecc Implementation on Msp430 Microcontrollers. International Conference on Cryptology and Information Security in Latin America, 2014. Springer, 31-47.
Horng, S.-J., Tzeng, S.-F., Huang, P.-H., Wang, X., Li, T. and Khan, M. K. (2015). An Efficient Certificateless Aggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks. *Information Sciences,* 317**,** 48-66.
Hossain, M., Islam, S. R., Ali, F., Kwak, K.-S. and Hasan, R. (2018). An Internet of Things-Based Health Prescription Assistant and Its Security System Design. *Future generation computer systems,* 82**,** 422-439.
Hossain, M. M., Fotouhi, M. and Hasan, R. (Year) Published. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. Services (SERVICES), 2015 IEEE World Congress on, 2015a. IEEE, 21-28.
Hossain, M. M., Fotouhi, M. and Hasan, R. (Year) Published. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. 2015 ieee world congress on services, 2015b. IEEE, 21-28.
Hsieh, W.-B. and Leu, J.-S. (2014). A Robust Ser Authentication Scheme Sing Dynamic Identity in Wireless Sensor Networks. *Wireless personal communications,* 77(2)**,** 979-989.
Hu, Z. (Year) Published. The Research of Several Key Question of Internet of Things. Intelligence Science and Information Engineering (ISIE), 2011 International Conference on, 2011. IEEE, 362-365.
Huo, F. and Gong, G. (Year) Published. A New Efficient Physical Layer Ofdm Encryption Scheme. INFOCOM, 2014 Proceedings IEEE, 2014. IEEE, 1024-1032.
Hussain, F., Ferdouse, L., Anpalagan, A., Karim, L. and Woungang, I. (2017). Security Threats in M2m Networks: A Survey with Case Study. *COMPUTER SYSTEMS SCIENCE AND ENGINEERING,* 32(2)**,** 117-135.
Hussain, F. F., Lilatul & Anpalagan, Alagan & Karim, Lutful & Woungang, Issac (2016). Security Threats in M2m Networks: A Survey with Case Study. *International Journal of Computer Systems Science and Engineering,* 32.
Hutter, M. and Schwabe, P. (Year) Published. Nacl on 8-Bit Avr Microcontrollers. International Conference on Cryptology in Africa, 2013. Springer, 156-172.
Iqbal, W., Afzal, M. and Ahmad, F. (Year) Published. An Efficient Elliptic Curve Based Signcryption Scheme for Firewalls. 2013 2nd National Conference on Information Assurance (NCIA), 2013. IEEE, 67-72.
Islam, K., Shen, W. and Wang, X. (Year) Published. Security and Privacy Considerations for Wireless Sensor Networks in Smart Home Environments.

Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2012. IEEE, 626-633.
Jaigirdar, F. T., Rudolph, C. and Bain, C. (Year) Published. Can I Trust the Data I See? A Physician's Concern on Medical Data in Iot Health Architectures. Proceedings of the Australasian computer science week multiconference, 2019. 1-10.
Jiang, C., Li, B. and Xu, H. (Year) Published. An Efficient Scheme for User Authentication in Wireless Sensor Networks. null, 2007. IEEE, 438-442.
Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J. and Yang, Y. (2016). An Untraceable Temporal-Credential-Based Two-Factor Authentication Scheme Using Ecc for Wireless Sensor Networks. *Journal of Network and Computer Applications,* 76**,** 37-48.
Jiang, R., Lai, C., Luo, J., Wang, X. and Wang, H. (2013). Eap-Based Group Authentication and Key Agreement Protocol for Machine-Type Communications. *International Journal of Distributed Sensor Networks,* 9(11)**,** 304601.
Jing, Q., Vasilakos, A. V., Wan, J., Lu, J. and Qiu, D. (2014). Security of the Internet of Things: Perspectives and Challenges. *Wireless Networks,* 20(8)**,** 2481-2501.
Jung, K.-R., Park, A. and Lee, S. (Year) Published. Machine-Type-Communication (Mtc) Device Grouping Algorithm for Congestion Avoidance of Mtc Oriented Lte Network. International Conference on Security-Enriched Urban Computing and Smart Grid, 2010. Springer, 167-178.
Kamble, A. and Bhutad, S. (Year) Published. Survey on Internet of Things (Iot) Security Issues & Solutions. 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018. IEEE, 307-312.
Kang, N., Park, J., Kwon, H. and Jung, S. (2015). Esse: Efficient Secure Session Establishment for Internet-Integrated Wireless Sensor Networks. *International Journal of Distributed Sensor Networks,* 11(8)**,** 393754.
Kavun, E. B. and Yalcin, T. (Year) Published. Ram-Based Ultra-Lightweight Fpga Implementation of Present. 2011 International Conference on Reconfigurable Computing and FPGAs, 2011. IEEE, 280-285.
Khan, R., Khan, S. U., Zaheer, R. and Khan, S. (Year) Published. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. Frontiers of Information Technology (FIT), 2012 10th International Conference on, 2012. IEEE, 257-260.
Khoo, B. (Year) Published. Rfid as an Enabler of the Internet of Things: Issues of Security and Privacy. Internet of Things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing, 2011. IEEE, 709-712.
Kim, J., Susilo, W., Au, M. H. and Seberry, J. (Year) Published. Efficient Semi-Static Secure Broadcast Encryption Scheme. International Conference on Pairing-Based Cryptography, 2013. Springer, 62-76.
Kitsos, P., Sklavos, N., Parousi, M. and Skodras, A. N. (2012). A Comparative Study of Hardware Architectures for Lightweight Block Ciphers. *Computers & Electrical Engineering,* 38(1)**,** 148-160.
Koner, C., Bhattacharjee, P. K., Bhunia, C. T. and Maulik, U. (2009). A Novel Four Entity Mutual Authentication Technique for 3-G Mobile Communications. *International Journal of Recent Trends in Engineering,* 2(2)**,** 111.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (Year) Published. A Dtls Based End-to-End Security Architecture for the Internet of Things with Two-Way Authentication. Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, 2012. IEEE, 956-963.

Krebsonsecurity (2017). All About Skimmers.

Kumar, N. C., Basit, A., Singh, P. and Venkaiah, V. C. (2018). Lightweight Cryptography for Distributed Pki Based Manets. *arXiv preprint arXiv:1804.06313*.

Lai, C., Li, H., Li, X. and Cao, J. (2015). A Novel Group Access Authentication and Key Agreement Protocol for Machine-Type Communication. *Transactions on emerging telecommunications technologies,* 26(3)**,** 414-431.

Lai, C., Li, H., Lu, R. and Shen, X. S. (2013). Se-Aka: A Secure and Efficient Group Authentication and Key Agreement Protocol for Lte Networks. *Computer Networks,* 57(17)**,** 3492-3510.

Lai, C., Lu, R., Zheng, D., Li, H. and Shen, X. S. (2016a). Glarm: Group-Based Lightweight Authentication Scheme for Resource-Constrained Machine to Machine Communications. *Computer Networks,* 99**,** 66-81.

Lai, J., Mu, Y., Guo, F., Susilo, W. and Chen, R. (Year) Published. Anonymous Identity-Based Broadcast Encryption with Revocation for File Sharing. Australasian Conference on Information Security and Privacy, 2016b. Springer, 223-239.

Lange, D. J. B. a. T. (2014a). *Safecurves: Choosing Safe Curves for Elliptic-Curve Cryptography* [Online]. Available: https://safecurves.cr.yp.to [Accessed December 1, 2014].

Lange, T. (2014b). Safecurves: Choosing Safe Curves for Elliptic-Curve Cryptography Daniel J. Bernstein University of Illinois at Chicago &.

Lara-Nino, C. A., Morales-Sandoval, M. and Diaz-Perez, A. (Year) Published. Novel Fpga-Based Low-Cost Hardware Architecture for the Present Block Cipher. 2016 Euromicro Conference on Digital System Design (DSD), 2016. IEEE, 646-650.

Laya, A., Bratu, V.-L. and Markendahl, J. (2013). Who Is Investing in Machine-to-Machine Communications?

Le, X. H., Khalid, M., Sankar, R. and Lee, S. (2011). An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare. *Journal of Networks,* 6(3)**,** 355.

Li, F., Zheng, Z. and Jin, C. (2016a). Secure and Efficient Data Transmission in the Internet of Things. *Telecommunication Systems,* 62(1)**,** 111-122.

Li, J., Wen, M. and Zhang, T. (2015). Group-Based Authentication and Key Agreement with Dynamic Policy Updating for Mtc in Lte-a Networks. *IEEE Internet of Things Journal,* 3(3)**,** 408-417.

Li, J., Wen, M. and Zhang, T. (2016b). Group-Based Authentication and Key Agreement with Dynamic Policy Updating for Mtc in Lte-a Networks. *IEEE Internet of Things Journal,* 3(3)**,** 408-417.

Li, X., Ibrahim, M. H., Kumari, S., Sangaiah, A. K., Gupta, V. and Choo, K.-K. R. (2017a). Anonymous Mutual Authentication and Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks. *Computer Networks,* 129**,** 429-443.

Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M. and Kumari, S. (2018a). A Robust Ecc-Based Provable Secure Authentication Protocol with Privacy

Preserving for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics,* 14(8)**,** 3599-3609.

Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K. and Choo, K.-K. R. (2018b). A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments. *Journal of Network and Computer Applications,* 103**,** 194-204.

Li, X., Peng, J., Niu, J., Wu, F., Liao, J. and Choo, K.-K. R. (2017b). A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. *IEEE Internet of Things Journal,* 5(3)**,** 1606-1615.

Lin, Y.-H., Huang, J.-J., Fan, C.-I. and Chen, W.-T. (2018a). Local Authentication and Access Control Scheme in M2m Communications with Computation Offloading. *IEEE Internet of Things Journal,* 5(4)**,** 3209-3219.

Lin, Y.-H., Huang, J.-J., Fan, C.-I. and Chen, W.-T. (2018b). Local Authentication and Access Control Scheme in M2m Communications with Computation Offloading. *IEEE Internet of Things journal*.

Liu, A. and Ning, P. (Year) Published. Tinyecc: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. Proceedings of the 7th international conference on Information processing in sensor networks, 2008. IEEE Computer Society, 245-256.

Liu, J., Xiao, Y., Li, S., Liang, W. and Chen, C. P. (2012). Cyber Security and Privacy Issues in Smart Grids. *IEEE Communications Surveys & Tutorials,* 14(4)**,** 981-997.

Liu, Z., Seo, H., Großschädl, J. and Kim, H. (2015). Efficient Implementation of Nist-Compliant Elliptic Curve Cryptography for 8-Bit Avr-Based Sensor Nodes. *IEEE Transactions on Information Forensics and Security,* 11(7)**,** 1385-1397.

Liu, Z., Weng, J., Hu, Z. and Seo, H. (2016). Efficient Elliptic Curve Cryptography for Embedded Devices. *ACM Transactions on Embedded Computing Systems (TECS),* 16(2)**,** 1-18.

Liu, Z., Wenger, E. and Großschädl, J. (Year) Published. Mote-Ecc: Energy-Scalable Elliptic Curve Cryptography for Wireless Sensor Networks. International Conference on Applied Cryptography and Network Security, 2014. Springer, 361-379.

Machado, C. and Fröhlich, A. a. M. (Year) Published. Iot Data Integrity Verification for Cyber-Physical Systems Using Blockchain. 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), 2018. IEEE, 83-90.

Maes, R. (2012). Physically Unclonable Functions: Constructions, Properties and Applications (Fysisch Onkloonbare Functies: Constructies, Eigenschappen En Toepassingen).

Mahalle, P. N., Anggorojati, B., Prasad, N. R. and Prasad, R. (2013). Identity Authentication and Capability Based Access Control (Iacac) for the Internet of Things. *Journal of Cyber Security and Mobility,* 1(4)**,** 309-348.

Mahmoud, R., Yousuf, T., Aloul, F. and Zualkernan, I. (Year) Published. Internet of Things (Iot) Security: Current Status, Challenges and Prospective Measures. Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for, 2015. IEEE, 336-341.

Maitra, T., Amin, R., Giri, D. and Srivastava, P. (2016). An Efficient and Robust User Authentication Scheme for Hierarchical Wireless Sensor Networks without Tamper-Proof Smart Card. *IJ Network Security,* 18(3)**,** 553-564.

Martínez-Ballesté, A., Pérez-Martínez, P. A. and Solanas, A. (2013). The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible. *IEEE Communications Magazine,* 51(6)**,** 136-141.

Mavrogiorgou, A., Kiourtis, A., Perakis, K., Pitsios, S. and Kyriazis, D. (2019). Iot in Healthcare: Achieving Interoperability of High-Quality Data Acquired by Iot Medical Devices. *Sensors,* 19(9)**,** 1978.

Meddeb, M., Dhraief, A., Belghith, A., Monteil, T., Drira, K. and Gannouni, S. (2018). Afirm: Adaptive Forwarding Based Link Recovery for Mobility Support in Ndn/Iot Networks. *Future Generation Computer Systems,* 87**,** 351-363.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. *Ad hoc networks,* 10(7)**,** 1497-1516.

Mišić, J., Mišić, V. B. and Khan, N. (2017). Sharing It My Way: Efficient M2m Access in Lte/Lte-a Networks. *IEEE Transactions on Vehicular Technology,* 66(1)**,** 696-709.

Mitrokotsa, A., Rieback, M. R. and Tanenbaum, A. S. (2010). Classification of Rfid Attacks. *Gen,* 15693**,** 14443.

Montgomery, P. L. (1987). Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of computation,* 48(177)**,** 243-264.

Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S. and Isoaho, J. (2018a). Low-Latency Approach for Secure Ecg Feature Based Cryptographic Key Generation. *IEEE Access,* 6**,** 428-442.

Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S. and Isoaho, J. (2018b). Performance Analysis of End-to-End Security Schemes in Healthcare Iot. *Procedia computer science,* 130(C)**,** 432-439.

Moosavi, S. R., Nigussie, E., Virtanen, S. and Isoaho, J. (Year) Published. Cryptographic Key Generation Using Ecg Signal. 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2017a. IEEE, 1024-1031.

Moosavi, S. R., Nigussie, E., Virtanen, S. and Isoaho, J. (Year) Published. Cryptographic Key Generation Using Ecg Signal. Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual, 2017b. IEEE, 1024-1031.

Mosenia, A. and Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing,* 5(4)**,** 586-602.

Mukherjee, A. (2015). Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints. *Proceedings of the IEEE,* 103(10)**,** 1747-1761.

Naru, E. R., Saini, H. and Sharma, M. (Year) Published. A Recent Review on Lightweight Cryptography in Iot. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017. IEEE, 887-890.

Nawari, M., Ahmed, H., Hamid, A. and Elkhidir, M. (Year) Published. Fpga Based Implementation of Elliptic Curve Cryptography. 2015 World Symposium on Computer Networks and Information Security (WSCNIS), 2015. IEEE, 1-8.

Noura, H., Melki, R., Chehab, A., Mansour, M. M. and Martin, S. (Year) Published. Efficient and Secure Physical Encryption Scheme for Low-Power Wireless

M2m Devices. 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018a. IEEE, 1267-1272.
Noura, H. N., Melki, R., Chehab, A. and Mansour, M. M. (2018b). A Physical Encryption Scheme for Low-Power Wireless M2m Devices: A Dynamic Key Approach. *Mobile Networks and Applications***,** 1-17.
Novelan, M., Husein, A., Harahap, M. and Aisyah, S. (Year) Published. Sms Security System on Mobile Devices Using Tiny Encryption Algorithm. Journal of Physics: Conference Series, 2018. IOP Publishing, 012037.
Odelu, V., Das, A. K., Rao, Y. S., Kumari, S., Khan, M. K. and Choo, K.-K. R. (2017). Pairing-Based Cp-Abe with Constant-Size Ciphertexts and Secret Keys for Cloud Environment. *Computer Standards & Interfaces,* 54**,** 3-9.
Oliveira, T., López, J., Hışıl, H., Faz-Hernández, A. and Rodríguez-Henríquez, F. (Year) Published. How to (Pre-) Compute a Ladder. International Conference on Selected Areas in Cryptography, 2017. Springer, 172-191.
Oualha, N. and Nguyen, K. T. (Year) Published. Lightweight Attribute-Based Encryption for the Internet of Things. 2016 25th International Conference on Computer Communication and Networks (ICCCN), 2016. IEEE, 1-6.
Padmavathi, D. G. and Shanmugapriya, M. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *arXiv preprint arXiv:0909.0576*.
Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G. and Dohler, M. (2013). Standardized Protocol Stack for the Internet of (Important) Things. *IEEE communications surveys & tutorials,* 15(3)**,** 1389-1406.
Pandey, J. G., Goel, T. and Karmakar, A. (Year) Published. A High-Performance and Area-Efficient Vlsi Architecture for the Present Lightweight Cipher. 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018. IEEE, 392-397.
Parne, B. L., Gupta, S. and Chaudhari, N. S. (2018). Segb: Security Enhanced Group Based Aka Protocol for M2m Communication in an Iot Enabled Lte/Lte-a Network. *IEEE Access,* 6**,** 3668-3684.
Parno, B., Perrig, A. and Gligor, V. (Year) Published. Distributed Detection of Node Replication Attacks in Sensor Networks. Security and Privacy, 2005 IEEE Symposium on, 2005. IEEE, 49-63.
Prasetyo, K. N., Purwanto, Y. and Darlis, D. (Year) Published. An Implementation of Data Encryption for Internet of Things Using Blowfish Algorithm on Fpga. 2014 2nd International Conference on Information and Communication Technology (ICoICT), 2014. IEEE, 75-79.
Qiu, Y. and Ma, M. (2016). A Mutual Authentication and Key Establishment Scheme for M2m Communication in 6lowpan Networks. *IEEE Transactions on Industrial Informatics,* 12(6)**,** 2074-2085.
Rabah, K. (2005). Elliptic Curve Elgamal Encryption and Signature Schemes. *Information technology journal,* 4(3)**,** 299-306.
Rachmawati, D., Sharif, A. and Budiman, M. A. (Year) Published. Hybrid Cryptosystem Using Tiny Encryption Algorithm and Luc Algorithm. IOP Conference Series: Materials Science and Engineering, 2018. IOP Publishing, 012042.
Rai, A. K., Tewari, R. R. and Upadhyay, S. K. (2010). Different Types of Attacks on Integrated Manet-Internet Communication. *International Journal of Computer Science and Security,* 4(3)**,** 265-274.

Rajesh, S., Paul, V., Menon, V. G. and Khosravi, M. R. (2019). A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded Iot Devices. *Symmetry,* 11(2)**,** 293.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM,* 21(2)**,** 120-126.

Rolfes, C., Poschmann, A., Leander, G. and Paar, C. (Year) Published. Ultra-Lightweight Implementations for Smart Devices–Security for 1000 Gate Equivalents. International Conference on Smart Card Research and Advanced Applications, 2008. Springer, 89-103.

Roman, R., Najera, P. and Lopez, J. (2011). Securing the Internet of Things. *Computer,* 44(9)**,** 51-58.

Roman, R., Zhou, J. and Lopez, J. (2013). On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks,* 57(10)**,** 2266-2279.

Sahai, A. and Waters, B. (Year) Published. Fuzzy Identity-Based Encryption. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2005. Springer, 457-473.

Sbeiti, M., Silbermann, M., Poschmann, A. and Paar, C. (Year) Published. Design Space Exploration of Present Implementations for Fpgas. 2009 5th Southern Conference on Programmable Logic (SPL), 2009. IEEE, 141-145.

Selvi, S. S. D., Vivek, S. S., Srinivasan, R. and Rangan, C. P. (Year) Published. An Efficient Identity-Based Signcryption Scheme for Multiple Receivers. International Workshop on Security, 2009. Springer, 71-88.

Seys, S. and Preneel, B. (Year) Published. Authenticated and Efficient Key Management for Wireless Ad Hoc Networks. Proceedings of the 24th Symposium on Information Theory in the Benelux, 2003. Werkgemeenschap voor Informatie-en Communicatietheorie, 195-202.

Shen, Y.-L. (Year) Published. An Access Control Scheme in Wireless Sensor Networks. Proc. 4th IFIP International Conference on Network and Parallel Computing Workshops (NPC2007), Sept., 2007. 362-367.

Shi, W. and Gong, P. (2013). A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *International Journal of Distributed Sensor Networks,* 9(4)**,** 730831.

Singh, D., Tripathi, G. and Jara, A. J. (Year) Published. A Survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services. Internet of things (WF-IoT), 2014 IEEE world forum on, 2014. IEEE, 287-292.

Song, T., Li, R., Mei, B., Yu, J., Xing, X. and Cheng, X. (2017). A Privacy Preserving Communication Protocol for Iot Applications in Smart Homes. *IEEE Internet of Things Journal,* 4(6)**,** 1844-1852.

Srilaya, S. and Velampalli, S. (2020). Cryptography: The Key Technology for Security Management. *International Journal of Research and Analytical Reviews,* 7(1).

Stajano, F. and Anderson, R. (2002). The Resurrecting Duckling: Security Issues for Ubiquitous Computing. *Computer,* 35(4)**,** supl22-supl26.

Stallings, W. (2006). *Cryptography and Network Security, 4/E.* Pearson Education India.

Szczechowiak, P., Oliveira, L. B., Scott, M., Collier, M. and Dahab, R. (Year) Published. Nanoecc: Testing the Limits of Elliptic Curve Cryptography in

Sensor Networks. European conference on Wireless Sensor Networks, 2008. Springer, 305-320.
Tanaka, H. (Year) Published. Information Leakage Via Electromagnetic Emanation and Effectiveness of Averaging Technique. Information Security and Assurance, 2008. ISA 2008. International Conference on, 2008. IEEE, 98-101.
Tay, J., Wong, M. D., Wong, M., Zhang, C. and Hijazin, I. (Year) Published. Compact Fpga Implementation of Present with Boolean S-Box. 2015 6th Asia Symposium on Quality Electronic Design (ASQED), 2015. IEEE, 144-148.
Tehranipoor, M. and Koushanfar, F. (2010). A Survey of Hardware Trojan Taxonomy and Detection. *IEEE design & test of computers*, 27(1).
Toorani, M. and Beheshti, A. A. (2010). Cryptanalysis of an Elliptic Curve-Based Signcryption Scheme. *arXiv preprint arXiv:1004.3521*.
Touati, L. and Challal, Y. (Year) Published. Batch-Based Cp-Abe with Attribute Revocation Mechanism for the Internet of Things. 2015 International Conference on Computing, Networking and Communications (ICNC), 2015a. IEEE, 1044-1049.
Touati, L. and Challal, Y. (Year) Published. Efficient Cp-Abe Attribute/Key Management for Iot Applications. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015b. IEEE, 343-350.
Touati, L. and Challal, Y. (Year) Published. Collaborative Kp-Abe for Cloud-Based Internet of Things Applications. 2016 IEEE International Conference on Communications (ICC), 2016. IEEE, 1-7.
Touati, L., Challal, Y. and Bouabdallah, A. (Year) Published. C-Cp-Abe: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things. 2014 International Conference on Advanced Networking Distributed Systems and Applications, 2014. IEEE, 64-69.
Tsai, K. L., Huang, Y. L., Leu, F. Y., Tan, J. S. and Ye, M. (Year) Published. High-Efficient Multi-Key Exchange Protocol Based on Three-Party Authentication. 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2014. IEEE, 487-492.
Tuna, G., Kogias, D. G., Gungor, V. C., Gezer, C., Taşkın, E. and Ayday, E. (2017). A Survey on Information Security Threats and Solutions for Machine to Machine (M2m) Communications. *Journal of Parallel and Distributed Computing*, 109**,** 142-154.
Turner, S. and Polk, T. (Year) Published. Security Challenges for the Internet of Things. IAB Interconnecting Smart Objects with the Internet Workshop, Prague, Czech Republic, 2011.
Vaidya, B., Makrakis, D. and Mouftah, H. T. (Year) Published. Improved Two-Factor User Authentication in Wireless Sensor Networks. Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on, 2010. IEEE, 600-606.
Vasserman, E. Y. and Hopper, N. (2013). Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE transactions on mobile computing*, 12(2)**,** 318-332.

Von Oheimb, D. (Year) Published. The High-Level Protocol Specification Language Hlpsl Developed in the Eu Project Avispa. Proceedings of APPSEM 2005 workshop, 2005. 1-17.
Walters, J. P., Liang, Z., Shi, W. and Chaudhary, V. (2007). Wireless Sensor Network Security: A Survey. *Security in distributed, grid, mobile, and pervasive computing,* 1**,** 367.
Wang, H. and Li, Q. (2012). Achieving Distributed User Access Control in Sensor Networks. *Ad Hoc Networks,* 10(3)**,** 272-283.
Wen-Bin Hsieh, J.-S. L. (2013). A Robust User Authentication Scheme Using Dynamic
Identity in Wireless Sensor Networks. *Wireless Pers Commun*.
Wenger, E., Unterluggauer, T. and Werner, M. (Year) Published. 8/16/32 Shades of Elliptic Curve Cryptography on Embedded Processors. International Conference on Cryptology in India, 2013. Springer, 244-261.
Wu, F., Xu, L., Kumari, S. and Li, X. (2017). A Privacy-Preserving and Provable User Authentication Scheme for Wireless Sensor Networks Based on Internet of Things Security. *Journal of Ambient Intelligence and Humanized Computing,* 8(1)**,** 101-116.
Wu, W. and Zhang, L. (Year) Published. Lblock: A Lightweight Block Cipher. International Conference on Applied Cryptography and Network Security, 2011. Springer, 327-344.
Xue, K., Ma, C., Hong, P. and Ding, R. (2013). A Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks. *Journal of Network and Computer Applications,* 36(1)**,** 316-323.
Yalla, P. and Kaps, J.-P. (Year) Published. Lightweight Cryptography for Fpgas. 2009 International Conference on Reconfigurable Computing and FPGAs, 2009. IEEE, 225-230.
Yan-Rong, S. and Tao, H. (Year) Published. Internet of Things Key Technologies and Architectures Research in Information Processing. Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013.
Yang, G., Xu, J., Chen, W., Qi, Z.-H. and Wang, H.-Y. (2010). Security Characteristic and Technology in the Internet of Things. *Nanjing Youdian Daxue Xuebao(Ziran Kexue Ban)/ Journal of Nanjing University of Posts and Telecommunications(Natural Nanjing University of Posts and Telecommunications(Natural,* 30(4).
Yang, X., Li, Z., Geng, Z. and Zhang, H. (2012). A Multi-Layer Security Model for Internet of Things. *Internet of Things.* (pp. 388-393). Springer.
Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things journal,* 4(5)**,** 1250-1258.
Yao, J., Wang, T., Chen, M., Wang, L. and Chen, G. (Year) Published. Gbs-Aka: Group-Based Secure Authentication and Key Agreement for M2m in 4g Network. 2016 International Conference on Cloud Computing Research and Innovations (ICCCRI), 2016. IEEE, 42-48.
Yao, X., Chen, Z. and Tian, Y. (2015). A Lightweight Attribute-Based Encryption Scheme for the Internet of Things. *Future Generation Computer Systems,* 49**,** 104-112.

Yeh, H.-L., Chen, T.-H., Liu, P.-C., Kim, T.-H. and Wei, H.-W. (2011). A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors,* 11(5)**,** 4767-4779.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things journal,* 1(1)**,** 22-32.

Zhang, G.-H., Poon, C. C. and Zhang, Y.-T. (2011). Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine,* 16(1)**,** 176-182.

Zhang, R., Zhang, Y. and Ren, K. (Year) Published. Dp²ac: Distributed Privacy-Preserving Access Control in Sensor Networks. IEEE INFOCOM 2009, 2009. IEEE, 1251-1259.

Zhang, Y. (Year) Published. Technology Framework of the Internet of Things and Its Application. Electrical and Control Engineering (ICECE), 2011 International Conference on, 2011. IEEE, 4109-4112.

Zhdanov, O. N. and Sokolov, A. V. (2016). Block Symmetric Cryptographic Algorithm Based on Principles of Variable Block Length and Many-Valued Logic. *Far East Journal of Electronics and Communications,* 16(3)**,** 573-589.

Zheng, Y. (Year) Published. Digital Signcryption or How to Achieve Cost (Signature & Encryption)≪ Cost (Signature)+ Cost (Encryption). Annual International Cryptology Conference, 1997. Springer, 165-179.

Zhou, Z., Zhang, H., Du, X., Li, P. and Yu, X. (Year) Published. Prometheus: Privacy-Aware Data Retrieval on Hybrid Cloud. INFOCOM, 2013 Proceedings IEEE, 2013. IEEE, 2643-2651.

Zhu, H., Lin, X., Zhang, Y. and Lu, R. (2015). Duth: A User-Friendly Dual-Factor Authentication for Android Smartphone Devices. *Security and Communication Networks,* 8(7)**,** 1213-1222.

Zia, M. and Ali, R. (2018). Cryptanalysis and Improvement of an Elliptic Curve Based Signcryption Scheme for Firewalls. *PloS one,* 13(12)**,** e0208857.