Thesis for the Degree of Doctor of Philosophy

ZERO-INTERACTION PAIRING AND AUTHENTICATION USING MOMS SECRET AND CONTEXTUAL CO-PRESENCE OF DEVICES

Ubaid Ur Rehman

Department of Computer Science and Engineering
Graduate School
Kyung Hee University
Seoul, Korea

February 2023

ZERO-INTERACTION PAIRING AND AUTHENTICATION USING MOMS SECRET AND CONTEXTUAL CO-PRESENCE OF DEVICES

Ubaid Ur Rehman

Department of Computer Science and Engineering
Graduate School
Kyung Hee University
Seoul, Korea

February 2023

Zero-Interaction Pairing and Authentication Using Moms Secret and Contextual Co-presence of Devices

by

Ubaid Ur Rehman

Supervised by

Prof. Sungyoung Lee

Prof. Seong-Bae Park

Submitted to the Department of Computer Science and Engineering and the Faculty of Graduate School of Kyung Hee University in partial fulfilment of the requirements of the degree of Doctor of Philosophy

Dissertation Committee:

Prof. Eui-Nam Huh*

Prof. Sung-Ki Kim

Prof. Jinsung Cho

Prof. Seong Tae Kim

Prof. Seong-Bae Park

Prof. Sungyoung Lee

I would like to dedicate my thesis to my beloved parents, siblings, my wife, and the innocent childhood of my daughter & son, who played a pivotal role for supporting me through out my PhD journey. Thank you so much for being a part of my life.

Abstract

The emergence of Internet-of-Things (IoT) presents significant challenges to security and privacy. IoT are usually constrained devices with limited resources in terms of power, memory, computation, and battery life. The consumer arena prioritizes the time to market at the expense of compromising security. The lack of standardization for IoT development at the initial stage has inherited the vulnerabilities. However, the recent tsunami of IoT devices has created a variety of competing technologies that lead to a highly fragmented threat model. These technologies have evolved our daily life with wearables and sensors, which analyze the ambient context and collects information about a specific entity. The collected contextual data can be used to evolve the user's daily life such as cost reduction-based energy management systems, home automation, and autonomous driving. These innovative technologies have access to highly sensitive information, often personal data, and become an active target of an attack. The constrained property of an IoT device makes it the weakest link of the connected network and often targeted by adversaries for exploitation. The current security measures such as conventional cryptography, Adhoc patches, and security policies are not adequate protection for these devices.

This thesis focus on the zero interaction pairing and authentication that identify the device based on its physical, virtual, or ambient context. We have identified that the existing approaches use the device's physical context as a dynamic credential for pairing and authentication, which has low entropy and require time synchronization. To solve this problem, we have proposed the Median of medians (Moms) secret key that converts the low entropy context to high entropy using time intervals. Similarly, we have identified the vulnerability of network key transportation in the user assistance pairing using virtual context and proposed an efficient zero-effort scheme, which ensures the mutual authentication and key provision among the devices using a self-signed identifier and integrated encryption scheme respectively. Moreover, the existing approaches for identifying the devices based on the contextual co-presence require sufficient data for adequate security and utilize an error correction mechanism, which leads to prolonged pairing time and contextual co-presence attacks respectively. For this purpose, we have used the Moms secret that analyze the multimodal data and selects a specific data dimension from each modality based on randomness and similarity, which leads to the reduction of pairing time. Additionally, we have used the password-authenticated key exchange instead of an error correction mechanism that ensures strong resistance against the contextual co-presence attack. The proposed approaches were evaluated using publicly available datasets and compared with the state-of-the-art. The evaluation result shows that the proposed approach reduces the operational overhead on the devices and improve security by providing strong resistance against contextual co-presence attack.

Acknowledgement

All praises be to Allah, the Lord of all the existence for his blessings. Thank you so much for giving me the valor and courage to complete my doctoral study. This work presents five years of mental toil, emotional conflicts, and insomnia. The effort is not mine only, but countless efforts and prayers are put in by my parents, teachers, friends, and family. I would like to express my sincere gratitude to all of them for their continuous support. However, there are those, without which this accomplishment may not be able to achieve.

Among them are my advisors, Professor Sungyoung Lee and Professor Seong-Bae Park. They provided me with courage, strength, and support during my PhD duration. Their experience and guidance help me to solve different challenges during my time as a student. Their high hopes and spirit make me aim higher than I thought. Therefore, I am extremely thankful to them for playing an important role in polishing my technical and research skills, and making me multi-tasking to prove my capabilities and competency in domestic and international collaborative industry-academia projects.

I am highly thankful to Professor Anita Sant'Anna from Halmstad University, Sweden for supervising me during my three months as a visiting researcher over there. I would like to express my sincere gratitude to my parents and siblings. Their continuous support and prayers make this journey possible. Moreover, I would like to thank my wife Mrs. Maleeha for her patience and endless support during this hard time. Finally, my daughter Rafiya Rehman and son Rubaid Ur Rehman are the greatest gifts and sources of inspiration from Allah.

Ubaid Ur Rehman

February, 2023

Table of Contents

List of Figures

List of Algorithms

Chapter 1

Introduction

The world is growing more connected with technological advancements. These interconnected devices have facilitated user's by providing a variety of services at their fingertips without effort. The connected technologies have proved Moore's law in terms of device size, computation, and performance. The production cost of computers and their peripheral devices has also been reduced, smaller and faster as compared with traditional mainframe systems. The embedded systems are found everywhere, even invisible to us. These embedded devices are cost-effective, often used for data acquisition, processing, and decision-making tasks in different application areas such as smart manufacturing, wireless sensor network, self-driving vehicles, health monitoring systems, and many consumer applications. Besides these advantages, the embedded devices are resource constrained with limited memory, computation, and battery lifetime. Therefore, a specific protocol or algorithm is deployed on these devices to fulfill the required task. The resource-constrained nature of these devices makes them vulnerable to a variety of security threats. The research community has exploited and proposed patches for these vulnerabilities. But due to competitive business, the consumer arena still prioritizes the time to market at the expense of compromising security. Also, cheap production may compromise quality assurance and security testing. When such devices become a part of the network, then it is considered as the weakest link and the adversary often targets them to get access to the network.

The Internet-of-Things (IoT) become popular by introducing the smart feature in the network, where the connected devices utilize the knowledge bases or machine learning to sense, anticipate and take actions considering the desires of users. Figure 1.1 presents the prominent application areas of IoT. These technological tsunamis of IoT have evolved our life with smart services such as healthcare, transportation, homes, and industries. IoT includes heterogeneous devices such as ac-

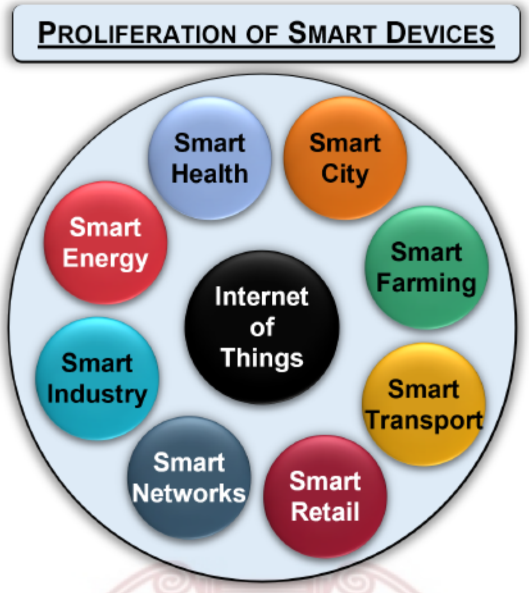


Figure 1.1: Proliferation of Smart Device in Different Domains

tuators, sensors, and smart nodes, which exchange network information and provide personalized services. The IoT devices have limited resources in terms of memory, energy, computation, and processing capabilities. The vast number of devices' connectivity may lead to several challenges such as scalability, diversified protocols, and communication channels. The IoT relies on two types of networks such as server-based and peer-to-peer. In the server-based, the server is responsible to process all the data, ensure data privacy, and provide services to the client. In this way, the overhead on the client side is minimized, but it leads to one-point failure. In case of failure, the whole network will be down. On the contrary, in peer-to-peer, each client process the data and provide relevant services to its neighboring node. The peer-to-peer network is easy to establish, but it has very minimum security measures and became the target of an adversary.

Pairing and authentication are used to ensure secure communication between communicating entities. The rapid increase of smart devices plays an important role in daily life, ranging from businesses to household management and healthcare services [1,2]. According to [3,4], the number of smart devices will increase three times by 2025, enabling a sustainable environment with autonomous processes that reduce cost and increase productivity [5]. On the downside, these smart devices collect physical, virtual, and ambient contextual data that leads to a wide range of security and privacy concerns [6, 7]. The collected data may have personally identifiable information and its leakage or misuse may have severe consequences [8, 9]. Moreover, IoT devices lack security standards, leading to vendor-specific mechanisms and provide weak security. The traditional cryptographic mechanism required fine-tuning to be deployed on these constrained devices. Therefore, new approaches need to be proposed that considered the limitation of constrained devices and provide optimum security to ensure strong resistance against a variety of attacks.

1.1 Motivation

The rapid growth of IoT needs the protection of devices and its transmitted data. IoT provide personalized service by analyzing the collected data from wearable and sensors. The attacker usually target the IoT for launching a variety of attacks such as masquerading, man in the middle, replay, and eavesdropping [10, 11]. These attacks not only compromise the privacy, but also leads to severe consequences such as identity theft, evidence tampering, and ransomware [12, 13]. The traditional security mechanism provide confidentiality, integrity, authentication, and authorization. Pairing allows the establishment of shared secret key among the communicating entities without the involvement of trusted third party, ensuring data confidentiality and integrity. While authentication identify and validate the identity of communicating entities, providing data origin authentication. In IoT, pairing and authentication provide strong resistance against a variety of attacks by protecting the data transmitted over the communication channel and prevent the devices from malicious code [14, 15].

Pairing and authentication are broadly divided into user assistance and zero interaction. The user assistance pairing and authentication utilizes the predefined credentials for managing the secure communication between the communicating devices [16, 17]. Figure 1.2 presents the conceptual workflow of the user assistance pairing and authentication. The predefined credentials includes the password, Quick Response (QR) code, or bar code. As the name depict, the user assistance is required for initial authentication by entering the password or scanning the QR/bar code. Usually smartphone is utilized to scan/enter the credential and transmit via Wireless Fidelity (WiFi) channel. upon receiving the device credential, the coordinator share network key and the corresponding device become the part of network. With the increasing number of IoT devices, the high user effort

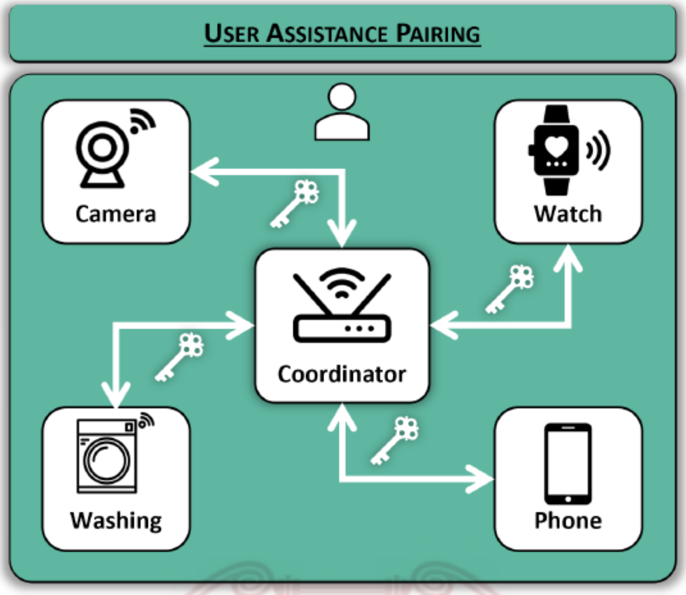


Figure 1.2: User Assistance Pairing and Authentication

will be needed during the initial management of devices. In order to solve the high user effort issue, the Zero Interaction Pairing and Authentication (ZIPA) was introduce, which eliminate the user assistance and utilize the contextual data as a security credential for identification and validation of devices [18, 19]. Figure 1.3 present the conceptual mechanism of ZIPA, where the targeted device use the physical, virtual, or ambient context, collected from smart device's on-board sensors. The collected contextual data decides the acceptance and rejection of devices [20]. The ZIPA do not require the another communication medium for transmission of security credentials and improve the network scalability.

With the constrained nature of IoT in terms of power, memory, computation, and battery life. The user assistance pairing and authentication are not suitable to be deployed directly because it relay on public key cryptography that required proper tailoring for deployment on constrained node. Therefore, the IoT preferred ZIPA due to its autonomous pairing and authentication without any prior association requirement. Despite these benefits, the ZIPA scheme utilize the contextual data that has low entropy and according to the Shannon Entropy in information theory [21], the low entropy value leads to high information gain. Based on this theory, the existing ZIPA schemes are vulnerable to brute-force and contextual co-presence attack [22, 23]. To solve the low entropy

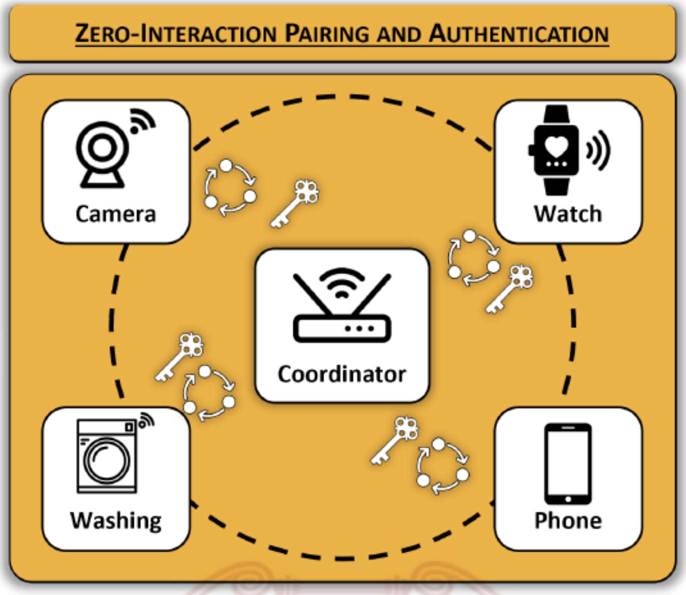


Figure 1.3: Zero Interaction Pairing and Authentication

issue, the existing approaches requires sufficient contextual data to provide adequate security that results in prolong pairing time [19,20,24–30]. Moreover, the existing user assistance pairing utilize the device virtual context that exists in plain text, the exploitation of this vulnerability can lead to key transportation attack, specifically during the network key sharing at the initial authentication phase [31–35]. Therefore, we are motivated to design an efficient ZIPA scheme that convert the low entropy contextual values to high entropy, reduces the pairing time, and ensure strong resistance against predictive contextual and key transportation attacks.

1.2 Challenges and Goal

The ultimate goal of this thesis is to design an efficient ZIPA mechanism that reduce the pairing time and ensure strong resistance against predictive contextual and key transportation attacks. To achieve this goal, we systematically analyze the existing literature related to ZIPA and identify its limitations. Base on the identified limitation, we have proposed the state-of-the-art ZIPA scheme and evaluated it with the publicly available datasets, which depict the real-world scenarios. According to the evaluation results, our proposed methodology provide strong resistance against a variety of attacks, improve the security and reduce the pairing time compared to the existing approaches. The ZIPA uses contextual data (physical, virtual, and ambient context) that have low entropy and leads to predictive contextual attacks. Therefore, the existing approaches require sufficent data for adequate security that results in prolong pairing time. Moreover, the existing user assistance pairing is also vulnerable to key transportation attacks. Some of the recent studies have considered these issues, but it required time synchronization, vulnerable to contextual co-presence attack, and take prolong pairing time. To solve these challenges, we have designed an efficient ZIPA mechanism that reduces the pairing time and ensure strong resistance against predictive contextual and key transportation attacks. The target goals are as follows:

Independent of Time Synchronization: For the server-based network, the existing ZIPA mechanism uses the device physical context as dynamic credential, which required the time synchronization among the client and server. In reality, achieving the time synchronization on commodity devices are infeasible and attacker can also exploit this vulnerability to launch an asynchronous attack. Therefore, we have considered an interval based approach for selecting the contextual information.

High Entropy and Low Information Gain: The device physical context have low entropy, which can be predicted by passive analysis or bruteforce attack. Therefore, we have proposed the median-of-medians (Moms) secret that convert the low entropy value to high entropy to reduce the information gain.

Reduction of Operational Overhead: The existing ZIPA scheme required user assistance for analyzing the device virtual context, which is vulnerable to key transportation attack. Either the device virtual context is globally available or transmitted in plaintext. Therefore, we have proposed the zero-effort approach that reduce the operational overhead by using the device virtual context for identification and shared key generation without user assistance.

Reduction of Pairing Time: The existing ZIPA scheme collect multi-modality data from co-presence environment and generate the device fingerprint by taking an average or single medical of each modality and concatenate it to increase the search space. According to our analysis the data collected from one modality with multiple dimension has similarity pattern, that increase the overhead on each peer. Therefore, our propose methodology considered one dimensional per

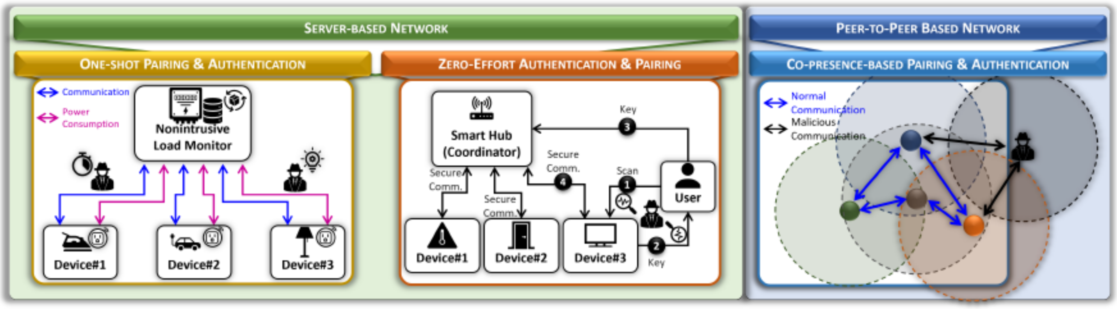


Figure 1.4: Overview of Research Scope to Improve Security

modality for generating the device fingerprint and reduces the pairing time.

Resistance against Contextual Co-presence Attack: The existing ZIPA scheme utilizes the fuzzy-based approach for contextual pattern, which allow and correct a certain amount of error in the contextual data pattern. The adversary exploit this feature and launch the contextual co-presence attack. We have utilizes the password authentication key exchange instead of the fuzzy-based approaches to provide resistance against such type of attacks.

1.3 Key Contributions

The key contributions of this thesis are described as follows:

1.3.1 Analysis of Existing Schemes

We analyzed the existing ZIPA schemes and categorized them based on the network architecture into server-based and peer-to-peer. In the server-based ZIPA scheme, the server verify and validate the end devices based on physical context or virtual context. The physical context include the unique property of device such as power consumption. While the virtual context include the personal identification number, password, or quick response code. In the peer-to-peer network, each device collect the ambient context using their own board sensors and verify the neighboring devices. Also, we find that the existing ZIPA schemes are vulnerable to a variety of attacks such as guessing, asynchronous, key transportation, masquerading, man-in-the-middle, and replay. Moreover, some of the existing schemes require user assistance. Therefore, we identified critical security, privacy, usability, and pairing time issues. Figure 1.4 present the scope of our thesis in term of attacking perspective.

1.3.2 Median-of-Medians (Moms) Secret

We address the problem of time synchronization and low entropy contextual information by proposing the median-of-medians (Moms) secret, which uses the interval based data that is independent of time synchronization and convert the low entropy values into high by taking the medians. The Moms secret can be used as a dynamic credential for ZIPA schemes that ensure the randomness and prevent information leakage.

1.3.3 Device Virtual Context as Self-signed Identifier

To ensure prevention against the key transportation attack, we proposed zero-effort protocol that utilizes the device virtual context as a self-signed identifier (instead of considering it as a key) for mutual authentication and then generate a shared key based on integrated encryption scheme. With this approach, the existing user assistance schemes can be evolved to zero-interaction and automate the joining process of new device, which will reduce the operational overhead and also mitigate the vulnerabilities of masquerading, man-in-the-middle, key transportation, and replay attacks.

1.3.4 Pairing Time Reduction

We solve the problem of prolong pairing time by selecting one data dimension from each modality based on the similarity, then use the selected data dimension from all the modalities for device fingerprint generation using Moms secret that significantly decrease it predictability, increase the entropy and reduce the pairing time.

1.3.5 Resistance against Contextual Co-presence Attack

The existing approaches adopt the fuzzy-based approach for ZIPA such as Reed-Solomon code that detect and correct multiple symbol errors. The adversary can exploit this vulnerability to launch the contextual co-presence attack. To solve this issue, we adopt the password authenticated

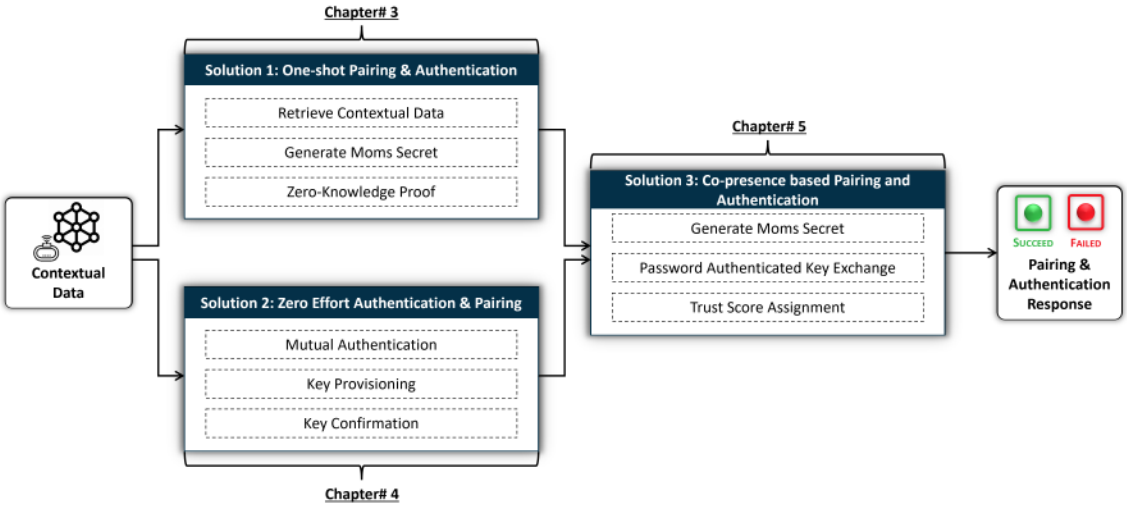

Chapter# 3
Solution 1: One-shot Pairing & Authentication
Retrieve Contextual Data
Generate Moms Secret
Zero-Knowledge Proof
Contextual Data
Solution 2: Zero Effort Authentication & Pairing
Mutual Authentication
Key Provisioning
Key Confirmation
Chapter# 4
Chapter# 5
Solution 3: Co-presence based Pairing and Authentication
Generate Moms Secret
Password Authenticated Key Exchange
Trust Score Assignment
Succeed
Failed
Pairing & Authentication Response

Figure 1.5: Idea Diagram Representation and Mappings of Chapters

key exchange and integrate it with Moms secret, which results in reducing the pairing time and improving the security. In this way, the security is completely dependent on the generated Moms secret. The innovative design of Moms secret with PAKE provide strong resistance against the contextual co-presence attack.

1.4 Thesis Organization

This dissertation aims at investigating an efficient zero interaction pairing and authentication method that reduces the pairing time and ensure strong resistance against predictive contextual and key transportation attacks. Figure 1.5 presents the bird-eye view of the dissertation and connectivity between different components. The rest of thesis is organized as follows.

- **Chapter 1: Introduction**. Chapter 1 described the brief introduction of pairing and authentication schemes, which contains many vulnerabilities and its exploitation may leads to severe consequences. It focus on the motivation of this research, preliminary definitions, problems in areas, the goal to solve these problems and key contributions that achieved through this research work. Finally, this chapter conclude with the organization of this dissertation.

- **Chapter 2: Related work**. Chapter 2 provides detailed literature review of the studies related to zero interaction and pairing. This section described the literature in terms of one-shot, zero-effort, and co-presence-based pairing and authentication. For each of these area, the strengths and weakness are summarized that provide a base for supporting our proposed approach.

- **Chapter 3: One-shot Pairing and Authentication**. In this chapter we have describe our first solution that use the device physical context to ensure the pairing with server. Moreover, this chapter briefly describe our proposed Median-of-medians (Moms) secret key generation and proof the key sharing with zero knowledge proof. The evaluation of the proposed approach was illustrated in terms of entropy assessment, probability of guessing context, and time complexity. Based on the evaluation results, our proposed approach perform very-well as compare with the existing approaches.

- **Chapter 4: Zero-Effort Authentication and Pairing**. This chapter described our second solution that use the device virtual context to ensure the pairing with coordinator. The vulnerability exploitation of the existing approach was discussed in detail, which leads to key transportation attack and required user assistance. Based on these limitations, this chapter briefly described our proposed zero-effort scheme that solve these issues in an optimum way. Also, the proposed scheme was simulated with scyther and AVISPA for security vulnerability assessment, also the operational overhead was computed and compare with the existing approaches.

- **Chapter 5: Co-presence based Pairing and Authentication**. In this chapter, we address the identification of devices based on their contextual co-presence data. Each device collects their ambient from their own board sensor and generate a device fingerprint, which can be used to ensure pairing with the neighboring device. The existing approaches take prolong pairing time and vulnerable to contextual co-presence attack. Therefore, we have briefly describe how our proposed approach try to mitigate this kind of challenges. Moreover, we have used the publicly available dataset to evaluate our proposed methodology with the existing approach.

- **Chapter 6: Conclusion and Future directions**. This chapter summarizes the thesis with concluding remarks and provide future directions in the area of zero interaction and pairing. Furthermore, the relevant application areas of the proposed methodology are described in detail.

Chapter 2

Related Work

Zero Interaction Pairing and Authentication uses device physical, virtual, and ambient context to establish a shared secret key and validate the device identity. In this chapter, we described the critical analysis of the existing state-of-the art approaches and identified the limitations.

2.1 IoT Authentication

The IoT has revolutionized the daily life of human with personalized services. These device need to verify and validate its identity to become a part of the network, the procedure is known as IoT authentication. A variety of IoT authentication mechanisms has been proposed in the literature that ensure the security and provide reliable services. Figure 2.1 present the overall research taxonomy

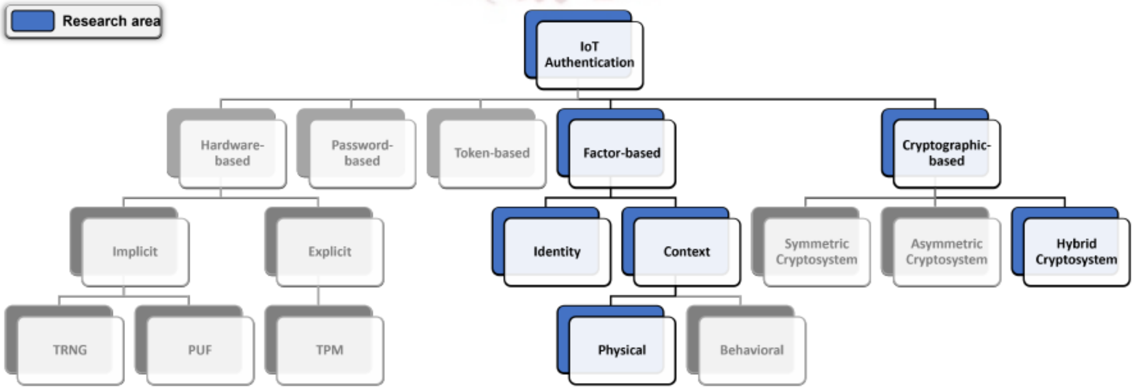


Figure 2.1: IoT Authentication Research Taxonomy and Targeted Area

of IoT authentication and the description of each category is described as follows:

2.1.1 Hardware-based

This type of authentication mechanism rely on a dedicated physical device/behavior that can be used as an authentication credential for getting access to a relevant resource or device [36]. Such type of mechanism is divided into implicit and explicit authentication [37]. The implicit approach identify the resources or devices based on its behavior [38]. For IoT devices, the most common implicit approaches are True Random Number Generator (TRNG) and Physical Unclonable Function (PUF). The TRNG generates random numbers from hardware level process instead of relying on an algorithm or random number generator [39]. While the PUF is a unique fingerprint of device generated from the implemented integrated circuit [40]. On the contrary, the explicit approach generate, store, and validate the hardware-based credentials [41]. Trusted Platform Module (TPM) is an appropriate category of explicit hardware-based authentication, which is a secure crypto-processor designed for managing the cryptographic operations [42].

2.1.2 Password-based

The secret credentials, key, or code that grant access to the device or resource after verification can be considered as password [43]. It can be graphical [44], pattern [45], or secret string [46], which require user assistance. Usually password based authentication required registration, where the appropriate credentials are set and stored securely. For granting access to a specific device or resource, the input and stored password are compared with each other for making an authentication decision [47].

2.1.3 Token-based

This type of authentication mechanism use a unique cryptographic token for verification of device or resource identity [48]. The token-based authentication depends on a cryptographic protocol, which generate a token after verification of the device or resource credential [49]. The generated token have limited validity and used for identity verification instead of providing the credentials every time. The most common use of token-based authentication is the concept of Single Sign

On (SSO), which enable the device or user to access multiple resources with a single identity verification [50].

2.1.4 Factor-based

The factor-based authentication grant the access to a specific resource by verifying and validating two or more evidences that prove the identity of a device or user. It is also known as multi-factor authentication and usually deployed for protecting high sensitive resources such as preventing privacy, securing financial assets and applications rely on personally identifiable information [51,52]. The factor-based authentication mechanisms are further divided into identity and context based approaches. The identity-based approach use independent identifier to verify and validate the device or user identity [53]. It includes biometrics, smart card, and passwords. While the context-based approach analyze the user or device contextual data in term of physical, virtual, and ambient context for the purpose of authentication [54]. The context-based authentication is further divided into physical and behavioral. The physical context use the device and environmental factors such as noises, lighting, temperature and location [55]. While the behavioral context is influence by external and internal factors related to a specific situation such as activity analysis and pattern recognition [56].

2.1.5 Cryptographic-based

This type of authentication scheme use the cryptographic primitives for key establishment, encryption, and authentication [57].The cryptographic-based approaches are classified into symmetric , asymmetric, and hybrid cryptosystem. The symmetric cryptosystem use one shared secret key for encryption and decryption [58]. The generation of similar key among the communicating entities can lead to successful authentication. On contrary, the asymmetric cryptosystem rely on secret key pair known as public and private [59]. The public key is used for encryption, while the private key is used for authentication combined with other cryptographic primitives. The hybrid cryptosystem use both the symmetric and asymmetric approaches based on the pre-defined protocol designed for a specific application [60].

2.2 Context-based Authentication Mechanisms

Among the IoT authentication schemes described in section 2.1, this thesis falls within the scope of factor-based and cryptographic-based approaches. We have emphasized on the pairing and authentication between IoT devices using contextual data in terms of physical, virtual, and ambient context. Therefore, we have critically analyzed the existing literature that utilizes these contextual information for establishing the shared key and validating the device identity within its proximity. The detailed descriptions of the existing literature is divided based on the contextual data and described as follows:

2.2.1 Physical Context

The physical context is related to the IoT itself. It is different from the hardware-based features because the hardware usually have a unique fingerprint due to the integrated circuit but the physical context maybe similar between vendor specific devices with a minor difference. The hardware-based features are mostly generated by the device itself, while the device physical context can be analyzed by a specific monitor. Rostami et al. designed a pairing scheme that extract the randomness from electrocardiography (ECG) and allow an external device to interact with the implantable medical devices (IMDs) [61]. The proposed approach ensure that only the devices in possession of patient can access the IMDs. Adversary may compromise a device closely in contact with the patient body and use it to compromise the target IMD. Han et al. proposed a pairing scheme that binds the vehicle's digital certificate with its location to identify the presence of legitimate vehicles in a convey and ensure prevention against ghost attack [62]. The proposed approach is vulnerable to replay attack on a specific road and traffic condition. In [63], the authors proposed a challenge response authentication protocol using micro-electro-mechanical sensors that collects the accelerometer and gyroscope measurement affiliated with targeted user, and authenticate the nearby devices. The approach used linear regression and hidden Markov model for movement and trajectory recognition, which required relevant data to train and fine tune the model. Melo et al. designed an authentication protocol using physical context that established shared secret key among the communicating entities and provide strong resistance against the external attacks [64]. The approach use error correction code for generation of unique bit stream and accept a certain bits of errors. Cabuk et al. in [65] proposed a mutual authentication protocol for Unmanned Aerial Vehicle (UAV) communication network. The protocol verify and validate a single or group of UAVs identity based on its mission identifier, which is considered as a physical context and easily guessed by an adversary. Also, the traditional cryptographic primitives (such as Rivest Shamir Adleman (RSA) and Advanced Encryption Standard (AES)) were considered that add computational overhead on each UAV. In [20], the authors considered device's power consumption as a physical context and use it as a dynamic credential for authentication in smart manufacturing environment. The approach can be beneficial as a factor-based authentication in the centralized constrained node network because the device physical context can be collected by a smart meter within the network and then the centralized server validate the IoT device identity to prevent malicious node. The proposed approach required time synchronization and use the contextual data as a dynamic credential for cryptographic hash function. According to avalanche effect [66], a minor change in the physical context due to time delay leads to the asynchronous attack [67]. Also, the power consumption value have low entropy, which lead to high information gain based on the notion of Shannon entropy [68].

2.2.2 Virtual Context

The virtual context is an imaginary identifier assigned to each device in form of quick response code, barcode, or personal identifier (such as registered password or cryptographic token). Such virtual context identify the specific device while connecting with a network. It required user assistance to scan or enter the credentials, which are usually available in plaintext and accessible to all the users. Moreover, another application or communication medium (such as WiFi/Bluetooth) for transporting the credential is needed. Coordinator utilizes the received credential for encrypting the network key and delivered it on an insecure communication channel. In [69], the authors proposed an efficient pairing and authentication scheme using public key cryptography, where the client precompute public and private key parameters. Then provide the precomputed parameters based on the proposed protocol to the server for shared secret key establishment and mutual authentication. The proposed scheme shift the computational burden from client to the server and suitable for centralized network. Esfahani et al. proposed a lightweight peer-to-peer authentication mechanism that use exclusive disjunction and hash function for validating the device identity [70]. The proposed approach reduce the computational overhead and provide strong resistance against the well known attacks such as man-in-the-middle, masquerading, replay, and data tampering. Similarly, Lara et al. in [71] proposed authentication protocol that reduce the exchange of messages among the communicating entities. The approaches proposed in [70] and [71] required a secret key distributed prior to the communication. In [72], the authors identify that the ZigBee touchlink commissioning process is vulnerable to active and passive attacks. The explotation of touchlink commissioning vulnerablity may help the adversary to compromise the network. To provide strong resistance against such vulnerability, an efficient and lightweight pairing and authentication mechanism is required. Wang et al. in [31] propose certificate-less protocol and leverage low-cost public key primitives that integrate elliptic curve Diffie Hellman exchange into existing association request/response messages. The goal was to improve the security of installation code by using public key cryptography. The security of this approach depends on the credential and its transmission over the communication channel. Furthermore, the credentials are normally global and publicly available to all the users, including the attacker. In [32], the authors analyze the existing protocols using the security verification tool such as Pro-Verify and presents the insecurity in the underlying communication protocol stacks. The limitation of this study was that the security analysis was performed based on one attacking model only. Amanlou et al. in [73] designed protocol using elliptic curve diffie hellman along with pre-shared secret and evaluated based on publish-subscribe framework such as MQTT protocol. The approach was proposed for fog and edge computing architectures. But this approach did not consider the overhead on the IoT end devices, which are usually constraint in nature. Similarly, Lu et al. impose the security policies and procedures on the edge node, ensuring mutual authentication between the communicating entities [74]. The approach is vulnerable to one-point failure, any vulnerability in the edge node may compromise the targeted network. A lightweight authentication protocol was proposed in [75], which use cryptographic hash function for device identity verification and validation. The approach transmit the digest value on an insecure channel that can be easily spoofed by an adversary.

2.2.3 Ambient Context

The ambient context is the immediate surrounding of an entity such as environmental and social factors. The ambient context can be utilized in a variety of research areas for analysis, prediction, and decision making. Kalamandeen et al. proposed a pairing and authentication scheme [76], named as Ensemble, which authenticate the device based on its proximity assessed from the strength of radio frequency. The approach classify close proximity devices into legitimate and adversarial. However, it required an observer device to collect the ground truth and support in decision making process. In [77], the authors proposed ProxiMate that establish the shared secret key among the communicating entities within its proximity. The authentication decision was made based on the established shared secret key, which gets computed by analyzing the ambient environment. Halevi et al. in [78] proposed a challenge-response protocol that sense the surrounding audio and lumination to identify the proximity of Near-Field Communication (NFC) devices. The selected ambient context can be affected by the surrounding activities such as noise, crowds, and lightning infrastructure. In order to solve the issue of pre-shared secret, Xiao et al. present proximity based authentication approach that uses the infinite Gaussian mixture model for proximity range control and improve the authentication accuracy [79]. The proposed approach is vulnerable to proximity based man-in-the-middle attack. In [80], the authors generate shared secret key among the communicating devices using the ambient audio. The approach considered fuzzy commitment for fingerprint generation that tolerate noises. Such vulnerability can be exploited by the adversary to launch a brute-force attack. In [81], the authors ensure prevention of rely attacks in radio frequency identification (RFID) readers and collects the contextual data using onboard sensors, which support in identification of valid tag within specific proximity. The approach required pretrained model for detecting the proximity between communicating devices. Urien et al. use the sensed value from temperature sensor and integrate it with elliptic curve cryptography to ensure prevention against relaying attack [82]. Each of the communicating device require a temperature sensor to capture the contextual information. Miettinen et al. proposed a pairing scheme that analyze the ambient noise and lumination to identify the co-presence devices [19]. The proposed approach use fuzzy commitment scheme for device fingerprint generation, which allow a certain percentage of erroneous bits and the adversary may take benefit from such vulnerability. In [26], the authors considered four modalities for co-presence device identification, which includes global positioning service (GPS), audio, WiFi and Bluetooth signals strength. The assessment results present the improve pairing on multimodal data compared to single modality. Karapanos et al. collects the ambient noise from user's smartphone and measure the proximity with targeted device [83]. Based on these factors, the smart phone compute the similarity scores between collected noise signal and accept/reject the login attempt. Such approach may not be feasible for the constrained node network, where node has limited resources and analyzing the audio may increase the computational overhead. Similarly, Gu et al. proposed co-presence based pairing scheme that authenticate a group of IoT devices based on ambient audio signal [84]. Each device analyze the audio signal using fuzzy extractor to generate a share secret key, which may be guessed by the adversary due to the error correcting code feature. In [28], the authors analyze context-based authentication in term of security and proposed an approach that mutually authenticate the devices based on their ambient context. The fuzzy vault was used for device's fingerprint generation that rely on error correction mechanism and support the adversary for launching guessing attacks. Fomichev et al. [30] address the challenge of schemes that do not reflect the realistic IoT scenarios and compare different schemes under the realistic conditions. Then collected and released billion of sensors reading including audio, accelerometer, gyroscope, magnetometer, and barometer. In [27], the authors used event timeline extracted from IoT gateway for generation of device fingerprint. The context data was collected in real-time from various smartphone sensors and then transform accordingly. The approach required user assistance for making a pairing decision. Han et al. [85] utilize time as a common factor across different sensors types for a specific event detection. The device co-located within a physically secure boundary can observe the events and ensure prevention from adversary. This approach perform clustering for group identification and use Fuzzy commitment for key establishment. Fomichev et al. in [29] proposed FastZIP that reduces the pairing time and provide prevention against the contextual co-presence attacks. The FastZIP adopt fuzzy password authenticated key exchange protocol for secure key agreement, which allows a certain amount of bits deviation in the generated device fingerprint bits.

2.3 Analysis Of Literature Survey

We have analyzed the existing literature related to pairing and authentication based on the device's contextual data in terms of physical, virtual, and ambient. According to our analysis, the existing approaches used the low entropy contextual data for pairing and authentication, which gets exploited by the adversary for launching predictive contextual attacks [20, 64]. Therefore, sufficient contextual data gets collected to provide adequate security that results in prolong pairing time. Thus, the existing solutions have a trade-off among security, computational overhead, and pairing time [19, 29, 83]. Moreover, the existing user assistance authentication and pairing schemes required another communication medium for device identity verification and validation that is vulnerable to key transportation attacks due to the availability of contextual data in plaintext [31,72,73].

We have identified that the existing approaches consider the physical context that require time synchronization for contextual data collection, which is infeasible in the commodity devices and delay may lead to asynchronous attack [67]. Also, the contextual data are used in keyed hash function for authentication, which increase the overhead on resource constrained devices [20]. Therefore, an efficient pairing and authentication is required that solve the synchronization issue, reduce the pairing time, and provide strong resistance against the guessing attacks. For the devices that utilized the virtual context for verifying and validating its identity, the security depends on the credentials and it transmission medium [72]. The credentials are usually global and publicly available in the device specification document. Also, it required user assistance for initial authentication, which increase burden on the human with increasing number of devices [31]. Thus, zero-effort mechanism is needed that reduce the operational overhead and provide resistance against key transportation, masquerading, man-in-the-middle, and replay attack. Moreover, the verification of neighboring device based on ambient context require sufficient contextual data for adequate security leads to prolong pairing time. Also, these approaches used fuzzy commitment that uses the error correction mechanism such as Reed-Solomon (RS) code that detect and correct multiple symbol errors [29]. The adversary can take advantage from this feature and launch the contextual co-presence attack [19]. Therefore, an innovative approach for co-presence device identification is required that reduce the pairing time and improve the security by ensuring strong resistance against predictive contextual attack.

In this dissertation, we have proposed one-shot, zero effort, and co-presence based pairing and authentication schemes, which provide an efficient and robust solutions to the above mentioned challenges. The one-shot pairing and authentication scheme is independent of time synchronization, convert the low entropy to high entropy for low information gain and resistance against the guessing context. Zero-effort authentication and pairing eliminate the assistance from user during the initial configuration, reduce the computational overhead and ensure prevention against key transportation, masquerading, man-in-the-middle, and replay attacks. The contextual co-presence-based pairing and authentication improve the security and reduce the pairing time based on the innovative design of Median-of-median secret with password authenticated key exchange. The detail description of the proposed solutions and it comparison with the state-of-the-art are described in the upcoming chapters.

Chapter 3

One-shot Pairing and Authentication

3.1 Introduction

The recent tsunami of IoT has evolve our daily life with different sensors and actuators. These devices sense the context and make an intelligent decision to improve the lifestyle [86, 87]. However, the acquired contextual data are sensitive in nature because it contain personally identifiable information and attract an adversary for launching a variety of attacks such as identity theft, man-in-the-middle, and data tampering. Therefore, many solutions were proposed to prevent the misuse of these personally identifiable information and provide strong resistance to the well-know attacks [88]. Inspired from the automation, time efficiency, cost reduction, and improve productivity, the research community considered to use these contextual data for pairing and authentication.

Pairing is the establishment and computation of secret credential (such as key) among the communication entities based on the commonly sensed context [30]. While authentication verify and validate the identities of communicating entities [89]. According to our analysis, the research of pairing and authentication using contextual data are broadly considered in terms of user and device perspectives. In user perspective, the objective is to identify the devices in possession of user [90–93]. Therefore, the contextual data are usually associated with the user and ensure that the acquired data belongs to the specific user, then validate the device within proximity. On contrary, the device-based contextual data is affiliated with the device and verify the identities of communicating devices within its proximity [19, 28–30]. Our focus in this dissertation is on the pairing and authentication mechanism in device perspective, instead of user perspective that is a very mature area of research.

In this chapter, we will described our proposed one-shot pairing and authentication approach that verify and validate the devices based on its physical context. The name one-shot described

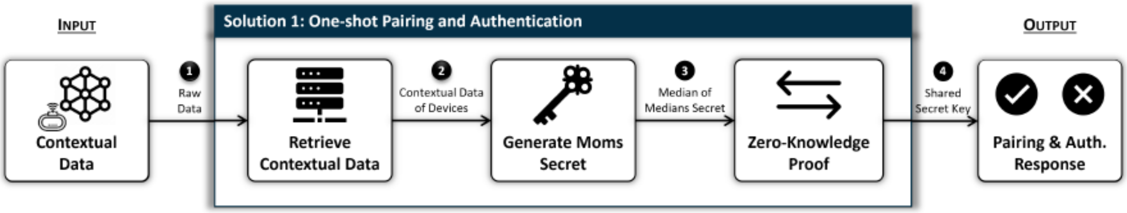


Figure 3.1: One-shot Pairing and Authentication

that only the end device contextual information will be used by the centralized server to verify and validate its identity. It is assumed that the device contextual data is already stored in a secured centralized repository and accessible to the server. The server acquire physical context of the specific device based on its identity, establish a share secret key, and identify the end device based on the shared secret key. The most prominent example is the non-intrusive load monitoring data, where each of the appliances shared the power consumption data with the centralized server for energy management system [94]. The goal of one-shot pairing and authentication is to utilize such kind of physical contextual data as dynamic credential, which is independent of time synchronization, reduce the time complexity and computational overhead, and ensure prevention against guessing attacks. The application areas include the energy management system, appliances management system, and healthcare monitoring system. Figure 3.1 presents the architecture of our proposed one-shot pairing and authentication, which analyzed the device physical context and validate its identity. The detail description of each component is described as follows.

3.1.1 Retrieve Contextual Data

The device share its physical context with the centralized server for long term storage and also utilize the same interval of data for pairing and authentication. It is assumed that the physical context can be transmitted over the secure communication channel. The interval for selecting the context are predefined based on the number of instances. Each device contextual data is linked with its unique identifier, which can be utilized while retrieving its corresponding context for validation and verification.

Algorithm 3.1: Median of Medians Secret Key Generation

```
Input: $C_{t_1}, ..., C_{t_n}$
Output: $M_{oms_{secret}}$
/* Retrieve Contextual Data                                      */
$d_{C_x} \leftarrow Collect(C_{t_1}, ..., C_{t_n})$
/* Compute the Median of $d_{C_x}$                               */
$f_{MedVal} \leftarrow median(d_{C_x})$
$G_{f_{upper}} \leftarrow d_{C_x}[f_{MedVal} > d_{C_x}]$
$G_{f_{lower}} \leftarrow d_{C_x}[f_{MedVal} < d_{C_x}]$
/* Compute the Median of $G_{f_{upper}}$                         */
$s_{MedVal} \leftarrow median(G_{f_{upper}})$
$G_{s_{upper}} \leftarrow G_{f_{upper}}[s_{MedVal} \geq G_{f_{upper}}]$
/* Compute the Median of $G_{f_{lower}}$                         */
$t_{MedVal} \leftarrow median(G_{f_{lower}})$
$G_{t_{lower}} \leftarrow G_{f_{lower}}[t_{MedVal} \leq G_{f_{lower}}]$
$G_{1bits}, G_{2bits} \leftarrow int(G_{s_{upper}}), int(G_{t_{lower}})$
$G_{concat} \leftarrow G_{1bits} || G_{2bits}$
$P_{adBits} \leftarrow len(G_{concat})\%8$                 /* for bytes */
$P_{adBits} \leftarrow 8 - P_{adBits}$                  /* Padding Bits */
if $P_{adBits} \neq 0$ then
    $G_{Pad} \leftarrow Add\ P_{adBits}\ padding\ to\ G_{concat}$
else
    $G_{Pad} \leftarrow G_{concat}$
$B_{itsChunk} \leftarrow$ shape $G_{Pad}$ into $8 - bits\ chunk$
$M_{oms_{secret}} \leftarrow int(B_{itsChunk}, 2)$
```

3.1.2 Generate Moms Secret

As the device physical context has low entropy, which is vulnerable to guessing attacks. Therefore, we proposed a method to convert the low entropy context to high entropy for low information again by using the median of medians (Moms) secret key generation as shown in Algorithm 3.1. Initially, the selected time interval contextual data ($C_{t_1}, ..., C_{t_n}$) related to a specific device is acquired from the centralized repository based on the unique identifier of targeted device. Then compute the first median to divide the contextual data into two approximately equal size groups such as $G_{f_{upper}}$ and $G_{f_{lower}}$. In order to convert the low entropy value to high entropy, the median of $G_{f_{upper}}$ and $G_{f_{lower}}$ are computed as s_{MedVal} and t_{MedVal} respectively. Figure 3.2 present the groups of contextual data divided based on median of medians. The corresponding groups ($G_{f_{upper}}$ and

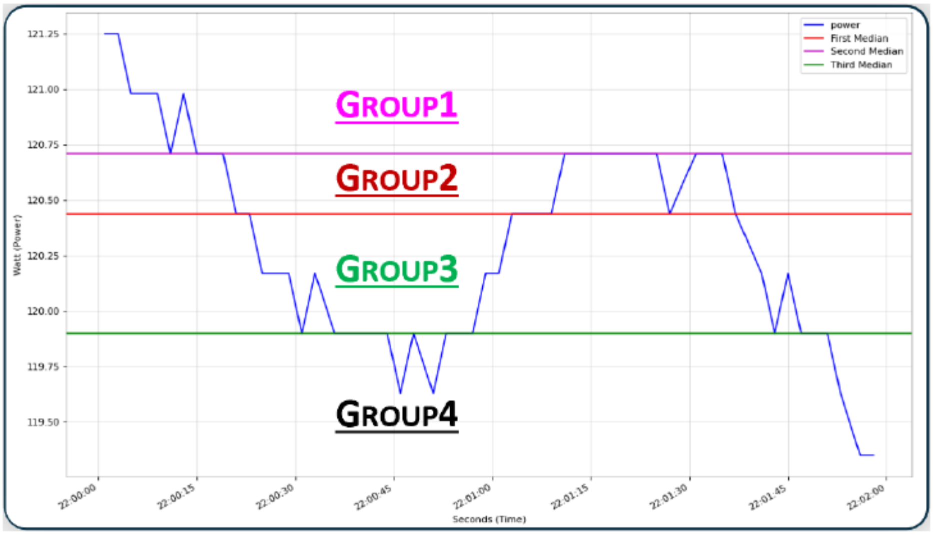


Figure 3.2: Median-of-medians (Moms) Groups

$G_{f_{lower}}$) are compared with s_{MedVal} and t_{MedVal} and the resultant boolean are stored in $G_{s_{upper}}$ and $G_{t_{lower}}$. In order to acquire the values in binary form, the $G_{s_{upper}}$ and $G_{t_{lower}}$ are converted into integer that results in zero's and one's, depicted as bits (G_{1bits} and G_{2bits}). The G_{1bits} and G_{2bits} are concatenated in G_{concat} and converted into bytes after padding (if required), which generate our proposed Moms secret ($M_{oms_{secret}}$).

3.1.3 Zero Knowledge Proof

In order to established a shared secret key among the communicating entities, we adopt the concept of Zero Knowledge Proof (ZKP) [95–97], which prove the possession of information without revealing the information itself. For the proof of concept, we used the ZKP with elliptic curve cryptography to generate a shared key based on $M_{oms_{secret}}$. Algorithm 3.2 described the process of generating shared secret key from the perspective of two communicating entities. Each device compute and reveal some information regarding the possession of $M_{oms_{secret}}$. Using the revealed information (T_{d1} and S_{d2}), both devices compute the share secret key $S_{hared_{secretKey}}$. In case of same $S_{hared_{secretKey}}$ generated between the communicating entities, the devices authenticated successfully. Otherwise, the process will be repeated upon failure.

Algorithm 3.2: Zero-Knowledge Proof

```
Input: $D_{M_{oms_{secret}}}, EC_M, EC_N$
Output: $D_{1S_{hared_{secretKey}}}, D_{2S_{hared_{secretKey}}}$
/* $D_1$ Preparation */
$r_{d1} \leftarrow$ selects random number $r_{d1} : 0 < r_{d1} < p$
$X_{d1} \leftarrow r_{d1} \cdot G$    /* G is a point on Elliptic Curve */
$T_{d1} \leftarrow D_{M_{oms_{secret}}} \cdot EC_M + X_{d1}$
$D_1$ share $T_{d1}$ with $D_2$
/* $D_2$ Preparation */
$r_{d2} \leftarrow$ selects random number $r_{d2} : 0 < r_{d2} < p$
$Y_{d2} \leftarrow r_{d2} \cdot G$    /* G is a point on Elliptic Curve */
$S_{d2} \leftarrow D_{M_{oms_{secret}}} \cdot EC_N + Y_{d2}$
$D_2$ share $S_{d2}$ with $D_1$
/* $D_1$ Compute $S_{hared_{secretKey}}$ */
$D_{1S_{hared_{secretKey}}} \leftarrow r_{d1} \cdot (S_{d2} - D_{M_{oms_{secret}}} \cdot EC_N)$
$D_{1S_{hared_{secretKey}}} \leftarrow r_{d1} \cdot (D_{M_{oms_{secret}}} \cdot EC_N + Y_{d2} - D_{M_{oms_{secret}}} \cdot EC_N)$
$D_{1S_{hared_{secretKey}}} \leftarrow r_{d1} \cdot Y_{d2}$
$D_{1S_{hared_{secretKey}}} \leftarrow r_{d1} \cdot r_{d2} \cdot G$
/* $D_2$ Compute $S_{hared_{secretKey}}$ */
$D_{2S_{hared_{secretKey}}} \leftarrow r_{d2} \cdot (T_{d1} - D_{M_{oms_{secret}}} \cdot EC_M)$
$D_{2S_{hared_{secretKey}}} \leftarrow r_{d2} \cdot (D_{M_{oms_{secret}}} \cdot EC_M + X_{d1} - D_{M_{oms_{secret}}} \cdot EC_M)$
$D_{2S_{hared_{secretKey}}} \leftarrow r_{d2} \cdot X_{d1}$
$D_{2S_{hared_{secretKey}}} \leftarrow r_{d2} \cdot r_{d1} \cdot G$
$D_{2S_{hared_{secretKey}}} \leftarrow r_{d1} \cdot r_{d2} \cdot G$
if $D_{1S_{hared_{secretKey}}} == D_{2S_{hared_{secretKey}}}$ then
    $A_{uthStatus} \leftarrow Succeed$
else
    $A_{uthStatus} \leftarrow Failed$
```

3.2 Comparison of One-shot Approach with State-of-the-art

We compared our proposed approach with Ustundag et al. context aware authentication mechanism [20], which used the device physical context as a dynamic credential for cryptographic hash function. Figure 3.3 present difference between [20] and our proposed approach. The Ustundag et al. approach require time synchronization at both the communicating entities, which is not feasible in the commodity devices and in case of asynchronization, the computed hash on the communi-

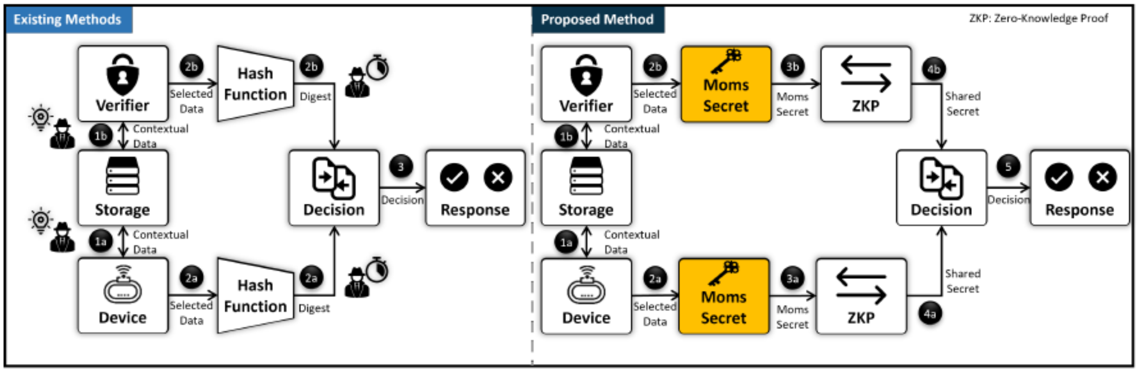


Figure 3.3: One-shot Pairing and Authentication - Existing vs Proposed Methodology

cating entities will be different [20]. Also, the Ustundag et al. approach used device physical contextual value directly, which has low entropy and vulnerable to guessing attacks. Therefore, we generated the Moms secret that uses interval based contextual data to prevent asynchronous attack. Also, our proposed approach covert the low entropy device physical context value to high entropy for low information gain and provide strong resistance against guessing attacks.

3.3 Evaluation and Results

The security of one-shot pairing and authentication using device physical context depends on the input values, especially the generated Moms secret. Therefore, we have evaluated our proposed approach based on three evaluation metrics, which includes entropy assessment, probability of guessing attacks, and time complexity. The acquired results of each evaluation criteria was compared with the state-of-the-art approach of Ustundag et al. [20], which is very similar to our proposed approach. The detail description about the dataset selection and evaluation metrics are described as follows:

3.3.1 Dataset Selection

We utilize the same datasets mentioned in the [20] to reproduce their result and avoid biasness. The first dataset was the Almanac of Minutely Power dataset (AMPds2), which contains the electricity consumption data from 21 power meters at one minute interval within house. The data was collected from non-intrusive load monitoring system for two year, which have timestamp, voltage, current, and power as features [98]. The second data was the Sustainable Data for Energy Disaggregation (SustDataED2) that contain smart meter data attached to 18 appliances within one household. The data was collected for 96 days, which have timestamp and power as features [99]. Using the AMPds2 and SustDataED2 datasets, we have evaluated our proposed one-shot approach and compared the result with Ustundag et al. scheme.

3.3.2 Entropy Assessment

Entropy measure the state of disorder, randomness, and uncertainty in a given sequence. The entropy is directly proportional to the randomness ($Entropy\ \alpha\ Randomness$), which mean that if entropy is high then randomness will be high as well and vice versa. In information theory and coding, the information gain uses the entropy to make a decision. According to Claude Shannon [21, 68], entropy is inversely proportional to the information gain ($Entropy\ \alpha\ InformationGain^{-1}$), if entropy is high then information gain will be low and vice versa. This

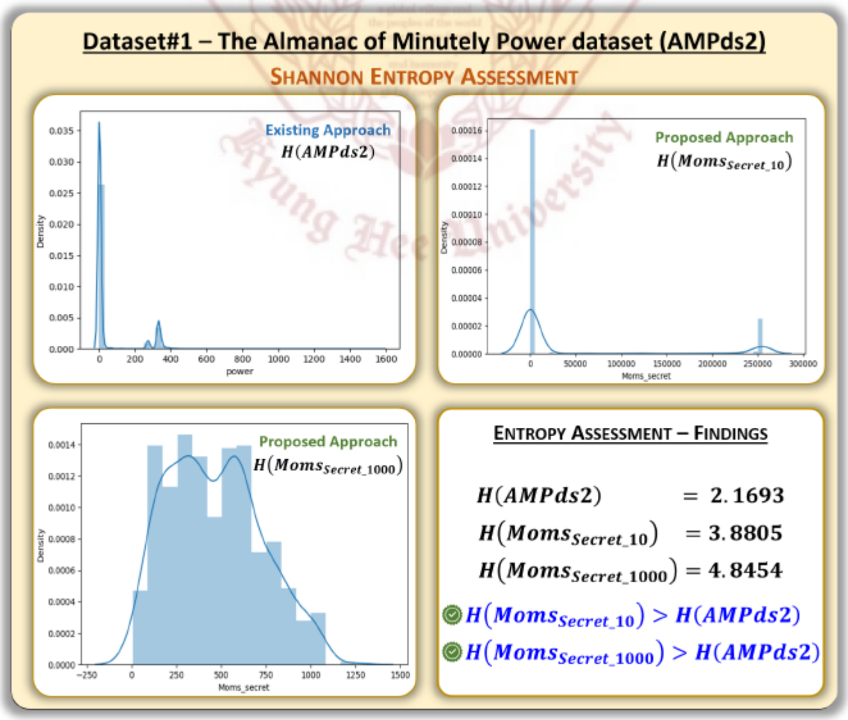
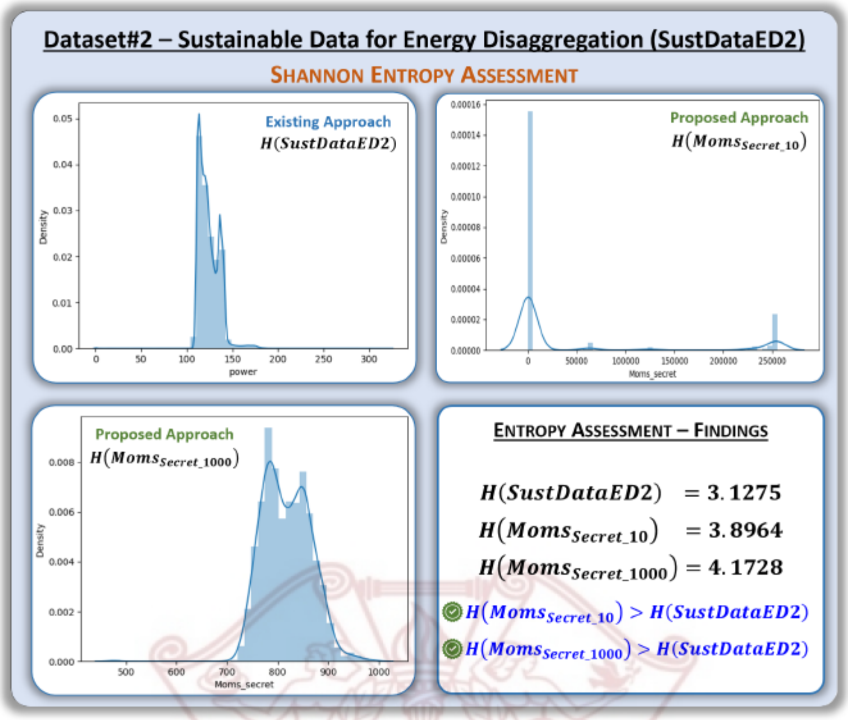


Figure 3.4: Shannon Entropy Assessment of AMPds2


Dataset#2 – Sustainable Data for Energy Disaggregation (SustDataED2)

Shannon Entropy Assessment

Entropy Assessment – Findings

$H(SustDataED2) = 3.1275$

$H(Moms_{Secret\_10}) = 3.8964$

$H(Moms_{Secret\_1000}) = 4.1728$

✓ $H(Moms_{Secret\_10}) > H(SustDataED2)$

✓ $H(Moms_{Secret\_1000}) > H(SustDataED2)$

Figure 3.5: Shannon Entropy Assessment of SustDataED2

concept is known as Shannon entropy and presented as $H(X) = -\sum_{x \epsilon X} p(x) \log_2 p(x)$. Figure 3.4 and Figure 3.5 presents the entropy assessment calculated for existing (Ustundag et al. [20]) and proposed (one-shot) approaches using AMPds2 and SustDataED2 datasets. The probability density function of AMPds2 dataset presented in Figure 3.4 shows a clear difference between the existing and proposed schemes. The x-axis presents the input data, while the y-axis present the density. The entropy of raw dataset is 2.1693 used by the existing approach, while the probability of Moms secret with a small window size of 10 is 3.8805 and large window size of 1000 is 4.8454. In both the cases the entropy of our proposed approach is high, compared with the state-of-the-art. Similarly, for SustDataED2 dataset shown in Figure 3.5, the entropy of existing approach is 3.1275, Moms secret generated with a window size of 10 instance is 3.8964, and large window size of 1000 instances is 4.1728. The results show that entropy of Moms secret is high as compared to Ustundag et al. scheme, which concludes that our proposed one-shot pairing and authentication mechanism ensure strong resistance against the information gain and prevent predictive contextual attacks.

Algorithm 3.3: Probability of Guessing the Contextual Value - Existing Approach

```
Input: Contextual Dataset $D_{C_{t_1},...,C_{t_n}}$
Output: Contextual Value Probability $p(C_t)$
/* Load the Data & Identify min and max value */
$C_{data} \leftarrow Load\ D_{C_{t_1},...,C_{t_n}}$
$C_{MinValue} \leftarrow C_{data}.min()$
$C_{MaxValue} \leftarrow C_{data}.max()$
/* Identify the total number of values between $C_{MinValue}$ & $C_{MaxValue}$ */
while $C_{MinValue} \leq C_{MaxValue}$ do
    $C_{MinValue} \leftarrow C_{MinValue} + 0.01$
    $T_{count} \leftarrow count + 1$
/* Identify the total values within $C_{data}$ */
$T_{values} \leftarrow len(C_{data})$
/* Compute the probability of Guessing the Contextual Value */
$p(C_t) \leftarrow \frac{1}{T_{count}} \times \frac{1}{T_{values}}$
```

3.3.3 Probability of Guessing Attack

Probability is the occurrence of an event, which is usually between 0 and 1. The 0 present uncertainty of an event, while 1 indicates certain event. The higher probability mean that the event will more likely be occur. The probability of guessing attack indicate the likelihood of an attacker to guess a specific contextual value used for a specific operation. Algorithm 3.3 described the procedure on which the guessing attack probability for the existing approach was computed. For this purpose, we have loaded the device specific contextual data ($D_{C_{t_1},...,C_{t_n}}$) as C_{data}. Then identify the minimum value ($C_{MinValue}$) and maximum value ($C_{MaxValue}$) existed in C_{data}. Based on the $C_{MinValue}$ and $C_{MaxValue}$, count all the possible values between $C_{MinValue}$ and $C_{MaxValue}$, and store in T_{count}. Next, identify the total values in the dataset C_{data} and save the resultant value in T_{values}. Finally, calculated the probability of guessing attack for existing approach as $\frac{1}{T_{count}} \times \frac{1}{T_{values}}$.

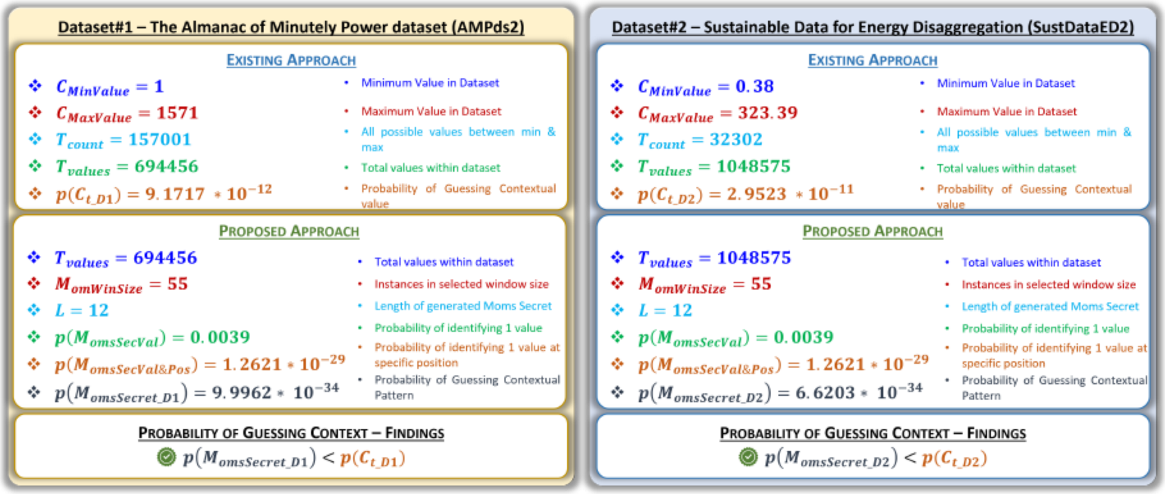
Our proposed Moms secret generation algorithm required specific time interval or window size. Therefore, the procedure for computing the probability of guessing Moms secret is different from the existing approach because the adversary has to guess the exact pattern instead of just identifying a single contextual value. Algorithm 3.4 described the steps for calculating the proba-

Algorithm 3.4: Probability of Guessing the Contextual Pattern of Moms Secret

```
Input: Contextual Dataset $D_{C_{t_1},\ldots,C_{t_n}}$
Output: Contextual Pattern Probability $p(M_{oms_{secret}})$
/* Load the Data */
$C_{data} \leftarrow Load\ D_{C_{t_1},\ldots,C_{t_n}}$
/* Identify the total values within $C_{data}$ */
$T_{values} \leftarrow len(C_{data})$
/* Identify the Selected Window Size $M_{omsWin_{size}}$ */
$M_{omsWin_{size}} \leftarrow len(M_{omsWin})$
/* Identify the Length of Generated $M_{omsSecret}$ */
$L \leftarrow len(M_{omsSecret})$
/* Total Possible combination of Binary value */
$T_{PossibleBits} \leftarrow 2^n$                    /* For 1 Byte, n=8 */
/* Probability of Identify 1 value of $M_{omsSecret}$ */
$p(M_{oms_{secVal}}) \leftarrow \frac{1}{2^n}$
/* Probability of Identify 1 value at a specific position
    of $M_{omsSecret}$ */
$p(M_{oms_{secVal\&Pos}}) \leftarrow (\frac{1}{2^n})^L$
/* Compute the Probability of Guessing Contextual Pattern
    */
$T_{M_{oms_{secretPossible}}} \leftarrow \frac{T_{values}}{M_{omsWin_{size}}}$
$p(M_{oms_{secret}}) \leftarrow \frac{1}{T_{M_{oms_{secretPossible}}} \times (2^n)^L)}$
```

bility of Moms secret. Initially, the device contextual data within specified interval ($D_{C_{t_1},\ldots,C_{t_n}}$) is loaded as C_{data}. First, the algorithm identifies the total values in C_{data} and store it in T_{values}, then count the number of instances in the selected window size and save the resultant value in $M_{omsWin_{size}}$. Next, it identify the length of generated Moms secret (L) and compute the total possible combination of binary values ($T_{PossibleBits}$). Finally, compute the guessing probability of Moms secret as probability of identifying one value $p(M_{oms_{secVal}})$, probability of identifying one value at a specific position $p(M_{oms_{secVal\&Pos}})$, and probability of guessing correct Moms secret $p(M_{oms_{secret}})$.

Based on Algorithm 3.3 and Algorithm 3.4, we have computed the probability of launching guessing attack on existing and proposed approaches using the AMPds2 and SustDataED2 datasets. Figure 3.6 presents the calculated probability of guessing attacks, which shows that the probability of guessing Moms secret is less than guessing the physical context of devices used by the existing approach. Because Moms secret require to first guess the length of selected time inter-



Dataset#1 – The Almanac of Minutely Power dataset (AMPds2)

EXISTING APPROACH

- $C_{MinValue} = 1$ — Minimum Value in Dataset
- $C_{MaxValue} = 1571$ — Maximum Value in Dataset
- $T_{count} = 157001$ — All possible values between min & max
- $T_{values} = 694456$ — Total values within dataset
- $p(C_{t\_D1}) = 9.1717 * 10^{-12}$ — Probability of Guessing Contextual value

PROPOSED APPROACH

- $T_{values} = 694456$ — Total values within dataset
- $M_{omWinSize} = 55$ — Instances in selected window size
- $L = 12$ — Length of generated Moms Secret
- $p(M_{omsSecVal}) = 0.0039$ — Probability of identifying 1 value
- $p(M_{omsSecVal\&Pos}) = 1.2621 * 10^{-29}$ — Probability of identifying 1 value at specific position
- $p(M_{omsSecret\_D1}) = 9.9962 * 10^{-34}$ — Probability of Guessing Contextual Pattern

PROBABILITY OF GUESSING CONTEXT – FINDINGS

✓ $p(M_{omsSecret\_D1}) < p(C_{t\_D1})$

Dataset#2 – Sustainable Data for Energy Disaggregation (SustDataED2)

EXISTING APPROACH

- $C_{MinValue} = 0.38$ — Minimum Value in Dataset
- $C_{MaxValue} = 323.39$ — Maximum Value in Dataset
- $T_{count} = 32302$ — All possible values between min & max
- $T_{values} = 1048575$ — Total values within dataset
- $p(C_{t\_D2}) = 2.9523 * 10^{-11}$ — Probability of Guessing Contextual value

PROPOSED APPROACH

- $T_{values} = 1048575$ — Total values within dataset
- $M_{omWinSize} = 55$ — Instances in selected window size
- $L = 12$ — Length of generated Moms Secret
- $p(M_{omsSecVal}) = 0.0039$ — Probability of identifying 1 value
- $p(M_{omsSecVal\&Pos}) = 1.2621 * 10^{-29}$ — Probability of identifying 1 value at specific position
- $p(M_{omsSecret\_D2}) = 6.6203 * 10^{-34}$ — Probability of Guessing Contextual Pattern

PROBABILITY OF GUESSING CONTEXT – FINDINGS

✓ $p(M_{omsSecret\_D2}) < p(C_{t\_D2})$

Figure 3.6: Probability of Guessing Context using AMPds2 and SustDataED2

val, then identify the exact pattern and value on each position that makes it hard for the adversary to guessing the Moms secret within the acceptable pairing and authentication time.

3.3.4 Time Complexity

Time complexity estimate the computational time of an algorithm by counting the number of tasks, which usually required a fixed operational time [100]. Therefore, the number of tasks and operational time of an algorithm are correlated with a constant factor called *big O notation* [101]. The *big O notation* consider the worst-case scenario of an algorithm and estimate its computational time accordingly [102]. The commonly used estimation of time complexity includes constant time $O(1)$, linear time $O(n)$, logarithmic time $O(\log n)$ and many others, the n present input size in bits. Based on *big O notation*, we compute the time complexity of our proposed one-shot approach based on Moms secret and compared with Ustundag et al. scheme [20]. According to our analysis, the time complexity of our proposed approach is $O(n)$. While, Ustundag et al. scheme adopt the cryptographic hash function (Secure Hash Algorithm (SHA)) and its time complexity is $O(c + xn)$ [103, 104]. Thus, our proposed one-shot approach is time efficient as compared with Ustundag et al. scheme, specifically if $x \geq 2$. Moreover, we have compared the time complexity of our proposed and existing approaches using AMPds2 and SustDataED2 datasets. Figure 3.7 present the obtained results and its comparison using AMPds2 and SustDataED2 datasets. Our proposed approach reduces the time complexity compared with Ustundag et al. scheme as an average of 7.5% and 18.5% compared to existing approach using SHA256 and SHA512 respectively.

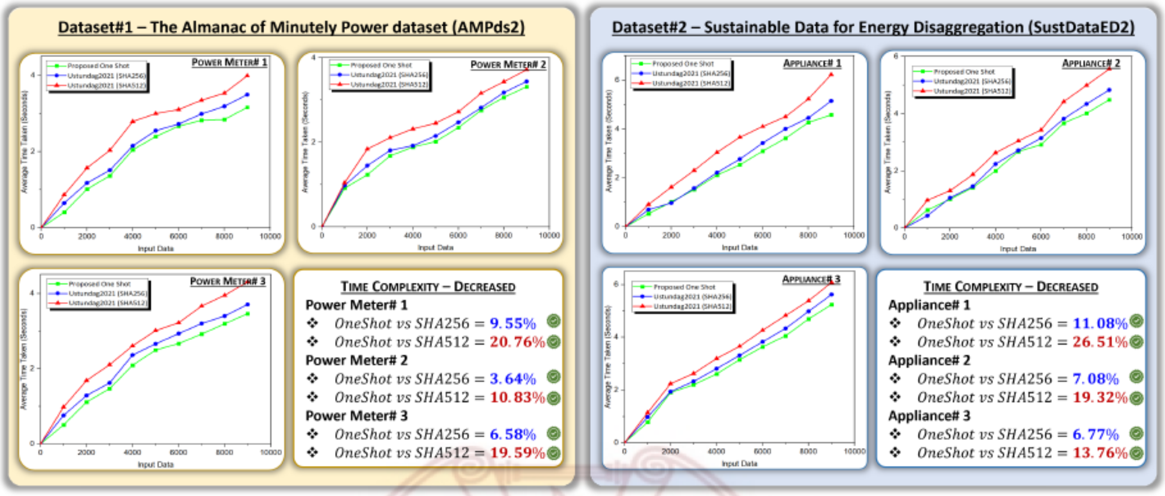


Figure 3.7: Time Complexity Assessment using AMPds2 and SustDataED2

Chapter 4

Zero-Effort Authentication and Pairing

4.1 Introduction

According to the World Economic Forum, the global spending on households IoT product is forecasted to reach \$1.1 trillion in 2023 due to the increasing number of IoT devices utilized for household purposes [105, 106]. These devices have limited resources in terms of memory, computation, and usually operated on battery with a life time of days, months, or years. Therefore, an efficient algorithm is deployed on such devices to fulfill a specific task and collect relevant data for optimum decision making, which increase productivity and reduce burden on human being. With all these benefits, these devices are highly targeted by the adversary for launching a variety of attacks due to its constraint nature and often considered as the weakest link of a network. Therefore, the research community have proposed many lightweight solutions that provide strong resistance against the well known attacks such as masquerading, man-in-the-middle, massage tampering, and replay attacks. Also, with the emergence of industrial IoT, many vendor have also considered the security of device and it communication as a primary factor such as the evolution of ZigBee from challenge response protocol (v1.0) to installation code based protocol (v3.0).

According to our analysis, the security of these existing approaches utilized the device virtual context as credential to become a part of network. The virtual context is an imaginary identifier assigned to each device in form of quick response code, barcode, or personal identifier (such as password or cryptographic token). Such virtual context identify the specific device while connecting with a network. It required user assistance to scan or enter the credentials, which are usually available in plaintext and accessible to all the users. Moreover, another application or communication medium (such as WiFi/Bluetooth/ZigBee) is required for transportation of credential. Coordinator utilizes the received credential for encrypting the network key and delivered it on an

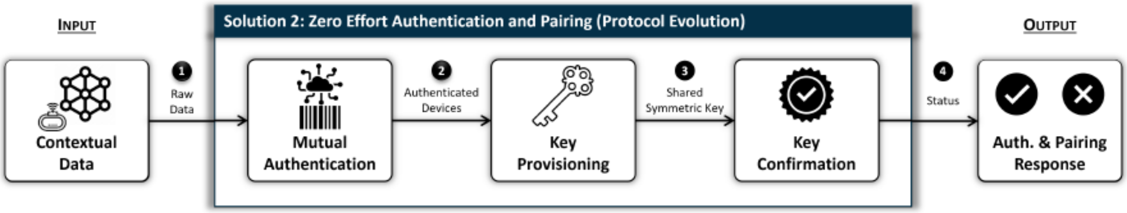


Figure 4.1: Zero-Effort Authentication and Pairing

insecure communication channel. For vendor specific devices, these credential are available in the device specification document, which support the adversary to launch key transportation attack. Also, it required user assistance for initial authentication, which increase burden on the human with increasing number of devices [31]. Therefore, an efficent approach is needed that reduce the operational overhead, increase efficency, and provide strong resistance to key transportation attack along with other well-known attacks such as masquerading, man-in-the-middle, massage tampering, and replay attacks.

For this purpose, we proposed zero-effort authentication and pairing mechanism that evolve the existing protocols by eliminating the assistance from user during the initial authentication and improve security by reducing the operational overhead. Figure 4.1 present the component workflow of our proposed zero-effort authentication and pairing approach, which automate the device joining process by mutually authenticating the devices based on their corresponding self signed identifier and then adopt the integrated encryption scheme for key provision. Finally, the algorithm confirm the generated shared secret key among the communicating devices in the key confirmation. The detail description about the initialization of communicating devices and the component of our proposed approach are described as follows.

4.1.1 Coordinator Initialization Process

The coordinator is responsible to start and manage the network. Algorithm 4.1 describe the initialization process of coordinator. After booting, the coordinator perform energy scan to check the radio frequency activities ($RF_{Activities}$) on the neighboring channels. Then perform the personal area network scan on the identified channels to find the nearby personal area networks ($P_{AN_{Neighbor}}$). Based on the scanning results, the coordinator selects personal area network identi-

Algorithm 4.1: Coordinator Initialization Process

```
Input: Scan $RF_{Activities}, P_{AN_{Neighbor}}$
Output: $P_{AN_{ID}}, O_{Channel}, S_{canTime}, N_{etworkSecurityKey}$
$RF_{Activities} \leftarrow Perform\ E_{nergy_{scan}}\ on\ C_{hannels}$
$P_{AN_{Neighbor}} \leftarrow Perform\ P_{AN_{scan}}\ on\ C_{hannels}$
$P_{AN_{ID}} \leftarrow Selects\ P_{AN_{ID}} : P_{AN_{ID}} \neq P_{AN_{Neighbor}}$
$O_{Channel} \leftarrow Selects\ O_{Channel} : O_{Channel} \neq RF_{Activities}$
$S_{canTime} \leftarrow Set\ S_{canTime}\ on\ O_{Channel}$
$N_{etSecKey} \leftarrow Set\ N_{etworkSecurityKey}$
```

fier ($P_{AN_{ID}}$) and operational channel ($O_{Channel}$) for its own network in such away that it can not duplicate with the neighboring network. Finally, selects the scanning time ($S_{canTime}$) and network key ($N_{etSecKey}$). The $S_{canTime}$ is the time coordinator can listen to a beacon and the $N_{etSecKey}$ is used to secure communication after joining the network. These information are broadcast over the communication channel and wait for response from clients.

4.1.2 End Device Initialization Process

The end device broadcast its identity to scan for nearby coordinator and initiate the association process. Algorithm 4.2 describe the initialization process of end device. After booting, the end

Algorithm 4.2: End Device Initialization Process

```
Input: Contextual Data $P_{AN_{ID}}, O_{Channel}$
Output: $A_{ssociation_{flag}}$
$O_{Channel} \leftarrow Perform\ E_{nergy_{scan}}\ on\ O_{Channels}$
$P_{AN_{ID}} \leftarrow Perform\ P_{AN_{scan}}\ on\ O_{Channels}$
$B_{eacon_{Request}} \leftarrow Broadcast\ B_{eacon}$
$B_{eacon_{Response}} \leftarrow Wait\ for\ time(t)\ after\ B_{eacon_{Request}}$
if $B_{eacon_{Response}} \neq null$ then
    $C_{hannel_{PANID}} \leftarrow validate$
      $P_{AN_{ID}} : P_{AN_{ID}} > 0 \wedge len(bin(P_{AN_{ID}}))\%len(S_{elected_{PANID}}) == 0$
    if $C_{hannel_{PANID}}$ is valid then
        $J_{oin_{flagStatus}} \leftarrow check\ J_{oin_{flag}}$
        if $J_{oin_{flagStatus}} \neq 0$ then
            $A_{ssociation_{flag}} \leftarrow set A_{ssociation_{flag}}\ to\ 1$
            $Call\ MutualAuthentication()$
```

device perform the energy scan and personal area network scan to identify the nearby operational channel ($O_{Channel}$) and personal area network identifier ($P_{AN_{ID}}$) respectively. Upon identification of $O_{Channel}$ and $P_{AN_{ID}}$, the beacon is broadcast and wait for its response ($B_{eacon_{Response}}$) from the coordinator. Upon the $B_{eacon_{Response}}$, the end device verify and validate the $P_{AN_{ID}}$, channel identifier ($C_{hannel_{PANID}}$), and joining flag status ($J_{oin_{flagStatus}}$). Then initiate the mutual authentication process with the coordinator.

4.1.3 Mutual Authentication

Authentication verify and validate the identity of devices. The mutual authentication mean that both the communicating parties prove their identities to each other. In zero-effort authentication and pairing, we utilized the self-signed identifier for device identification. Algorithm 4.3 presents our proposed mutual authentication scheme. Initially, the end device generate a self signed iden-

Algorithm 4.3: Mutual Authentication

```
Input: Association Flag $A_{ssociation_{flag}}$
Output: Authentication Status $A_{uthStatus}$
/* $E_{nd_{Device}}$ Initiate the Association Phase */
if $A_{ssociation_{flag}} == 1$ then
    $D_{evice_{Signed_{Identifier}}} \leftarrow S_{ign}(D_{evice_{ID}} || T_{imeStamp})$
    $A_{ssoc_{Request}} \leftarrow A_{ssoc_{Request}} || D_{evice_{Signed_{Identifier}}}$
/* $E_{nd_{Device}}$ sent $A_{ssoc_{Request}}$ to $C_{oordinator}$ */
/* $C_{oordinator}$ validate $A_{ssoc_{Request}}$ */
if $(T_r - T_i) \leq \triangle T$ then
    if $D_{evice_{Signed_{Identifier}}}$ is valid then
        $A_{uthStatus} \leftarrow 1$
        $C_{oord_{Signed_{Identifier}}} \leftarrow S_{ign}(C_{oord_{ID}} || T_{imeStamp})$
        $A_{ssoc_{Response}} \leftarrow A_{ssoc_{Response}} || C_{oord_{Signed_{Identifier}}} || A_{uthStatus}$
/* $C_{oordinator}$ sent $A_{ssoc_{Response}}$ to $E_{nd_{Device}}$ */
/* $E_{nd_{Device}}$ Validate $A_{ssoc_{Response}}$ */
if $(T_r - T_i) \leq \triangle T$ then
    if $C_{oord_{Signed_{Identifier}}}$ is valid then
        $A_{uthStatus} \leftarrow 1$
        $keyProvisioning()$
```

tifier ($D_{evice_{Signed_{Identifier}}}$) of virtual context appended with timestamp and sent this to the coordinator for verification. The coordinator verify the $D_{evice_{Signed_{Identifier}}}$ with the pre-shared public key after the assessment of time delay ($\triangle T$). In case of successful verification, the coordinator generate its own self-signed identifier ($C_{oord_{Signed_{Identifier}}}$) using the virtual context appended with timestamp and send it to the end device, which verify and validate the $C_{oord_{Signed_{Identifier}}}$. If the generated self-signed identifiers are validated then the devices are mutual authenticated and proceeded to the key provision. Otherwise, the authentication process will be repeated, in case of failure.

4.1.4 Key Provisioning

The key provisioning initiated after the successful mutual authentication of devices. We adopted the concept of integrated encryption scheme for key provisioning between the end device and coordinator as shown in Algorithm 4.4. The end device initiate the process by sharing the newly generated public key (D_{pk}) with the coordinator. The coordinator select a random number (r_{Coord}) as private key on elliptic curve and perform a dot multiplication ($\times$) with the D_{pk} to generate a share secret key ($S_{hared_{Key}}$). Then the coordinator encrypt the network key ($N_{etSecKey}$) using

Algorithm 4.4: Key Provisioning

```
Input: Authentication Status $A_{uthStatus}$
Output: Shared Network Key $N_{etSecKey}$
if $A_{uthStatus} == 1$ then
    $E_{nd_{Device}}$ share $D_{pk}$ (Device Public Key) with $C_{oordinator}$
    /* $D_{pk} = r_d \times G$ */
    /* $r_d : 0 < r_d < p$ & $G$ is a point on Elliptic Curve */
/* $C_{oordinator}$ compute $S_{hared_{Key}}$ */
$S_{hared_{Key}} \leftarrow D_{pk} \times r_{Coord}$
/* $r_{Coord}$ used in generating $C_{pk}$ (Coordinator Public Key) */
/* $C_{pk} = r_{Coord} \times G$ */
/* $r_{Coord} : 0 < r_{Coord} < p$ & $G$ is a point on Elliptic Curve */
$D_{ata_{pkt}} \leftarrow E_{ncryptS_{hared_{Key}}}(C_{oordinator_{ID}} || D_{evice_{ID}} || N_{etSecKey} || T_{imeStamp}) || C_{pk}$
/* $C_{oordinator}$ share $D_{ata_{pkt}}$ with $E_{nd_{Device}}$ */
$S_{hared_{Key}} \leftarrow C_{pk} \times r_d$
$N_{etSecKey} \leftarrow D_{ecryptS_{hared_{Key}}}(D_{ata_{pkt}})$
```

$S_{hared_{Key}}$ and send it to the end device along with Coordinator public key (C_{pk}). The end device validate the receive data packet ($D_{ata_{pkt}}$), compute the $S_{hared_{Key}}$ by multiplying C_{pk} with end device's private key r_d, and then retrieve the $N_{etSecKey}$.

4.1.5 Key Confirmation

In order to confirm the legitimate possession of $N_{etSecKey}$, the end device have to perform one more step of key confirmation, in which the end device shared the same $D_{evice_{Signed_{Identifier}}}$ generated during the mutual authentication process, concatenate with the current timestamp and encrypted it using the retrieved $N_{etSecKey}$ as illustrated in Algorithm 4.5. After receiving the data packet ($D_{ata_{pkt1}}$), the coordinator extract $D_{evice_{Signed_{Identifier}}}$, validate it with end device previous public key and set the key confirmation status (K_{eyCfm}) as $true(0)/false(1)$.

Algorithm 4.5: Key Confirmation

```
Input: Network Key $N_{etSecKey}$, Device Signature $D_{evice_{Signed_{Identifier}}}$
Output: Key Confirmation $K_{eyCfm}$
$D_{ata_{pkt1}} \leftarrow E_{ncryptN_{etSecKey}}(D_{evice_{ID}}||C_{oordinator_{ID}}||D_{evice_{Signed_{Identifier}}}||T_{imeStamp})$
/* $E_{nd_{Device}}$ share $D_{ata_{pkt1}}$ with $C_{oordinator}$ */
/* $C_{oordinator}$ validate $D_{ata_{pkt1}}$ */
$K_{eyCfm} \leftarrow$ set $K_{eyCfm}$ to $[0, 1]$
```

4.2 Comparison of Zero-effort Approach with State-of-the-art

We compared our proposed approach with Wang et al. scheme [31], which leverage low-cost public key primitives and integrate Elliptic Curve Diffie Hellman key exchange into existing association request/response messages. The Wang et al. scheme is similar to our proposed approach except the user assistance and vulnerable to key transportation attack. Also, the existing approach includes non-user assistance scheme that required pre-shared key distributed among devices [32], which are usually available in the device specification document. Figure 4.2 presents the difference between existing and our proposed zero-effort authentication and pairing approaches. The existing schemes utilizes two type of methods: i) Device send request to coordinator and receive the $N_{etSecKey}$ encrypted with pre-shared link key [32]. The pre-shared link key is usually same

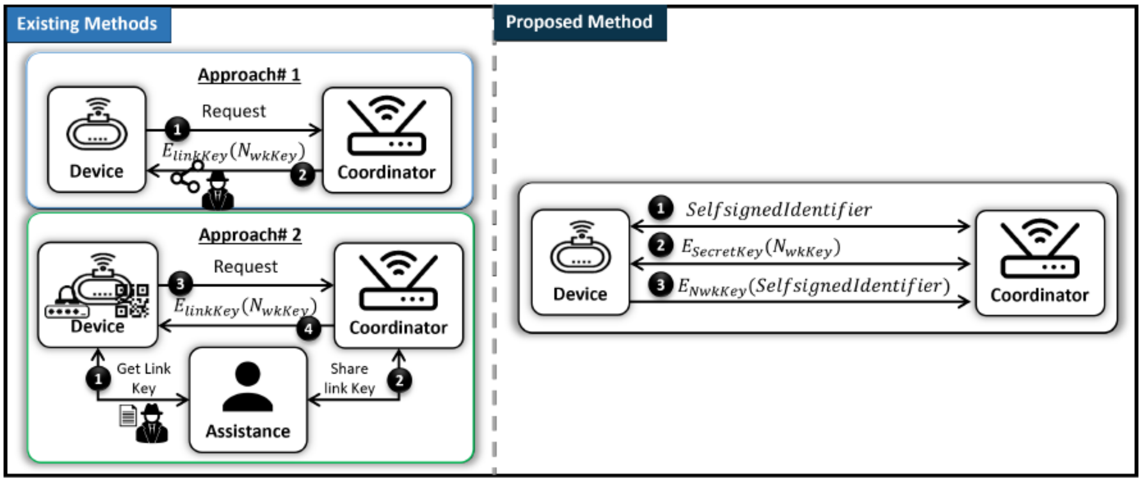


Figure 4.2: Zero-Effort Authentication and Pairing - Existing vs Proposed Methodology

for all devices and publicly available in the specification document. ii) The second approach try to mitigate the issue of publicly available link key by assigning a unique identifier in form of virtual context to each device (such as Quick Response (QR) code, barcode, or Personal Identification Number (PIN)). In Wang et al. approach [31], the virtual context require user assistance during the initial authentication and need to be transmitted via another communication medium or application to the coordinator. The problem with this approach is that the virtual context existed in plaintext and its exploitation can lead to key transportation attack. Therefore, we have designed a lightweight scheme, considering the resource constrained devices and proposed the zero-effort authentication and pairing mechanism, which do not required user assistance and authenticate the devices based on self signed identifier. Moreover, the key provisioning are performed using the integrated encryption scheme to reduce the computational overhead. Finally, the generated shared key is used for encrypting the network key and then ensure that only legitimate devices are in possession of the network key.

4.3 Overall Workflow of Zero-effort Authentication and Pairing

In this section, we described the detail workflow of our proposed zero-effort authentication and pairing mechanism. Figure 4.3 presents the overall concept in a sequential manner between the communicating entities, where the end device interact with coordinator to become a part of net-

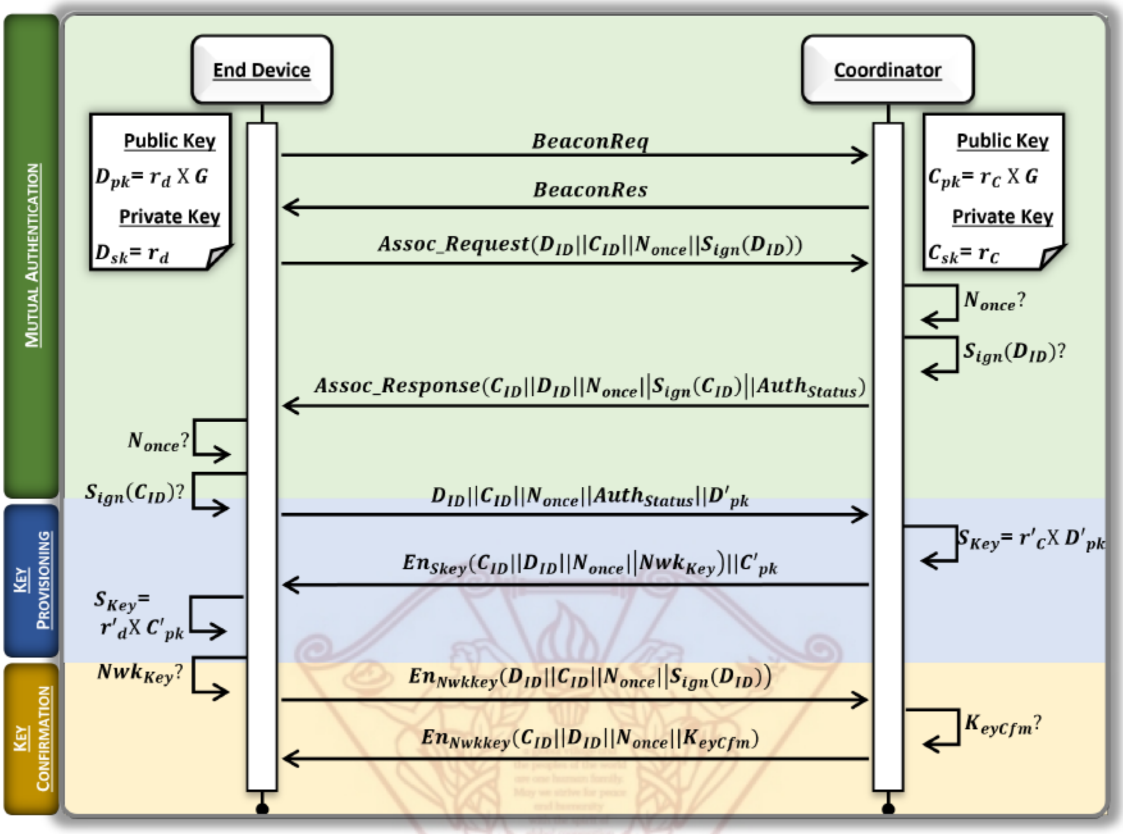

MUTUAL AUTHENTICATION
KEY PROVISIONING
KEY CONFIRMATION
End Device
Coordinator
Public Key
$D_{pk}= r_d$ X G
Private Key
$D_{sk}= r_d$
Public Key
$C_{pk}= r_C$ X G
Private Key
$C_{sk}= r_C$
BeaconReq
BeaconRes
$Assoc\_Request(D_{ID}||C_{ID}||N_{once}||S_{ign}(D_{ID}))$
N_{once}?
$S_{ign}(D_{ID})$?
$Assoc\_Response(C_{ID}||D_{ID}||N_{once}||S_{ign}(C_{ID})||Auth_{Status})$
N_{once}?
$S_{ign}(C_{ID})$?
$D_{ID}||C_{ID}||N_{once}||Auth_{Status}||D'_{pk}$
$S_{Key}= r'_C$X D'_{pk}
$En_{Skey}(C_{ID}||D_{ID}||N_{once}||Nwk_{Key})||C'_{pk}$
$S_{Key}= r'_d$X C'_{pk}
Nwk_{Key}?
$En_{Nwkkey}(D_{ID}||C_{ID}||N_{once}||S_{ign}(D_{ID}))$
K_{eyCfm}?
$En_{Nwkkey}(C_{ID}||D_{ID}||N_{once}||K_{eyCfm})$

Figure 4.3: Overall Workflow of Zero-effort Authentication and pairing

work. We assumed that both the communicating devices have generated a public-private key pair using elliptic curve cryptography. These key pair can be used to ensure security and privacy of our proposed zero-effort authentication and pairing mechanism. Initially, the end device broadcast a beacon request ($Beacon_{Req}$) on the communication channels and wait for response. When the coordinator receive device's $Beacon_{Req}$ in its open state, which illustrate that the coordinator can accept the devices to form a network. Therefore, a beacon response ($Beacon_{Res}$) is shared with the end devices from coordinator to notify about the network identifier and operational channel. The end device create and share an association request ($Assoc_{Request}$) with coordinator, which includes the communicating device identifiers (D_{ID}, C_{ID}), timestamp (T_S), and device self-signed identifier ($S_{ign_{D_{ID}}}$) of virtual context. The coordinator assess time delay ($\triangle T$), verify the $S_{ign_{D_{ID}}}$, then create its own self-signed identifier ($S_{ign_{C_{ID}}}$), which gets included in the association response

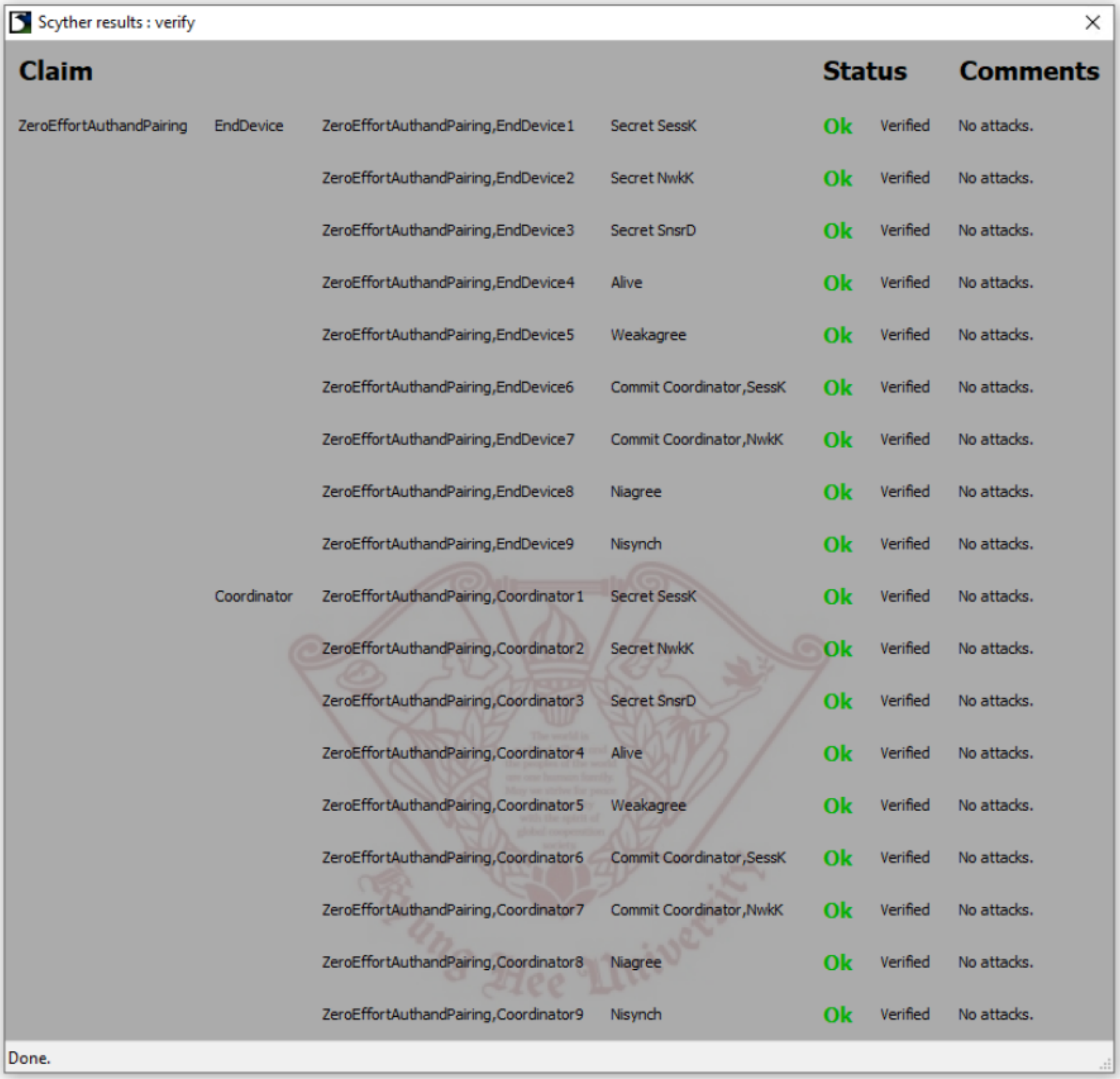
$(Assoc_{Response})$ and shared with the end device. Similarly, the end device assess the $\triangle T$ and verify $S_{ign_{C_{ID}}}$. After successful verification, the end device generate a new public-private key pair (D'_{pk}, r'_{d}) and share the public key (D'_{pk}) with coordinator. The coordinator also generate a new public-private key pair (C'_{pk}, r'_{c}) and generate a share secret key (S_{Key}) by taking a dot product of end device public key (D'_{pk}) and coordinator private key (r'_{c}). Then encrypt the network key (Nwk_{Key}) using the generated S_{Key} and share it with end device along with coordinator public key (C'_{pk}). Upon receiving, the end device create a share secret key (S_{Key}) by taking a dot product of coordinator public key (C'_{pk}) and end device private key (r'_{d}). Using S_{Key}, the end device decrypt the receive packet and extract the Nwk_{Key}. In order to prove the possession of Nwk_{Key}, the end device share the same $S_{ign_{D_{ID}}}$ generated in the authentication phase, encrypted with Nwk_{Key}. Finally, the coordinator validate the received $S_{ign_{D_{ID}}}$ and set the key confirmation status.

4.4 Evaluation and Results

Zero-effort authentication and pairing evolve the existing communication protocol with automated joining process and eliminate the assistance of user during the initial device authentication. The goal of our proposed approach was to improved the security and reduce the computational overhead. Therefore, we evaluated the proposed approach based on two evaluations metrics: i) Formal security analysis, and ii) Performance measure. The detail description about the mentioned evaluation criteria are described as follows:

4.4.1 Formal Security Analysis

According to our analysis, the existing user assistance approaches proposed for device authentication are vulnerable to the network key transportation attack due to the availability of virtual context in plaintext. Therefore, our proposed approach considered the vulnerabilities of existing approaches (such as key transportation, masquerading, eavesdropping, replay, and man-in-the-middle) and proposed a reliable zero-effort authentication and pairing mechanism. In order to prove our claims, we evaluated our proposed approach in different attacking environment using



Scyther results : verify

Claim				Status		Comments
ZeroEffortAuthandPairing	EndDevice	ZeroEffortAuthandPairing,EndDevice1	Secret SessK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice2	Secret NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice3	Secret SnsrD	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice4	Alive	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice5	Weakagree	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice6	Commit Coordinator,SessK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice7	Commit Coordinator,NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice8	Niagree	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,EndDevice9	Nisynch	Ok	Verified	No attacks.
	Coordinator	ZeroEffortAuthandPairing,Coordinator1	Secret SessK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator2	Secret NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator3	Secret SnsrD	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator4	Alive	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator5	Weakagree	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator6	Commit Coordinator,SessK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator7	Commit Coordinator,NwkK	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator8	Niagree	Ok	Verified	No attacks.
		ZeroEffortAuthandPairing,Coordinator9	Nisynch	Ok	Verified	No attacks.

Done.

Figure 4.4: Formal Security Analysis Result of Zero-effort Approach Using Scyther

two type of simulation tools such as Scyther and AVISPA [107–109]. Both tools utilize Dolev and Yao model, where adversary take full control of a network and actively try to tamper the data packets on the communication channel. Figure 4.4 present the formal security analysis results of our proposed approach obtained from Scyther, which identify the packets reachability among the communicating entities. The detailed description of the verified claims obtained from Scyther are described as follows.

- **Secret:** Zero-effort authentication and pairing approach generate the shared key by multiplying the elliptic curve primitives and encrypt network key with the computed shared key. Then use the received network key for encrypting the data transmitted over the communication channel. Therefore, our proposed approach verify the secret claim and ensure strong resistance against eavesdropping.

- **Alive:** Our proposed approach utilized the self-signed identifier of communicating entities for mutual authentication, which illustrate that only the device's private key can be used to generate such kind of signature. That ensure the integrity and prevent identity spoofing.

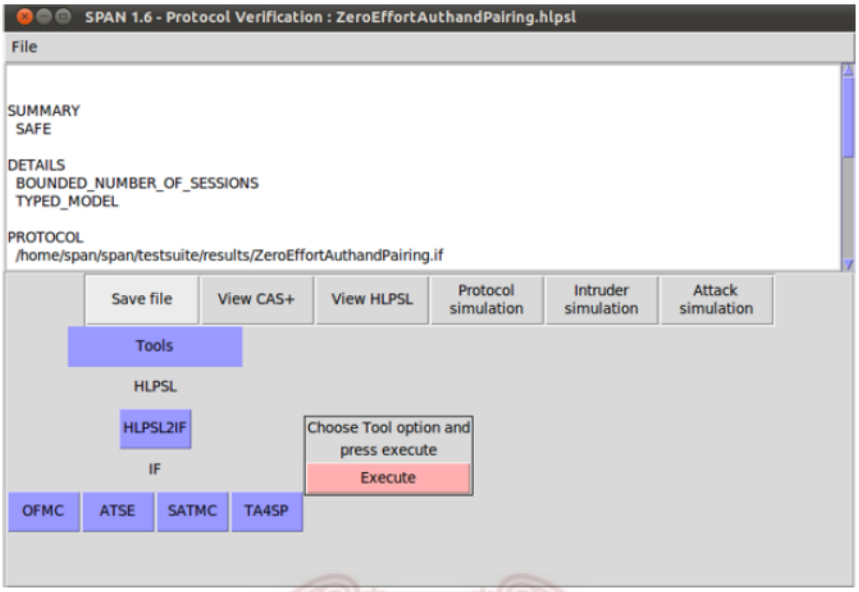
- **Weakagree:** Weak agreement (Weakagree) assess the identity and data authentication of targeted approach by evaluating in different attacking environment. Our proposed zero-effort mechanism used self-signed identifier for authentication and adopt integrated encryption scheme for key provision, which ensure verification and validation of device's identity and its transmitted data among the communicating entities.

- **Commit:** Commitment (Commit) evaluate the running events among the communicating entities, which includes key establishment, session management, and data exchange. Our proposed approach establish the shared key after successful authentication, assess the response time, and ensure the data security over the communication channel. Thus, verify the commit claim and prevent data loss.

- **Niagree:** Non-injective agreement (Niagree) assess the targeted approach for man-in-the-middle attack. Our proposed zero-effort mechanism consider identity based verification and validating between the communicating entities, which ensure strong resistance against man-in-the-middle attack.

- **Nisynch:** Our proposed zero-effort approach verify the Non-injective synchronization (Nisynch) because each message include a fresh nonce in form of timestamp, which ensure prevention against replay attack. In case of re-transmission, the packet will be discarded and the communicating entity has to initiate the authenticate process.

Furthermore, we evaluated the proposed zero-effort mechanism using the Automated Validation of Internet Security Protocols and Applications (AVISPA), which perform the assess-



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/ZeroEffortAuthandPairing.if
```

Figure 4.5: Formal Security Analysis Result of Zero-effort Approach Using AVISPA

ment based on a variety of attacking models such as On-the-Fly Model-Checker (OFMC) [110], Constraint Logic-based Attack Searcher (CL-ATSE) [111], Satisfiability-based Model Checker (SATMC) [112], and Tree Automata-based Protocol Analyzer (TA4SP) [113]. Each of these model support the adversary for identifying the specification, message generation and manipulation. Figure 4.5 presents the result of formal security analysis of zero-effort approach obtained from AVISPA. The summary report described that the proposed approach provide strong resistance to active and passive attacks, declared as SAFE because it provide source identity and data authentication, secrecy, and integrity. The evaluations were performed in a bounded number of sessions, under the assumption that attacker has full control of the network. In order to launch an offline attack, the existing and proposed approach required 2^{-256} attempts to retrieve the network key.

4.4.2 Performance Measure

The performance measure assess the efficiency of an algorithm in terms of operational, time, and memory overhead. We considered the limitation of resource constrained devices and designed the zero-effort approach to ensure the efficiency and reliability. In order to justify our claims, we identify the cryptographic primitives of both the existing and proposed approaches as shown

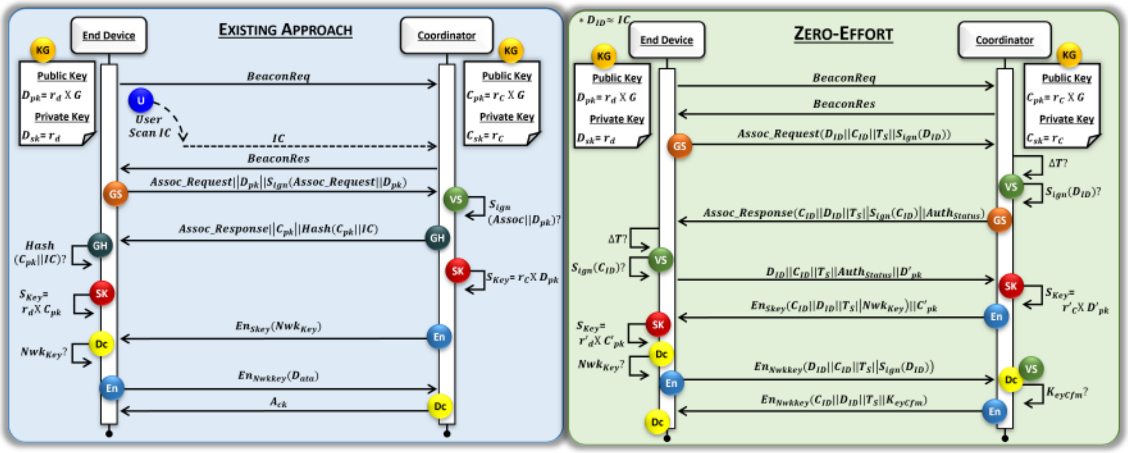
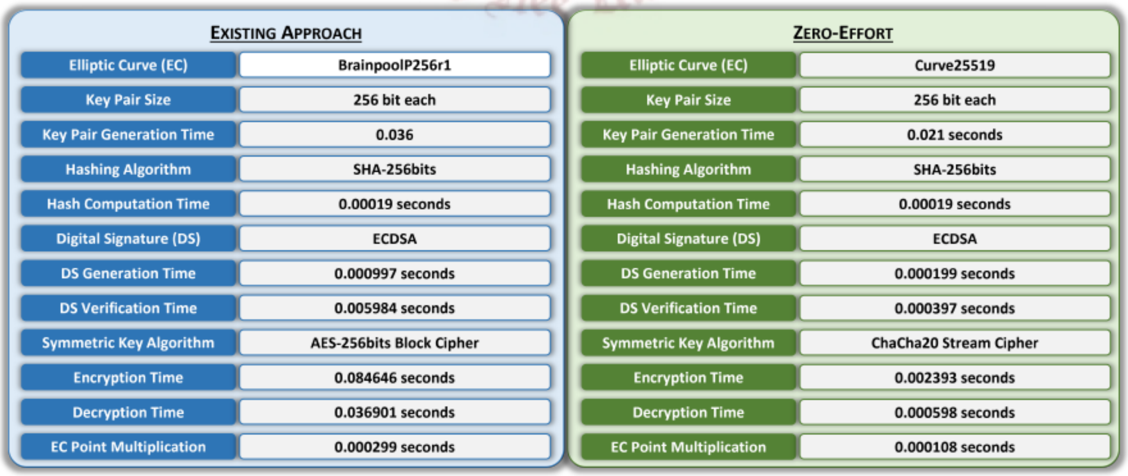


Figure 4.6: Comparison Workflow of Existing and Proposed Approaches

in Figure 4.6. These cryptographic primitives support in operational overhead identification on the end device and coordinator. We computed the average execution time of each cryptographic primitive and specify the exact algorithm adopted by the existing (Wang et al. [31]) and proposed (zero-effort) approaches. Figure 4.7 presents the obtained results. Wang et al. [31] uses the BrainpoolP256r1 curve for elliptic curve cryptography, which according to National Institute of Standards and Technology (NIST), not recommended for constrained devices. Therefore, we used the Curve25519, which is lightweight in nature and recommended for resource constrained de-



EXISTING APPROACH

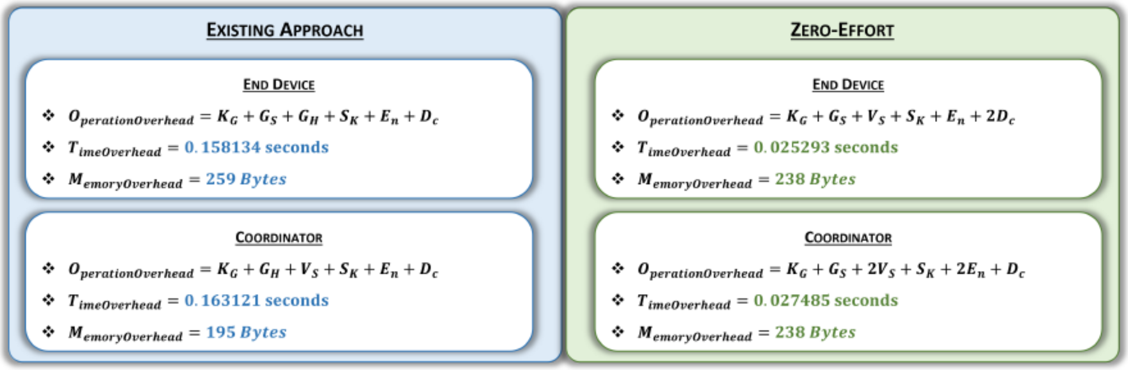
Elliptic Curve (EC)	BrainpoolP256r1
Key Pair Size	256 bit each
Key Pair Generation Time	0.036
Hashing Algorithm	SHA-256bits
Hash Computation Time	0.00019 seconds
Digital Signature (DS)	ECDSA
DS Generation Time	0.000997 seconds
DS Verification Time	0.005984 seconds
Symmetric Key Algorithm	AES-256bits Block Cipher
Encryption Time	0.084646 seconds
Decryption Time	0.036901 seconds
EC Point Multiplication	0.000299 seconds

ZERO-EFFORT

Elliptic Curve (EC)	Curve25519
Key Pair Size	256 bit each
Key Pair Generation Time	0.021 seconds
Hashing Algorithm	SHA-256bits
Hash Computation Time	0.00019 seconds
Digital Signature (DS)	ECDSA
DS Generation Time	0.000199 seconds
DS Verification Time	0.000397 seconds
Symmetric Key Algorithm	ChaCha20 Stream Cipher
Encryption Time	0.002393 seconds
Decryption Time	0.000598 seconds
EC Point Multiplication	0.000108 seconds

Figure 4.7: Computation Time of Existing and Proposed Approaches

vices. With the selection of an appropriate curve (Curve25519), the computational time of key pair generation, digital signature formation and verification, and point/dot multiplication have significantly reduced. Also, instead of block cipher (Advanced Encryption Standard) used in Wang et al. approach, we used the stream cipher (ChaCha20), which perform the addition, rotation, and exclusive disjunction for key stream generation and required 512 bits of memory for state maintenance. Moreover, the Secure Hash Algorithm (256 bits) was used as a cryptographic hash function by both the existing and proposed approaches. Based on the cryptographic primitive used by end device and coordinator, we formulated the operation overhead of existing and proposed approaches as shown in Figure 4.8. Using the execution time and algorithms information, we calculated the time and memory overhead for existing and proposed approaches. According to our analysis, the end device's time overhead of existing and proposed approaches were 0.158134 seconds and 0.025293 seconds respectively. Thus, the proposed zero-effort reduced 84% of time overhead on end device, compared with the Wang et al. approach. Similarly, the end device's memory overhead of existing and proposed approaches were 259 Bytes and 238 Bytes respective, which illustrate a reduction of 8.1%. From the coordinator perspective, 83.15% time overhead reduced as compared with the existing approach. However, the memory overhead of existing approach was 195 Bytes, while, our proposed approach was 238 Bytes. The difference of 43 bytes was due to the generated shared key using Curve25519, and fixed memory required for maintaining the state of selected stream cipher. Usually the coordinator are rich in resources, compared to the end devices and the 43 bytes of memory overhead can be accommodated without compromising the efficiency.



EXISTING APPROACH

END DEVICE

- $O_{perationOverhead} = K_G + G_S + G_H + S_K + E_n + D_c$
- $T_{imeOverhead} = 0.158134$ seconds
- $M_{emoryOverhead} = 259\ Bytes$

COORDINATOR

- $O_{perationOverhead} = K_G + G_H + V_S + S_K + E_n + D_c$
- $T_{imeOverhead} = 0.163121$ seconds
- $M_{emoryOverhead} = 195\ Bytes$

ZERO-EFFORT

END DEVICE

- $O_{perationOverhead} = K_G + G_S + V_S + S_K + E_n + 2D_c$
- $T_{imeOverhead} = 0.025293$ seconds
- $M_{emoryOverhead} = 238\ Bytes$

COORDINATOR

- $O_{perationOverhead} = K_G + G_S + 2V_S + S_K + 2E_n + D_c$
- $T_{imeOverhead} = 0.027485$ seconds
- $M_{emoryOverhead} = 238\ Bytes$

Figure 4.8: Performance Overhead of Existing and Proposed Approaches

Chapter 5

Co-presence based Pairing and Authentication

5.1 Introduction

The emergence of enterprise IoT enable devices to shared the data and facilitate the users with personalized services such as resource management [114], automation [115], and remote monitoring [116]. The sharing of data depends on the network architecture, which can be centralized, distributed, or federated. Each of these architectures utilized its own security mechanism to verify and validate the device identity, and ensure data transmission security [117]. Our emphasis was on identification of a single or group of devices based on their ambient context. The recent trend of smart devices usually have built-in onboard sensors, which sense the surrounding environment and utilized the data for a variety of services [118–120]. The goal of co-presence based pairing and authentication is to verify and validate the neighboring devices based on their ambient context, which can also be used for personalized services and reduce the computational overhead on the end devices for operating a separate communication protocol for authentication.

According to our analysis, the existing solution are proposed in two major perspectives such as user centric [121–124], and device centric [19, 28–30]. The user centric co-presence based approaches collect the data affiliated with a specific user and ensure the authentication of devices in user's possession. Such approaches first identify the user behavior based on the collected data and initiate the pairing process to select the legitimate devices in possession of the targeted user, preventing the contextual co-presence attack. In device-centric, each device sense the surrounding environment and utilize the collected data for identifying the legitimate devices within its proximity using pairing and authentication. The surrounding contextual data depends on the number of sensors involved in the data acquisition process and its corresponding data modalities such as the collected data can be either single or multimodal [125].

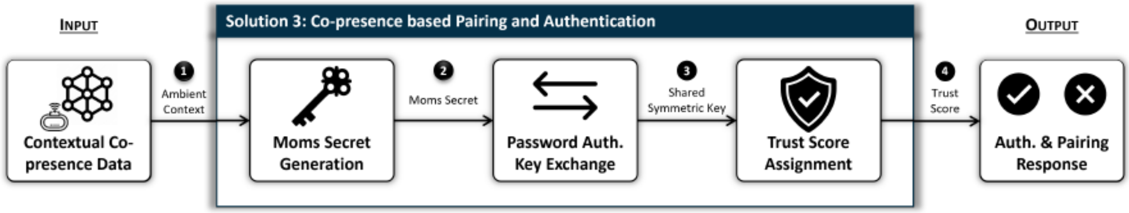


Figure 5.1: Co-presence based Pairing and Authentication

In this chapter, we focused on the device centric approaches that verify and validate the devices based on their co-presence-based contextual data. The existing co-presence-based pairing and authentication mechanisms adopt either fuzzy commitment or fuzzy password authenticated key exchange for device fingerprint generation using the collected data of surrounding environment [19, 28–30]. However, the fuzzy-based use error correction mechanism such as Reed-Solomon code, which detect and correct multiple symbol errors existed in the devices fingerprint generated from ambient context. The attacker can exploit this vulnerability to launch a contextual co-presence attack. In order to provide strong resistance against such type of attacks, the existing approaches generate the device fingerprint based on adequate amount of collected data that lead to prolong pairing time. Also, it increases the computational overhead due to collection and processing of large amount multimodal contextual data. Therefore, we proposed an innovative design of Median-of-Medians Password Authenticated Key Exchange (Moms PAKE), which generate the device fingerprint based on the selected data dimensions from different modalities and used it with PAKE for shared secret key establishment. Figure 5.1 present the overview of our proposed co-presence based pairing and authentication scheme, where the end device collects the ambient context, generate a Moms secret, then utilized the generated Moms Secret as a password for both the devices and establish a secret key. Upon successful key establishment, assign a trust score to each device based on the pairing attempt and success rate that supports in threats identification. The detail description about the components of our proposed approach are described as follows.

5.1.1 Moms Secret Generation based on Multimodality Data

We adopt our proposed Moms secret key generation mechanism as described in Chapter 3, but instead of using the uni-dimensional contextual data, we considered the multimodality and mul-

Algorithm 5.1: Co-presence based Pairing and Authentication

```
   Input: Co-presence-based Modalities Data $M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}}$
   Output: Authentication Status $A_{uthStatus}$
1  $\mathcal{M}_{Ctx} \leftarrow Load\ M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}}$
2  foreach $c \in \mathcal{M}_{Ctx}$ do
3      $M_{dims} \leftarrow dimension(c)$
4      if $M_{dims} > 1$ then
5          $M_{dic}(k_{ey}, v_{alue}) \leftarrow split(c, M_{dims})$
6          for $i\ in\ range(M_{dic})$ do
7              $D_{evMoms_{Secret}}[i] \leftarrow M_{omsSecret}(d)$
8          $O_{pMoms_{Secret}} \leftarrow Optimum_{Secret}(D_{evMoms_{Secret}})$
9      else
10         $O_{pMoms_{Secret}} \leftarrow M_{omsSecret}(c)$
11     $S_{electedMoms_{Secret}}.append(O_{pMoms_{Secret}})$
12 $D_{Shared_{Key}} \leftarrow PAKE(S_{electedMoms_{Secret}})$
13 if $D_{Shared_{Key}} == D'_{Shared_{Key}}$ then
14     $A_{uthStatus} \leftarrow Succeed$
15     $D_{T_{score}}, D'_{T_{score}} \leftarrow Assign\ T_{score}$
16 else
17     $A_{uthStatus} \leftarrow Failerd$
18     $D_{T_{score}}, D'_{T_{score}} \leftarrow Assign\ T_{score}$
```

tidimensional ambient data for Moms secret key generation as illustrated in Algorithm 5.1 (*line* 1 $\sim$ 11). Initially, the modalities data within the specified window size ($M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}}$) are loaded into contextual modality dataframe ($\mathcal{M}_{Ctx}$). Then assess the data dimension (M_{dims}) of each device ambient context (c) retrieved from $\mathcal{M}_{Ctx}$. In case of uni-dimensional data, the Moms secret ($M_{omsSecret}$) gets generated from the selected c and appended with the multimodal-based Moms Secret ($S_{electedMoms_{Secret}}$). If M_{dims} of a specific c has more than one data dimensional, then each dimension gets split into key-value pair and stores in modality dictionary ($M_{dic}(k_{ey}, v_{alue})$) for generating $M_{omsSecret}$. For each of M_{dims} existed in $M_{dic}(k_{ey}, v_{alue})$, generate a $M_{omsSecret}$ and store the resultant in $D_{evMoms_{Secret}}$, which gets parsed for selecting an optimum Moms secret ($O_{pMoms_{Secret}}$) based on the bits similarity score. The process repeats for all $c \in \mathcal{M}_{Ctx}$ and the selected $O_{pMoms_{Secret}}$ extracted from each $M_{nC_{t(ws)}}$ gets concatenated, producing the final multimodal-based Moms secret ($S_{electedMoms_{Secret}}$).

5.1.2 Password Authenticated Key Exchange

Password Authenticated Key Exchange (PAKE) presents the concept of establishing a shared secret key among the communicating entities using password known to the targeted devices [96, 97, 126]. PAKE rely on the concept of zero-knowledge proof, where the devices can verify and validate the possession of password without revealing or sharing it over the communication channel [95]. In PAKE, all the communicating entities must required to have the same password to derive a common secret key. Therefore, the security of our proposed co-presence-based pairing and authentication scheme rely on the generation of Moms secret among the participating devices. We used the generated multimodal-based Moms secret ($S_{electedMoms_{Secret}}$) as a password and adopt PAKE to generate 256 bits shared secret key as presented in Algorithm 5.1 ($line$ 12). PAKE provide strong resistance against offline analysis because the exchange of parameters occur online. In case of a spoofing attempt, the adversary gets only one chance to guess the accurate Moms secret for deriving the shared secret key within the acceptable pairing and authentication time.

5.1.3 Trust Score Assignment

In IoT, trust presents the integrity, strength and confidence of a specific entity, which can be assessed with interactive communication and network parameters [127]. Our proposed approach evaluate the device's trust based on the pairing attempts (P_{rAtt}) and success rate (S_{uccRt}). When all the communicating entities generate the shared secret key, then a simple challenge response protocol initiated to verify and validate the secret key possession among the devices. Upon assessment, set the authentication status ($A_{uthStatus}$) and assign the trust score (T_{score}) to each participating entity using equation 5.1. The P_{rAtt} identify the total number of pairing and authentication attempts with the targeted device. While, the S_{uccRt} is the number of successful attempts and summation ($\sum$) is used to maintain the state of P_{rAtt} and S_{uccRt} for each targeted device, which drastically reduce the trust score, if $P_{rAtt} > S_{uccRt}$.

$$T_{score} = \sum \frac{S_{uccRt}}{P_{rAtt}} \tag{5.1}$$

5.2 Comparison of Moms-PAKE with State-of-the-art

We compare our proposed approach with Fomichev et al. schemes [29, 30], which adopt fuzzy-based (Commitment, PAKE) approaches for fingerprint generation and allow pairing among the legitimate devices within proximity. Figure 5.2 presents the difference between existing and our proposed approaches. The existing schemes considered the low entropy ambient contextual data for device fingerprint generation, which can be exploited by the adversary for passive analysis and pattern identification. Also, the fuzzy-based approaches adopted in [29, 30], detect and correct multiple symbol errors existed in the device fingerprint and its exploitation may lead to contextual co-presence attack. For multimodal-based device fingerprint generation, the existing approaches select an interval based ambient contextual data, compute the average of each data dimension per modality, and concatenate it for increasing the search space. Such multimodal fusioning technique required randomized contextual value to avoid duplication/repetition in device fingerprint. Thus, the collection of sufficient data is required for randomized interval selection that leads to prolong pairing time because it depends on the rate of deviation in the ambient context. Also, it increases the computational and memory overhead on the end devices to process and store large interval contextual data respectively. Moreover, the pairing and authentication decision on the existing approaches are biased towards the multidimensional data. Therefore, we proposed an innovative design of Moms PAKE, which analyze the data dimension of acquired multimodal ambient context

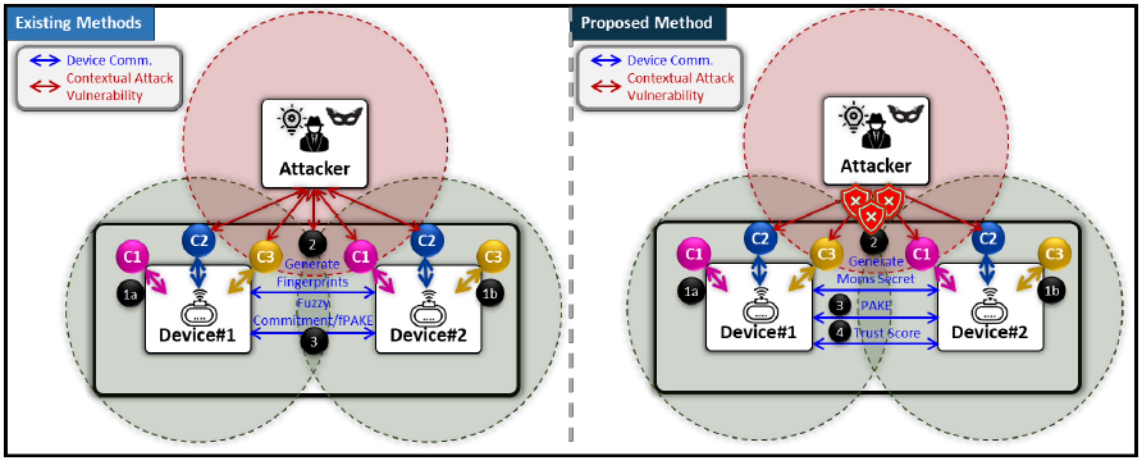


Figure 5.2: Co-presence based Pairing and Authentication - Existing vs Proposed Methodology

and selects one data dimension per modality for Moms secret generation. We used the generated multimodal-based Moms secret as a password for PAKE algorithm to generate a shared secret and assign a trust score accordingly to each communicating entity. The generated multimodal-based Moms secret have high entropy with low information gain (without selecting a randomized interval) and assign equal weights to each modality for optimum decision making, results in reduced pairing time. Also, we eliminate the use of fuzzy-based approaches for device fingerprint generation and ensure that the multimodal-based Moms secret correctly generated among the legitimate devices for PAKE.

5.3 Evaluation and Results

The security of our proposed co-presence-based pairing and authentication mechanism rely on the multimodal-based Moms secret, generated among the communicating entities. Therefore, we conducted an ablation study on the publicly available dataset to identify the similarity pattern of bits in the multidimensional data, then selects an appropriate data dimension per modality and generate the Moms secret among the communicating entities using the acquired ambient context. In order to prove our claims regarding efficiency and robustness, we evaluated our proposed approach based on two evaluation metrics, which includes pairing time, device identification and attack resistance rate. The acquired results of each evaluation criteria was compare with the state-of-the-art approaches of Fomichev et al. [29, 30] by reproducing their results. The detail description about the dataset selection, ablation study, and evaluation metrics are described as follows:

5.3.1 Dataset Selection

We analyzed the existing datasets proposed by Fomichev et al. for co-presence-based pairing and authentication [29, 30], which includes the data collection from different experimental scenarios using cars and offices. We selected the cars scenario, specifically the dataset that was produced and used for FastZIP evaluation [29], which is similar to our proposed Moms PAKE. The dataset includes accelerometer, gyroscope, and barometer data, collected from multiple smartphones placed in each car at different positions such as dashboard, seats, and trunk. Also, the authors defined the car's route in such away that it can cover a variety of scenarios from parking lots to city areas, and country roads. The interesting fact about the data collection was the adversarial and non-adversarial settings using two cars, which supports the pairing and authentication assessment under both circumstances.

5.3.2 Similarity Pattern Identification

In order to reduce the computation and memory overhead on end devices, we selected an appropriate data dimension per modality for multimodal Moms secret generation. For this purpose, we analyzed the existing dataset, which includes accelerometer, gyroscope, and barometer data. Accelerometer and gyroscope measure the acceleration and angular momentum of an object in three dimensional space x, y, and z respectively. While, barometer measure the atmospheric pressure in one dimensional space. Therefore, our proposed Moms PAKE required to selects one data dimensional from accelerometer and gyroscope, then append with barometer data for multimodal Moms secret generation. For this purpose, we use the sliding window concept for dataset parsing and compute the similarity pattern between data dimension. Initially, selects a fixed window size (w_s), then acquire accelerometer (a_x, a_y, a_z), gyroscope (g_x, g_y, g_z), and barometer (b_m) data within w_s. In order to identify the similarity pattern, we considered the

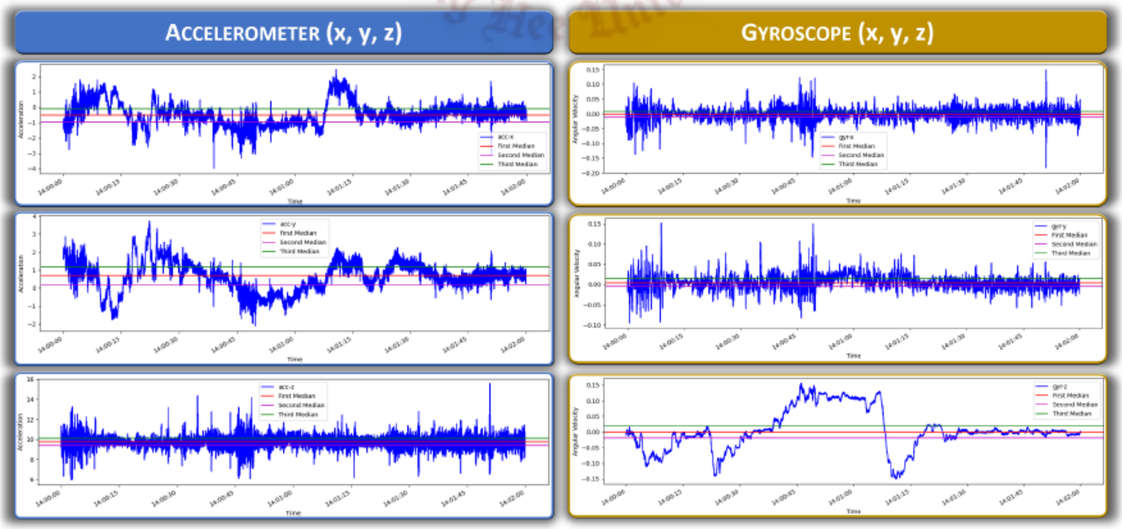
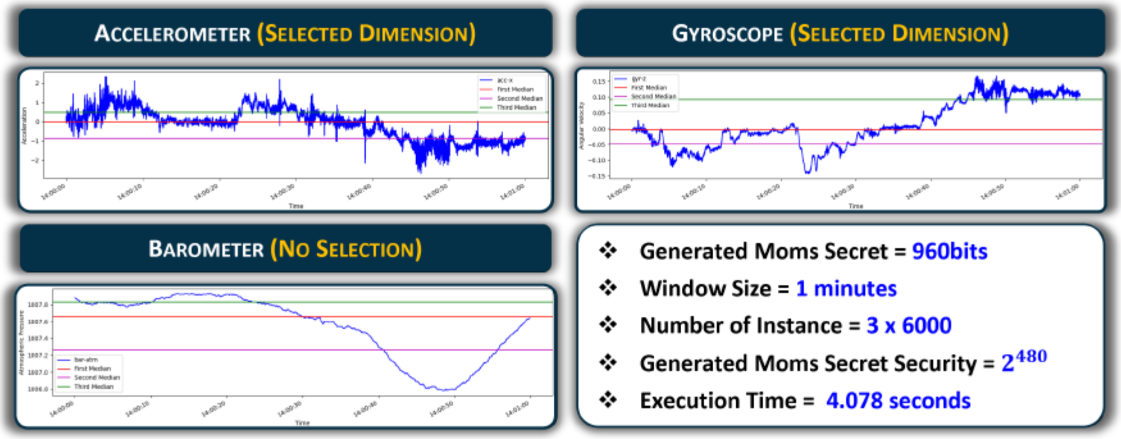


Figure 5.3: Accelerometer and Gyroscope Multidimensional Data Patterns

acquired data as one dimensional $(a_x, a_y, a_z, g_x, g_y, g_z, b_m)$ and generates the Moms secret as $(Moms_{sec_{a_x}}, Moms_{sec_{a_y}}, Moms_{sec_{a_z}}, Moms_{sec_{g_x}}, Moms_{sec_{g_y}}, Moms_{sec_{g_z}}, Moms_{sec_{b_m}})$. Then perform the bit-wise comparison between the Moms secret generated from data dimension affiliated with same modalities as $(Moms_{sec_{a_x}}, Moms_{sec_{a_y}})$, $(Moms_{sec_{a_x}}, Moms_{sec_{a_z}})$, $(Moms_{sec_{a_y}}, Moms_{sec_{a_z}})$, $(Moms_{sec_{g_x}}, Moms_{sec_{g_y}})$, $(Moms_{sec_{g_x}}, Moms_{sec_{g_z}})$, $(Moms_{sec_{g_y}}, Moms_{sec_{g_z}})$ for identifying the exact pattern of bits and compute the similarity score accordingly. The same process repeat for parsing the whole dataset by sliding the window incrementally, and finally compute the average similarity score.

According to our analysis on FastZIP dataset, 60.42% similar bits pattern existed in $(Moms_{sec_{a_x}}, Moms_{sec_{a_y}})$, 50.24% in $(Moms_{sec_{a_x}}, Moms_{sec_{a_z}})$, 51.45% in $(Moms_{sec_{a_y}}, Moms_{sec_{a_z}})$, 52.21% in $(Moms_{sec_{g_x}}, Moms_{sec_{g_y}})$, 48.78% in $(Moms_{sec_{g_x}}, Moms_{sec_{g_z}})$, and 53.63% in $(Moms_{sec_{g_y}}, Moms_{sec_{g_z}})$. Figure 5.3 presents a two minutes visual representation of accelerometer and gyroscope multidimensional data patterns. We identified that with the conversion of accelerometer and gyroscope multidimensional data into Moms secret, around 50% bits are similar because Moms secret extract the pattern out of multimodal data instead of relying on the exact values. Therefore, utilizing multidimensional data affilated with same modality will increase the computational overhead on end devices and leads to an unreliable Moms secret due to repeated bits pattern. Hence, the optimum and correctly generated multimodal-based Moms secret among the communicating entities can be extracted



ACCELEROMETER (SELECTED DIMENSION)

GYROSCOPE (SELECTED DIMENSION)

BAROMETER (NO SELECTION)

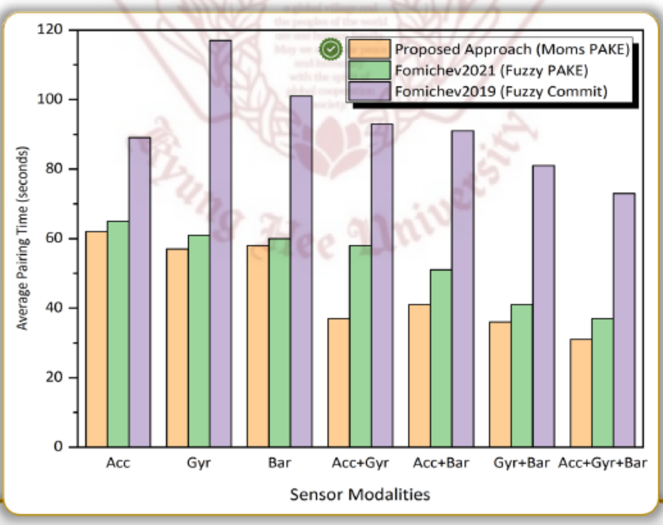
- Generated Moms Secret = 960bits
- Window Size = 1 minutes
- Number of Instance = 3 x 6000
- Generated Moms Secret Security = 2^{480}
- Execution Time = 4.078 seconds

Figure 5.4: Selected Data Dimension for Multimodal-based Moms Secret Generation

using the selected data dimension as ($Moms_{sec_{a_x}}||Moms_{sec_{g_z}}||Moms_{sec_{b_m}}$) on FastZIP dataset, where a_x measure rate of change in velocity, g_z measure the clockwise and counter clockwise rotation, and b_m measure air pressure. Figure 5.4 presents a sample of selected dimensions from multimodal data, which generate 960bits of Moms secret with 1 minute interval and complete one cycle in 4.078 seconds from data acquisition to multimodal-based Moms secret generation.

5.3.3 Pairing Time Assessment

Pairing is the establishment and computation of secret credential (such as key) among the communicating entities using the acquired contextual data. While, the time required for an end device to complete the pairing process from data collection to secret key establishment is known as pairing time. We evaluated the pairing time of our proposed Moms PAKE approach and compare with the state-of-the-art schemes of Fomichev et al. [29, 30]. For a fair comparison, we used the FastZIP dataset, select the window size (w_s) for multimodal data acquisition, and used two Raspberry



Comparison	Acc	Gyr	Bar	Acc+Gyr	Acc+Bar	Gyr+Bar	Acc+Gyr+Bar
$Moms_{PAKE}$ *vs* $Fuzzy_{PAKE}$	4.62%	6.56%	3.33%	36.21%	19.61%	12.2%	16.22%
$Moms_{PAKE}$ *vs* $Fuzzy_{Commit}$	30.34%	51.28%	42.57%	60.22%	54.95%	55.56%	57.53%

Figure 5.5: Pairing Time Comparison of Moms PAKE with Fuzzy PAKE and Fuzzy Commitment

Pi 4 Model B for Pairing time assessment. We assess pairing among the communicating entities (Raspberry Pi devices) using multimodal data selected in w_s, and incrementally slide the window upon completion of pairing process for the targeted scheme, then compute the average pairing time. For evaluating the impact of modalities on pairing time, we perform the assessment based on modalities (inspired from [29]) such as accelerometer (Acc), Gyroscope (Gyr), Barometer (Bar), Acc+Gyr, Acc+Bar, Gyr+Bar, and Acc+Gyr+Bar. Finally, we compared the achieved pairing time of Moms PAKE, Fuzzy PAKE [29], and Fuzzy Commitment [30] as shown in Figure 5.5.

According to our analysis, the Moms PAKE has reduced the pairing time, compared to Fuzzy PAKE [29], and Fuzzy Commitment [30]. For single modality based pairing using Acc, Gyr, and Bar, an average of 4.83% and 41.39% pairing time is reduced compared to Fuzzy PAKE and Fuzzy Commitment respectively. Similarly, an average of 22.67% (Fuzzy PAKE) and 56.91% (Fuzzy Commitment) on dual modalities, and 16.22% (Fuzzy PAKE) and 57.53% (Fuzzy Commitment) on triple modalities. The result shows that the reduction time of Fuzzy Commitment is high compared to the Fuzzy PAKE because it required randomized contextual value and use cryptographic hash function for proving the committed value. Also, we identified that with the increasing number of modalities, the pairing time decreases for all the approaches, and vice versa. Hence, our proposed Moms PAKE highly reduced the pairing time on triple modalities, compare to dual and single. Also, with the increasing number of modalities, the security of Moms PAKE increases as well.

5.3.4 Device Identification and Attack Resistance Rate

Device identification verify and validate the identity of legitimate devices within proximity based on the acquired ambient context and filtered out the malicious communicating entities. While, the attack resistance rate analyze the intelligence of an algorithm to assess the preventive strategy against the adversary for launching attacks. In order to evaluate the device identification and attack resistance rate, we used the same experimental setup described in section 5.3.3, which includes two Raspberry Pi 4 Model B devices, the FastZIP dataset, and sliding window with fixed w_s for data acquisition. The data collection in adversarial and non-adversarial settings of FastZIP dataset supports the real-time assessment of algorithms such as Moms PAKE, Fuzzy PAKE [29], and

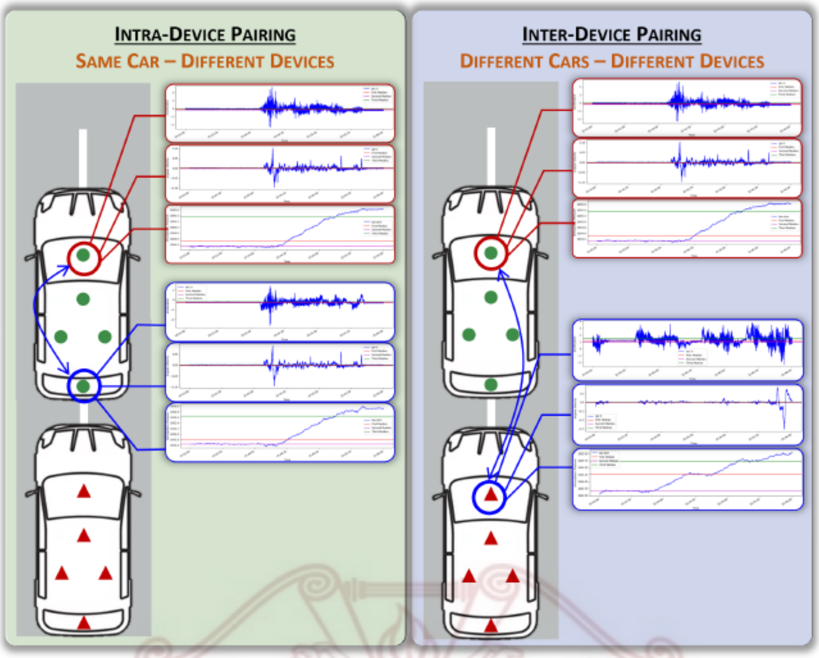
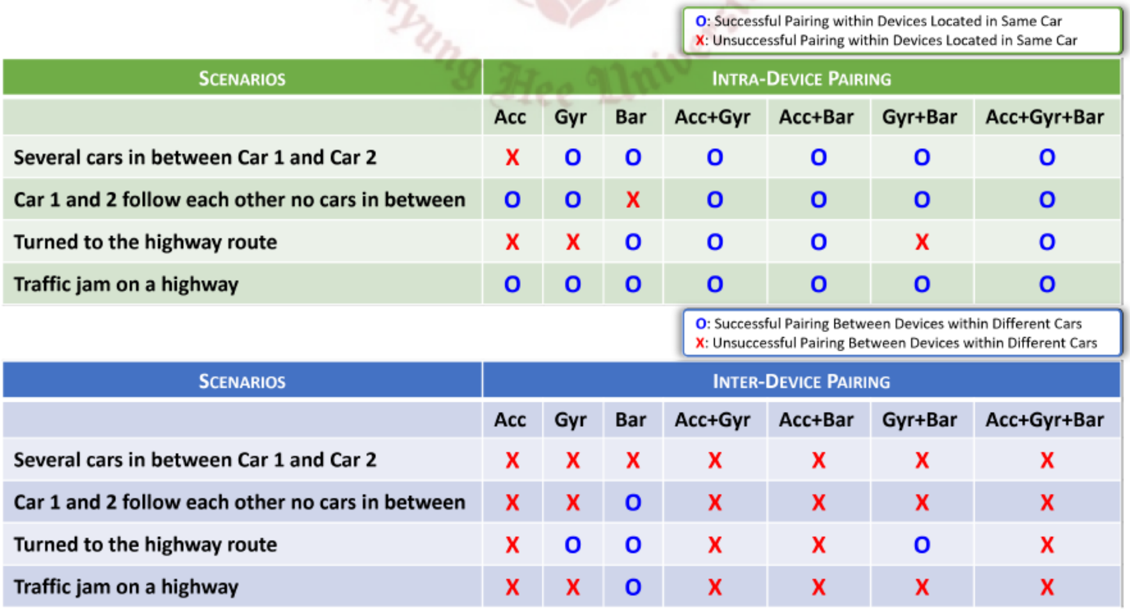

Intra-Device Pairing
Same Car – Different Devices
Inter-Device Pairing
Different Cars – Different Devices

Figure 5.6: Intra-Device and Inter-Device Pairing

Fuzzy Commitment [30]. For the assessment of these algorithms, we considered intra-device and inter-device pairing mechanisms based on triple modalities (accelerometer, gyroscope, barometer), presented in Figure 5.6.

The intra-device pairing establish the shared secret among the communicating entities within the same car. While, inter-device pairing establish the shared secret among the communicating entities between different cars. For intra-device pairing based on triple modalities, we used the data collected in non-adversarial settings of four cars and performs pairing among the devices placed in each car to achieve the average score of co-presence based device identification. In intra-device pairing, the device 1 (d_1) initiate pairing with d_2, d_3, d_4, and d_5, d_2 pairs with d_3, d_4, and d_5, d_3 pairs with d_4, and d_5, d_4 pairs with d_5, results in a total of ten pairing among each car, incrementally sliding the window with w_s after storing the resultant values. Similarly, we utilized the collected data in adversarial settings for inter-device pairing, where one-car follows the other to collects the same ambient context and acts as adversary for launching contextual co-presence attacks. In inter-device pairing, each device in the following car perform pairing attempt with the followed car devices to launch a contextual co-presence attack, results a total of twenty five pairing between car's devices. We analyzed the intra-device and inter-device pairing for co-presence based device identification and attack resistance rate respectively. According to our analysis, Moms PAKE achieved 93.04% co-presence based device identification on FastZIP dataset in non-adversarial settings. While, Fuzzy PAKE and Fuzzy Commitment attained 92.15% and 91.37% respectively. Similarly, the attack resistance rate computed based on the inter-device pairing using triple modalities, Moms PAKE achieved 96.91%, Fuzzy PAKE attained 93.64%, and Fuzzy Commitment secured 79.19%. The results shows that 0.95% and 1.79% co-presence based device identification gets improved using Moms PAKE, compared to Fuzzy PAKE and Fuzzy Commitment respectively. In terms of co-presence based attack resistance rate, Moms PAKE provide 3.37% and 18.28% strong resistance against contextual co-presence attacks, compared to Fuzzy PAKE and Fuzzy Commitment respectively. The low attack resistance rate of Fuzzy PAKE and Fuzzy Commitment are due to the fuzzy-based approach for device fingerprint generation that support the adversary (following car) to use its ambient contextual data collected in the adversarial settings and launch the co-presence attacks. Thus, our Moms PAKE improved the device identification and attack resistance rate, compare to the state-of-the-art approaches.

Moreover, we perform a pilot study to analyze the impact of our proposed Moms PAKE in term



O: Successful Pairing within Devices Located in Same Car
X: Unsuccessful Pairing within Devices Located in Same Car

Scenarios	Intra-Device Pairing						
	Acc	Gyr	Bar	Acc+Gyr	Acc+Bar	Gyr+Bar	Acc+Gyr+Bar
Several cars in between Car 1 and Car 2	X	O	O	O	O	O	O
Car 1 and 2 follow each other no cars in between	O	O	X	O	O	O	O
Turned to the highway route	X	X	O	O	O	X	O
Traffic jam on a highway	O	O	O	O	O	O	O

O: Successful Pairing Between Devices within Different Cars
X: Unsuccessful Pairing Between Devices within Different Cars

Scenarios	Inter-Device Pairing						
	Acc	Gyr	Bar	Acc+Gyr	Acc+Bar	Gyr+Bar	Acc+Gyr+Bar
Several cars in between Car 1 and Car 2	X	X	X	X	X	X	X
Car 1 and 2 follow each other no cars in between	X	X	O	X	X	X	X
Turned to the highway route	X	O	O	X	X	O	X
Traffic jam on a highway	X	X	O	X	X	X	X

Figure 5.7: Intra-Device and Inter-Device Pairing Scenario

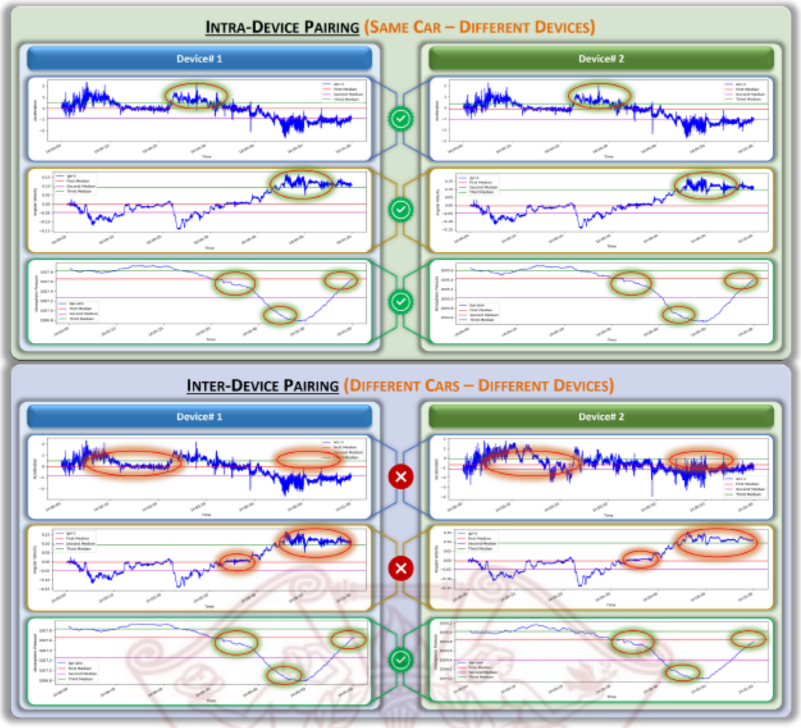


Figure 5.8: Intra-Device and Inter-Device Pairing Modalities Analysis

of mobility, and environmental factors. For this purpose, we analyze a 26 minute interval acquired from FastZIP dataset in adversarial setting, which includes four scenarios and evaluate each scenario with single, dual, triple modalities as shown in Figure 5.7. The experiments were performed in intra-device and inter-device pairing, which shows that our proposed Moms PAKE achieved good results with dual and triple modalities, compared to single modality. Figure 5.8 presents the analysis of modalities in term of intra-device and inter-device pairing. In single modality, barometer data is highly vulnerable to launch the contextual co-presence attack because it measure the environmental pressure, which can be capture by adversary within the same environment. Also, the gyroscope data on a highway can also support in inter-device pairing. In intra-device pairing, a minor change in the single modality data of different devices can lead to unsuccessful pairing such as turning or slope, where the devices at front and back acquired different contextual values. Our objective from this pilot study was to considered a diversified real-time use cases and improved our proposed Moms PAKE. In future, we will analyze the dataset for multiple scenarios and extend our proposed approach based on the results obtained from the pilot study.

Chapter 6

Conclusion and Future Work

In this chapter, we summarized the thesis with concluding remarks and provide future directions in the area of zero interaction and pairing. Furthermore, we described the relevant application areas of the proposed methodology.

6.1 Conclusion

In this dissertation, we focused on the ZIPA, which utilized the device physical, virtual, or ambient context to established secret key among the communicating entities and validate it accordingly. According to our analysis, the existing approaches used the low entropy contextual data of device as dynamic credential for cryptographic hash function, which required time synchronization and vulnerable to asynchronous attacks. Also, the existing user assistance pairing and authentication required human effort to setup the devices based on their virtual context, which required another interface or application to transmit the virtual context to centralized server for identity verification and validation, leads to increase operational overhead. Usually the device credentials are publicly available in the specification document, which supports the adversary for launching network key transportation attack. Moreover, the existing approaches that verify the neighboring devices based on their ambient context considered the fuzzy-based (commitment, PAKE) schemes for device fingerprint generation, which required sufficient contextual data with randomized value and support error correction mechanism for correcting multiple symbol errors. The collection of sufficient contextual data and error correction mechanism leads to prolong pairing time and contextual co-presence attacks respectively. Therefore, we proposed an efficient ZIPA scheme in terms of one-shot, zero-effort, and co-presence-based, which convert the low entropy contextual value to high entropy, reduce the pairing time, and ensure strong resistance against predictive contextual and key transportation attacks.

The one-shot pairing and authentication verify and validate the devices based on its physical context. The name one-shot described that only the end device contextual information will be used by the centralized server to verify and validate its identity. It is assumed that the device contextual data is already stored in a secured centralized repository and accessible to the server, which acquire physical context of a specific device based on its identity, establish a share secret key, and identify the end device based on the shared secret key. We compare our proposed one-shot approach with the Ustundag et al. context aware authentication mechanism [20] based on three evaluation metrics, which includes entropy assessment, probability of guessing attacks, and time complexity. The result shows that our proposed approach achieve high entropy, low probability of guessing attack, and low time complexity, compared to state-of-the-art approach.

In order to solve the identified network key transportation vulnerability in user assistance pairing, we proposed zero-effort authentication and pairing mechanism that evolve the existing protocols by eliminating the assistance from user during the initial authentication and improve security by reducing the operational overhead. Our proposed approach automate the device joining process by mutually authenticating the devices based on their corresponding self signed identifier and then adopt the integrated encryption scheme for key provision. Then confirm the generated shared secret key among the communicating devices. We compared our proposed approach with Wang et al. scheme [31] in terms of security and performance measure. The result shows that our proposed approach provide strong resistance against a variety of attacks such as man-in-the-middle, spoofing, data tampering and replay. Also, it reduced the operational overhead, time overhead, and memory overhead, compared to the state-of-the-art approach.

Moreover, we proposed an innovative design of Median-of-Medians Password Authenticated Key Exchange (Moms PAKE) for co-presence based device identification, which generate the device fingerprint based on the selected data dimensions from different modalities and used it with PAKE for shared secret key establishment. In our proposed approach, the end device collects the ambient context, generate a multimodal-based Moms secret, then utilized the generated Moms Secret as a password for both the devices and establish a secret key. Upon successful key establishment, assign a trust score to each device based on the pairing attempt and success rate that supports in threats identification. We compare our proposed approach with Fomichev et al. schemes [29, 30] based on pairing time, and device identification and attack resistance rate. The result shows that our proposed approach reduced the pairing time, and improve co-presence based device identification and attack resistance rate, compared to the state-of-the-art approaches.

6.2 Future Work

In future, we will analyze the impact of our proposed Moms PAKE based on speed, mobility, and environmental factors, then evaluate success rate, and failure rate of pairing and authentication. In our proposed approach, we considered that all the devices have same onboard sensors to collect the contextual data, which rise to other research questions:

1. How to handle the devices with different sensors?
2. How to deal with pairing and authentication, if the contextual data from one or more sensor is missing?
3. Is it possible to adaptively change the modalities for Moms Secret generation based on the availability of contextual data?
4. How to identify and prevent an insider threats in co-presence based pairing and authentication?

Considering these research questions, we will extend our proposed ZIPA scheme to further improve security, reliability and efficiency. Moreover, we will setup an actual testbed for realtime assessment of our proposed approach, instead of relying on publicly available datasets. Finally, we will considered machine learning and blockchain based technology for proposing a lightweight pairing and authentication mechanism.

6.3 Application Areas

Our proposed solutions can be applicable to a variety of application areas to provide efficient and robust pairing, utilizing the same contextual data for security and eliminate the use of specific

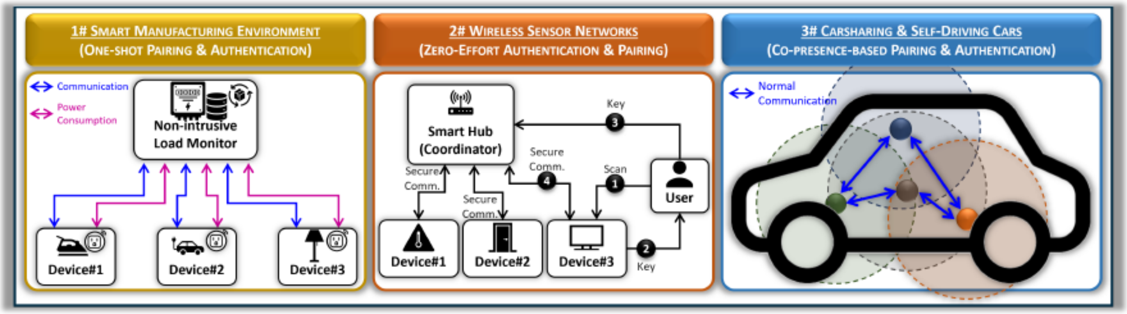

1# Smart Manufacturing Environment
(One-shot Pairing & Authentication)
Communication
Power Consumption
Non-intrusive Load Monitor
Device#1
Device#2
Device#3
2# Wireless Sensor Networks
(Zero-Effort Authentication & Pairing)
Smart Hub (Coordinator)
Key
3
Secure Comm.
Scan
1
4
User
Secure Comm.
Secure Comm.
Device#1
Device#2
Device#3
2
Key
3# Carsharing & Self-Driving Cars
(Co-presence-based Pairing & Authentication)
Normal Communication

Figure 6.1: Potential Application Areas of Our Proposed ZIPA Schemes

protocol for authentication. Figure 6.1 presents the visual representation of targeted application areas and the detail descriptions are described as follows:

6.3.1 Smart Manufacturing

With the industrial revolution, the smart technology has rapidly involved in the industries to automate the process, increase productivity, optimize the supply and demand to fulfill the customer needs [128, 129]. A significant part of smart manufacturing is the non-intrusive load monitoring system, which analyze the power consumption of each device and make an intelligent decision for cost reduction [130, 131]. In our proposed one-shot pairing and authentication, we considered such power consumption of devices and utilize it to established a shared secret among the communicating entities. Depending upon the availability of contextual data, our proposed one-shot approach can also be deployed in energy management system [132], appliance management system [133], and healthcare monitoring system [134], for improving the security.

6.3.2 Wireless Sensor Networks

The wireless sensor networks utilized sensors to analyze the environment and collects the data for monitoring purposes [135, 136]. The small embedded devices usually gets authenticated based on their virtual context to become a part of network, which required user assistance and increase burden on the human with increasing number of devices [137]. Therefore, our proposed zero-effort authentication and pairing mechanism evolve the existing protocols by eliminating the user assistance. Thus, applicable to all the potential application areas, where the communication protocol require assistance from user during the initial authentication, which includes mobile ad-hoc network [138], swarm intelligence [139], personal healthcare [140], and residential/industrial automation and control [141].

6.3.3 Carsharing and Self-driving Cars

The concept of carsharing and self-driving cars evolve the transportation industries by providing reliable services and comfortable trips [142, 143]. The embedded sensors of car sense the ambient context, identify the users for accessibility, and ensure the safe journey with optimum route selection [144]. Our proposed co-presence based pairing and authentication also utilize the ambient context, identify the legitimate devices within proximity and revoke the rights based on the rate of change in contextual data. Moreover, our proposed co-presence based approach can be applied in enterprise IoT [27], anti-theft system [145], and activity monitoring inside smart environment [85].

Bibliography

[1] A. Menychtas, C. Doukas, P. Tsanakas, and I. Maglogiannis, “A versatile architecture for building iot quantified-self applications,” in *2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS)*. IEEE, 2017, pp. 500–505.

[2] M. R. Bataineh, W. Mardini, Y. M. Khamayseh, and M. M. B. Yassein, “Novel and secure blockchain framework for health applications in iot,” *IEEE Access*, vol. 10, pp. 14 914–14 926, 2022.

[3] A. Almansoori, C. Ncube, and S. A. Salloum, “Internet of things impact on the future of cyber crime in 2050,” in *The International Conference on Artificial Intelligence and Computer Vision*. Springer, 2021, pp. 643–655.

[4] B. Sivathanu, “Adoption of internet of things (iot) based wearables for healthcare of older adults–a behavioural reasoning theory (brt) approach,” *Journal of Enabling Technologies*, 2018.

[5] F. Almalki, S. H. Alsamhi, R. Sahal, J. Hassan, A. Hawbani, N. Rajput, A. Saif, J. Morgan, J. Breslin *et al.*, “Green iot for eco-friendly and sustainable smart cities: future directions and opportunities,” *Mobile Networks and Applications*, pp. 1–25, 2021.

[6] Á. Verdejo Espinosa, J. L. López, F. Mata Mata, and M. E. Estevez, “Application of iot in healthcare: keys to implementation of the sustainable development goals,” *Sensors*, vol. 21, no. 7, p. 2330, 2021.

[7] L. Liu, “Iot and a sustainable city,” *Energy Procedia*, vol. 153, pp. 342–346, 2018.

[8] M. Khamis, M. Hassib, E. v. Zezschwitz, A. Bulling, and F. Alt, “Gazetouchpin: protecting sensitive data on mobile devices using secure multimodal authentication,” in *Proceedings of the 19th acm international conference on multimodal interaction*, 2017, pp. 446–450.

[9] X. Dong, R. Li, H. He, W. Zhou, Z. Xue, and H. Wu, “Secure sensitive data sharing on a big data platform,” *Tsinghua science and technology*, vol. 20, no. 1, pp. 72–80, 2015.

[10] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, “Iot forensics: Amazon echo as a use case,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487–6497, 2019.

[11] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, “{IoTPOT}: Analysing the rise of {IoT} compromises,” in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, 2015.

[12] F. Belanger, J. S. Hiller, and W. J. Smith, “Trustworthiness in electronic commerce: the role of privacy, security, and site attributes,” *The journal of strategic Information Systems*, vol. 11, no. 3-4, pp. 245–270, 2002.

[13] S. Katsikas and V. Gkioulos, “Security, privacy, and trustworthiness of sensor networks and internet of things,” p. 3846, 2020.

[14] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, and D.-H. Nguyen, “A survey of iot malware and detection methods based on static features,” *ICT Express*, vol. 6, no. 4, pp. 280–286, 2020.

[15] G. P. Hancke, K. E. Mayes, and K. Markantonakis, “Confidence in smart token proximity: Relay attacks revisited,” *Computers & Security*, vol. 28, no. 7, pp. 615–627, 2009.

[16] P. P. Churi, V. Ghate, and K. Ghag, “Jumbling-salting: an improvised approach for password encryption,” in *2015 International Conference on Science and Technology (TICST)*. IEEE, 2015, pp. 236–242.

[17] K. Marky, P. Mayer, N. Gerber, and V. Zimmermann, “Assistance in daily password generation tasks,” in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, 2018, pp. 786–793.

[18] M. D. Corner and B. D. Noble, “Zero-interaction authentication,” in *Proceedings of the 8th annual international conference on Mobile computing and networking*, 2002, pp. 1–11.

[19] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, “Context-based zero-interaction pairing and key evolution for advanced personal devices,” in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 880–891.

[20] E. Ustundag Soykan, L. KaraÇay, Z. Bilgin, E. Tomur, M. Akif Ersoy, F. KarakoÇ, and P. Çomak, “Context-aware authentication with dynamic credentials using electricity consumption data,” *The Computer Journal*, 2021.

[21] C. E. Shannon, “A mathematical theory of communication,” *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[22] J. Sühnel, “Zero interaction response surfaces, interaction functions and difference response surfaces for combinations of biologically active agents,” *Arzneimittel Forschung*, vol. 42, pp. 1251–1251, 1992.

[23] N. Schütz, S. E. Knobel, A. Botros, M. Single, B. Pais, V. Santschi, D. Gatica-Perez, P. Buluschek, P. Urwyler, S. M. Gerber *et al.*, “A systems approach towards remote health-monitoring in older adults: Introducing a zero-interaction digital exhaust,” *NPJ digital medicine*, vol. 5, no. 1, pp. 1–13, 2022.

[24] H. Zhang, W. Zhou, and H. Li, “Contextual adversarial attacks for object detection,” in *2020 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, 2020, pp. 1–6.

[25] M. Conti and C. Lal, “A survey on context-based co-presence detection techniques,” *arXiv preprint arXiv:1808.03320*, 2018.

[26] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, “Using contextual co-presence to strengthen zero-interaction authentication: Design, integration and usability,” *Pervasive and Mobile Computing*, vol. 16, pp. 187–204, 2015.

[27] N. Yu, J. Ma, X. Jin, J. Wang, and K. Chen, “Context-aware continuous authentication and dynamic device pairing for enterprise iot,” in *International Conference on Internet of Things*. Springer, 2019, pp. 114–122.

[28] M. Miettinen, T. D. Nguyen, A.-R. Sadeghi, and N. Asokan, “Revisiting context-based authentication in iot,” in *Proceedings of the 55th Annual Design Automation Conference*, 2018, pp. 1–6.

[29] M. Fomichev, J. Hesse, L. Almon, T. Lippert, J. Han, and M. Hollick, “Fastzip: faster and more secure zero-interaction pairing,” in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, 2021, pp. 440–452.

[30] M. Fomichev, M. Maass, L. Almon, A. Molina, and M. Hollick, “Perils of zero-interaction security in the internet of things,” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 1, pp. 1–38, 2019.

[31] W. Wang, F. Cicala, S. R. Hussain, E. Bertino, and N. Li, “Analyzing the attack landscape of zigbee-enabled iot systems and reinstating users’ privacy,” in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 133–143.

[32] L. Li, P. Podder, and E. Hoque, “A formal security analysis of zigbee (1.0 and 3.0),” in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, 2020, pp. 1–11.

[33] S. Khanji, F. Iqbal, and P. Hung, “Zigbee security vulnerabilities: Exploration and evaluating,” in *2019 10th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2019, pp. 52–57.

[34] C. B. Liang, M. Tabassum, S. B. A. Kashem, Z. Zama, P. Suresh, and U. Saravanakumar, “Smart home security system based on zigbee,” in *Advances in Smart System Technologies*. Springer, 2021, pp. 827–836.

[35] S. Okada, D. Miyamoto, Y. Sekiya, and H. Nakamura, “Proposal for ldos attack using indirect transmission in zigbee and a countermeasure against it,” *IEICE Technical Report; IEICE Tech. Rep.*, vol. 120, no. 413, pp. 179–184, 2021.

[36] E. T. Michailidis and D. Vouyioukas, “A review on software-based and hardware-based authentication mechanisms for the internet of drones,” *Drones*, vol. 6, no. 2, p. 41, 2022.

[37] M. T. Arafin and G. Qu, “Hardware-based authentication applications,” in *Authentication of Embedded Devices*. Springer, 2021, pp. 145–181.

[38] W.-H. Lee and R. Lee, “Implicit sensor-based authentication of smartphone users with smartwatch,” in *Proceedings of the Hardware and Architectural Support for Security and Privacy 2016*, 2016, pp. 1–8.

[39] M. Stipčević and Ç. K. Koç, “True random number generators,” in *Open Problems in Mathematics and Computational Science*. Springer, 2014, pp. 275–315.

[40] Y. Gao, S. F. Al-Sarawi, and D. Abbott, “Physical unclonable functions,” *Nature Electronics*, vol. 3, no. 2, pp. 81–91, 2020.

[41] R. Elbaz, L. Torres, G. Sassatelli, P. Guillemin, M. Bardouillet, and A. Martinez, “Block-level added redundancy explicit authentication for parallelized encryption and integrity checking of processor-memory transactions,” in *Transactions on Computational Science X*. Springer, 2010, pp. 231–260.

[42] J. D. Osborn and D. C. Challener, “Trusted platform module evolution,” *Johns Hopkins APL Technical Digest (Applied Physics Laboratory)*, vol. 32, no. 2, pp. 536–543, 2013.

[43] A. Conklin, G. Dietrich, and D. Walz, “Password-based authentication: a system perspective,” in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. IEEE, 2004, pp. 10–pp.

[44] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” *International journal of human-computer studies*, vol. 63, no. 1-2, pp. 102–127, 2005.

[45] O. Alpar, “Intelligent biometric pattern password authentication systems for touchscreens,” *Expert Systems with Applications*, vol. 42, no. 17-18, pp. 6286–6294, 2015.

[46] M. Dell'Amico, P. Michiardi, and Y. Roudier, "Password strength: An empirical analysis," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–9.

[47] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 44–55.

[48] A. Bhawiyuga, M. Data, and A. Warda, "Architectural design of token based authentication of mqtt protocol in constrained iot device," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, 2017, pp. 1–4.

[49] I. Indu, R. A. PM, and V. Bhaskar, "Encrypted token based authentication with adapted saml technology for cloud web services," *Journal of Network and Computer Applications*, vol. 99, pp. 131–145, 2017.

[50] V. Radha and D. H. Reddy, "A survey on single sign-on techniques," *Procedia Technology*, vol. 4, pp. 134–139, 2012.

[51] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using iot enabled devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1419–1434, 2021.

[52] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[53] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications surveys & tutorials*, vol. 14, no. 2, pp. 380–400, 2011.

[54] M. Conti and C. Lal, "Context-based co-presence detection techniques: A survey," *Computers & Security*, vol. 88, p. 101652, 2020.

[55] M. Mehta and K. Patel, "A review for iot authentication–current research trends and open challenges," *Materials Today: Proceedings*, 2020.

[56] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.

[57] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, 2015.

[58] A. Biryukov and L. Perrin, "State of the art in lightweight symmetric cryptography," *Cryptology ePrint Archive*, 2017.

[59] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in iot," in *2017 International Conference on IoT and Application (ICIOT)*. IEEE, 2017, pp. 1–4.

[60] A. Darwish, M. M. El-Gendy, and A. E. Hassanien, "A new hybrid cryptosystem for internet of things applications," in *Multimedia Forensics and Security*. Springer, 2017, pp. 365–380.

[61] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h) authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 1099–1112.

[62] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*, 2017, pp. 73–78.

[63] M. Juuti, C. Vaas, I. Sluganovic, H. Liljestrand, N. Asokan, and I. Martinovic, "Stash: Securing transparent authentication schemes using prover-side proximity verification," in *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2017, pp. 1–9.

[64] W. S. Melo, R. Machado, and L. F. Carmo, "Using physical context-based authentication against external attacks: Models and protocols," *Security and Communication Networks*, vol. 2018, 2018.

[65] U. C. Cabuk, G. Dalkilic, and O. Dagdeviren, “Comad: Context-aware mutual authentication protocol for drone networks,” *IEEE Access*, vol. 9, pp. 78 400–78 414, 2021.

[66] Y. Yang, X. Zhang, J. Yu, P. Zhang *et al.*, “Research on the hash function structures and its application,” *Wireless Personal Communications*, vol. 94, no. 4, pp. 2969–2985, 2017.

[67] H. Huang, X. Miao, Z. Wu, and Q. Wei, “An efficient ecc-based authentication scheme against clock asynchronous for spatial information network,” *Mathematical Problems in Engineering*, vol. 2021, 2021.

[68] A. Lesne, “Shannon entropy: a rigorous notion at the crossroads between probability, information theory, dynamical systems and statistical physics,” *Mathematical Structures in Computer Science*, vol. 24, no. 3, 2014.

[69] M. Jakobsson and D. Pointcheval, “Mutual authentication for low-power mobile devices,” in *International Conference on Financial Cryptography.* Springer, 2001, pp. 178–195.

[70] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for m2m communications in industrial iot environment,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 288–296, 2017.

[71] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. García, “Lightweight authentication protocol for m2m communications of resource-constrained devices in industrial internet of things,” *Sensors*, vol. 20, no. 2, p. 501, 2020.

[72] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, “Insecure to the touch: attacking zigbee 3.0 via touchlink commissioning,” in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 230–240.

[73] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, “Lightweight and secure authentication scheme for iot network based on publish–subscribe fog computing model,” *Computer Networks*, vol. 199, p. 108465, 2021.

[74] Y. Lu, D. Wang, M. S. Obaidat, and P. Vijayakumar, “Edge-assisted intelligent device authentication in cyber-physical systems,” *IEEE Internet of Things Journal*, 2022.

[75] A. Adeel, M. Ali, A. N. Khan, T. Khalid, F. Rehman, Y. Jararweh, and J. Shuja, “A multi-attack resilient lightweight iot authentication scheme,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3676, 2022.

[76] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, “Ensemble: cooperative proximity-based authentication,” in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 331–344.

[77] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, “Proximate: proximity-based secure pairing using ambient wireless signals,” in *Proceedings of the 9th international conference on Mobile systems, applications, and services*, 2011, pp. 211–224.

[78] T. Halevi, D. Ma, N. Saxena, and T. Xiang, “Secure proximity detection for nfc devices based on ambient sensor data,” in *European Symposium on Research in Computer Security*. Springer, 2012, pp. 379–396.

[79] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, “Proximity-based security techniques for mobile users in wireless networks,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2089–2100, 2013.

[80] D. Schurmann and S. Sigg, “Secure communication based on ambient audio,” *IEEE Transactions on mobile computing*, vol. 12, no. 02, pp. 358–370, 2013.

[81] T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris, and T. Xiang, “Context-aware defenses to rfid unauthorized reading and relay attacks,” *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 2, pp. 307–318, 2013.

[82] P. Urien and S. Piramuthu, “Elliptic curve-based rfid/nfc authentication with temperature sensor input for relay attacks,” *Decision Support Systems*, vol. 59, pp. 28–36, 2014.

[83] N. Karapanos, C. Marforio, C. Soriente, and S. Capkun, "{Sound-Proof}: Usable {Two-Factor} authentication based on ambient sound," in *24th USENIX security symposium (USENIX security 15)*, 2015, pp. 483–498.

[84] Z. Gu and Y. Liu, "Scalable group audio-based authentication scheme for iot devices," in *2016 12th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2016, pp. 277–281.

[85] J. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, "Do you feel what i hear? enabling autonomous iot device pairing using different sensor types," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 836–852.

[86] M. Beale, H. Uchiyama, and J. C. Clifton, "Iot evolution: What's next?" *IEEE Wireless Communications*, vol. 28, no. 5, pp. 5–7, 2021.

[87] M. Ezechina, K. Okwara, and C. Ugboaja, "The internet of things (iot): a scalable approach to connecting everything," *The International Journal of Engineering and Science*, vol. 4, no. 1, pp. 09–12, 2015.

[88] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: Evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, 2020.

[89] L. B. Oliveira, D. F. Aranha, C. P. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab, "Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer communications*, vol. 34, no. 3, pp. 485–493, 2011.

[90] A. Primo, V. V. Phoha, R. Kumar, and A. Serwadda, "Context-aware active authentication using smartphone accelerometer measurements," in *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, 2014, pp. 98–105.

[91] R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior," *IEEE Access*, vol. 7, pp. 119 654–119 667, 2019.

[92] M. Baldauf, S. Dustdar, and F. Rosenberg, “A survey on context-aware systems,” *International Journal of ad Hoc and ubiquitous Computing*, vol. 2, no. 4, pp. 263–277, 2007.

[93] T. Sylla, M. A. Chalouf, F. Krief, and K. Samaké, “Context-aware security in the internet of things: a survey,” *International journal of autonomous and adaptive communications systems*, vol. 14, no. 3, pp. 231–263, 2021.

[94] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan, “An enhanced pairing-based authentication scheme for smart grid communications,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2021.

[95] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *Journal of cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[96] C. Boyd, P. Montague, and K. Nguyen, “Elliptic curve based password authenticated key exchange protocols,” in *Australasian Conference on Information Security and Privacy*. Springer, 2001, pp. 487–501.

[97] M. Abdalla, M. Barbosa, T. Bradley, S. Jarecki, J. Katz, and J. Xu, “Universally composable relaxed password authenticated key exchange,” in *Annual International Cryptology Conference*. Springer, 2020, pp. 278–307.

[98] S. Makonin, “AMPds2: The Almanac of Minutely Power dataset (Version 2),” 2016. [Online]. Available: https://doi.org/10.7910/DVN/FIE0S4

[99] L. Pereira, D. Costa, and M. Ribeiro, “A residential labeled dataset for smart meter data analytics,” *Scientific Data*, vol. 9, no. 1, pp. 1–11, 2022.

[100] I. Chivers and J. Sleightholme, “An introduction to algorithms and the big o notation,” in *Introduction to programming with Fortran*. Springer, 2015, pp. 359–364.

[101] S. Bae, “Big-o notation,” in *JavaScript Data Structures and Algorithms*. Springer, 2019, pp. 1–11.

[102] D. D. Sleator and R. E. Tarjan, “Time complexity in big o notation.”

[103] B. Applebaum, N. Haramaty-Krasne, Y. Ishai, E. Kushilevitz, and V. Vaikuntananthan, "Low-complexity cryptographic hash functions," 2017.

[104] "Time complexity of computing cryptographic hash," https://crypto.stackexchange.com/questions/67448/what-is-the-time-complexity-of-computing-a-cryptographic-hash-function-random-o (Accessed on August 19, 2021).

[105] "The market of smart home devices," https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/, (Accessed on August 19, 2021).

[106] I. Magomedov, A. Bagov, and A. Zolkin, "Internet of things: future business," in *European Proceedings of Social and Behavioural Sciences EpSBS*, 2020, pp. 553–558.

[107] "The scyther tool," https://people.cispa.io/cas.cremers/scyther/, (Accessed on January 11, 2021).

[108] T. Team *et al.*, "Avispa v1. 1 user manual," *Information society technologies programme (June 2006) http://avispa-project. org*, 2006.

[109] T. Genet, "A short span+ avispa tutorial," Ph.D. dissertation, IRISA, 2015.

[110] D. Basin, S. Mödersheim, and L. Vigano, "An on-the-fly model-checker for security protocol analysis," in *European Symposium on Research in Computer Security*. Springer, 2003, pp. 253–270.

[111] M. Turuani, "The cl-atse protocol analyser," in *International conference on rewriting techniques and applications*. Springer, 2006, pp. 277–286.

[112] A. Armando and L. Compagna, "Satmc: a sat-based model checker for security protocols," in *European workshop on logics in artificial intelligence*. Springer, 2004, pp. 730–733.

[113] R. Küsters and T. Wilke, "Automata-based analysis of recursive cryptographic protocols," in *Annual Symposium on Theoretical Aspects of Computer Science*. Springer, 2004, pp. 382–393.

[114] S. Ahmad and D. Kim, “A multi-device multi-tasks management and orchestration architecture for the design of enterprise iot applications,” *Future Generation Computer Systems*, vol. 106, pp. 482–500, 2020.

[115] J. Pisarov and G. Mester, “Implementing new mobility concepts with autonomous self-driving robotic cars,” *IPSI Transactions on Advanced Research (TAR)*, vol. 17, no. 2, pp. 41–49, 2021.

[116] N. Sharma, M. Mangla, S. N. Mohanty, D. Gupta, P. Tiwari, M. Shorfuzzaman, and M. Rawashdeh, “A smart ontology-based iot framework for remote patient monitoring,” *Biomedical Signal Processing and Control*, vol. 68, p. 102717, 2021.

[117] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, “Survey on enterprise internet-of-things systems (e-iot): A security perspective,” *Ad Hoc Networks*, vol. 125, p. 102728, 2022.

[118] B. A. Hickey, T. Chalmers, P. Newton, C.-T. Lin, D. Sibbritt, C. S. McLachlan, R. Clifton-Bligh, J. Morley, and S. Lal, “Smart devices and wearable technologies to detect and monitor mental health conditions and stress: A systematic review,” *Sensors*, vol. 21, no. 10, p. 3461, 2021.

[119] B. B. Sinha and R. Dhanalakshmi, “Recent advancements and challenges of internet of things in smart agriculture: A survey,” *Future Generation Computer Systems*, vol. 126, pp. 169–184, 2022.

[120] M. Alamer and M. A. Almaiah, “Cybersecurity in smart city: A systematic mapping study,” in *2021 International Conference on Information Technology (ICIT)*. IEEE, 2021, pp. 719–724.

[121] S. Mekruksavanich and A. Jitpattanakul, “Deep learning approaches for continuous authentication based on activity patterns using mobile sensing,” *Sensors*, vol. 21, no. 22, p. 7519, 2021.

[122] A. Z. Zaidi, C. Y. Chong, Z. Jin, R. Parthiban, and A. S. Sadiq, "Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 191, p. 103162, 2021.

[123] G. Cola, A. Vecchio, and M. Avvenuti, "Continuous authentication through gait analysis on a wrist-worn device," *Pervasive and Mobile Computing*, vol. 78, p. 101483, 2021.

[124] A. Vecchio, R. Nocerino, and G. Cola, "Gait-based authentication: Evaluation of energy consumption on commercial devices," in *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 2022, pp. 793–798.

[125] P. Delgado-Santos, G. Stragapede, R. Tolosana, R. Guest, F. Deravi, and R. Vera-Rodriguez, "A survey of privacy vulnerabilities of mobile device sensors," *ACM Computing Surveys (CSUR)*, vol. 54, no. 11s, pp. 1–30, 2022.

[126] P. MacKenzie, S. Patel, and R. Swaminathan, "Password-authenticated key exchange based on rsa," in *International conference on the theory and application of cryptology and information security*. Springer, 2000, pp. 599–613.

[127] U. U. Rehman, A. Ali, H. S. M. Bilal, M. A. Razzaq, S.-B. Park, and S. Lee, "A novel mutual trust evaluation method for identification of trusted devices in smart environment," in *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*. IEEE, 2022, pp. 1–4.

[128] P. Zheng, Z. Sang, R. Y. Zhong, Y. Liu, C. Liu, K. Mubarok, S. Yu, X. Xu *et al.*, "Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives," *Frontiers of Mechanical Engineering*, vol. 13, no. 2, pp. 137–150, 2018.

[129] B. Wang, F. Tao, X. Fang, C. Liu, Y. Liu, and T. Freiheit, "Smart manufacturing and intelligent manufacturing: A comparative review," *Engineering*, vol. 7, no. 6, pp. 738–757, 2021.

[130] A. U. Rehman, S. R. Tito, P. Nieuwoudt, G. Imran, T. T. Lie, B. Vallès, and W. Ahmad, "Applications of non-intrusive load monitoring towards smart and sustainable power grids: A

system perspective," in *2019 29th Australasian Universities Power Engineering Conference (AUPEC)*. IEEE, 2019, pp. 1–6.

[131] M. Sun, F. M. Nakoty, Q. Liu, X. Liu, Y. Yang, and T. Shen, "Non-intrusive load monitoring system framework and load disaggregation algorithms: A survey," in *2019 International Conference on Advanced Mechatronic Systems (ICAMechS)*. IEEE, 2019, pp. 284–288.

[132] C. Ju, P. Wang, and Y. Xu, "Two-stage energy management of residential microgrid community using pairing strategy," in *2017 IEEE Power & Energy Society General Meeting*. IEEE, 2017, pp. 1–5.

[133] S. Pan, C. Ruiz, J. Han, A. Bannis, P. Tague, H. Y. Noh, and P. Zhang, "Universense: Iot device pairing through heterogeneous sensing signals," in *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*, 2018, pp. 55–60.

[134] N. Gayathri, G. Thumbur, P. R. Kumar, M. Z. U. Rahman, P. V. Reddy *et al.*, "Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9064–9075, 2019.

[135] K. Gulati, R. S. K. Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in internet of things (iot)," *Materials Today: Proceedings*, vol. 51, pp. 161–165, 2022.

[136] X. Wei, H. Guo, X. Wang, X. Wang, and M. Qiu, "Reliable data collection techniques in underwater wireless sensor networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 404–431, 2021.

[137] N. Temene, C. Sergiou, C. Georgiou, and V. Vassiliou, "A survey on mobility in wireless sensor networks," *Ad Hoc Networks*, vol. 125, p. 102726, 2022.

[138] D. S. Gupta, S. H. Islam, M. S. Obaidat, and K.-F. Hsiao, "A novel identity-based deniable authentication protocol using bilinear pairings for mobile ad hoc networks." *Adhoc & Sensor Wireless Networks*, vol. 47, 2020.

[139] Q.-V. Pham, N.-N. Dao, T. Huynh-The, J. Zhao, and W.-J. Hwang, “Clustering and power allocation for uav-assisted noma-vlc systems: A swarm intelligence approach,” *arXiv preprint arXiv:2007.15430*, 2020.

[140] J. Liu, L. Wang, and Y. Yu, “Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5256–5266, 2020.

[141] R. Ufa, Y. Malkova, A. Gusev, N. Ruban, and A. Vasilev, “Algorithm for optimal pairing of res and hydrogen energy storage systems,” *International Journal of Hydrogen Energy*, vol. 46, no. 68, pp. 33 659–33 669, 2021.

[142] T. Thurner, K. Fursov, and A. Nefedova, “Early adopters of new transportation technologies: Attitudes of russia’s population towards car sharing, the electric car and autonomous driving,” *Transportation Research Part A: Policy and Practice*, vol. 155, pp. 403–417, 2022.

[143] K. Akimoto, F. Sano, and J. Oda, “Impacts of ride and car-sharing associated with fully autonomous cars on global energy consumptions and carbon dioxide emissions,” *Technological Forecasting and Social Change*, vol. 174, p. 121311, 2022.

[144] D. Olaru, S. Greaves, C. Leighton, B. Smith, and T. Arnold, “Peer-to-peer (p2p) carsharing and driverless vehicles: Attitudes and values of vehicle owners,” *Transportation Research Part A: Policy and Practice*, vol. 151, pp. 180–194, 2021.

[145] K. Mawonde, “Vehicular ad-hoc network based anti-theft model for car theft prevention in south africa,” Ph.D. dissertation, North-West University (South Africa), 2019.

Appendix A

List of Acronyms

Acronyms

In alphabetical order:

AVISPA Automated Validation of Internet Security Protocols and Applications

Dc Decryption

En Encryption

GH Generation of Hash

GS Generation of Signature

KG Elliptic Curve Key Pair Generation

SK Secret Key Generation

U User Association

VS Verification of Signature

ZIPA Zero-Interaction Pairing and Authentication

Appendix B

List of Publications

B.1 International Journal Papers [5]

1. **Ubaid Ur Rehman**, Seong-Bae Park, and Sungyoung Lee. “Secure Health Fog: A Novel Framework for Personalized Recommendations based on Adaptive Model Tuning.”, *IEEE Access* (SCIE, IF: 3.367), Vol. 9, 2021.

2. **Ubaid Ur Rehman**, Dong Jin Chang, Younhea Jung, Usman Akhtar, Muhammad Asif Razzaq, and Sungyoung Lee. “Medical instructed real-time assistant for patient with glaucoma and diabetic conditions.”, *Applied Sciences* (SCIE, IF:2.679), Vol.10, No.7, 2216, 2020.

3. Muhammad Asif Razzaq, Javier Medina Quero , Ian Cleland, Chris Nugent , Usman Akhtar, Hafiz Syed Bilal Ali, **Ubaid Ur Rehman**, and Sungyoung Lee. “uMoDT: An unobtrusive Multi-occupant Detection and Tracking using robust Kalman filter for real-time activity recognition”, *Multimedia Systems* (SCI, IF:1.935), Vol. 26, No.5, pp.553-569, 2020.

4. Taqdir Ali, Jamil Hussain, Muhammad Bilal Amin, Musarrat Hussain, Usman Akhtar, Wajahat Ali Khan, **Ubaid Ur Rehman**, Sungyoung Lee, Byeong Ho Kang, Maqbool Hussain, Muhammad Afzal, Ho-Seong Han, June Young Choi, Hyeong Won Yu, and Arif Jamshed, “The Intelligent Medical Platform: A novel dialogue-based platform for health-care services.”, *IEEE Magazine: Computer* (SCI, IF:3.564), Vol. 53, No.2, pp.35-45, 2020.

5. Usman Akhtar, Muhammad Asif Razzaq, **Ubaid Ur Rehman**, Muhammad Bilal Amin, Wajahat Ali Khan, Eui-Nam Huh, and Sungyoung Lee. “Change-aware scheduling for effectively updating linked open data caches.” , *IEEE Access* (SCIE, IF: 3.367), Vol. 6, pp.65862–65873, 2018.

B.2 Domestic Journal Paper [1]

1. 장동진, **Ubaid Ur Rehman**, 정윤혜, Hafiz Syed Muhammad Bilal, 이승룡, "자연어처리 기반 진화형 임상의사 결정지원시스템: 녹내장 진단 사례연구", *한국통신학회지(정보와 통신)*, Vol.37(9), pp.34-39, 2020.

B.3 International Conference Papers [4]

1. **Ubaid Ur Rehman**, Amir Ali, Hafiz Syed Muhammad Bilal, Muhammad Asif Razzaq, Seong-Bae Park, Sungyoung Lee, "A Novel Mutual Trust Evaluation Method for Identification of Trusted Devices in Smart Environment.", International Conference on Ubiquitous Information Management and Communication. IEEE, 2022.

2. **Ubaid Ur Rehman**, Sungyoung Lee, "TPP: Tradeoff Between Personalization and Privacy.", International Conference on Ubiquitous Information Management and Communication. Springer, Cham, 672-681, 2019.

3. **Ubaid Ur Rehman**, Sungyoung Lee, "Natural Language Voice based Authentication Mechanism for Smartphones.", In Proceedings of the 17th annual international conference on mobile systems, applications, and services, 600-601, 2019.

4. Hafiz Syed Muhammad Bilal, Usman Akhtar, Asim Abbas, Muhammad Asif Razzaq, **Ubaid Ur Rehman**, Jamil Hussain, Sunmoo Kang, Sungyoung Lee, Seong-Bae Park "CbI-M: Context-based Intervention Methodology for Rehabilitation of Persons with NCDs" , *The 15th International Conference on Ubiquitous Information Management and Communication (IMCOM 2021)*, Seoul, Korea, Jan 4-6, 2021.

B.4 Domestic Conference Papers [4]

1. **Ubaid Ur Rehman**, Sungyoung Lee, "A Novel Medication Adherence Framework using Voice-based Emotion Recognition Technique for Person with Dementia.", 한국정보과학회 학술발표논문집, 200-202, 2020.

2. **Ubaid Ur Rehman**, Sungyoung Lee, “Blockchain based Layered Architecture for Virtual Agents.” 한국정보과학회 학술발표논문집, 1191-1193, 2019.

3. **Ubaid Ur Rehman**, Sungyoung Lee, “Blockchain based Healthcare Virtual Agent Architecture.”, 한국정보과학회 학술발표논문집, 1003-1005, 2018.

4. **Ubaid Ur Rehman**, Sungyoung Lee, “Preventing the Data Privacy Issues in Healthcare Environment”, 대한의료정보학회 춘계학술대회에, 2018.

B.5 Domestic Patent [2]

1. 이승룡, **레만 우바이드 유알**, *“음성 이미지 기반 사용자 인증 장치 및 그 방법”*, 등록번호 *: 10-2444003, 2022년09월15일 (특허권자:경희대학교 산학협력단)*

2. 이승룡, **Ubaid Ur Rehman**, 박성배, *“무선 센서 네트워크를 위한 지능형 상황 감지 프로토콜 추천 시스템”, 출원번호: 10-2021-0188377, 2021.12.27 (출원인: 경희대학교 산학협력단)*