Protecting user’s data stored locally on smartwatches using Ascon encryption: A Lightweight cryptography approach.

MSc Research Project
Cyber Security

Noorullah Mohammed Sakhib
Student ID: X21225273

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Noorullah Mohammed Sakhib		
Student ID:	X21225273		
Programme:	MSc in Cybersecurity	**Year:**	2022-2023
Module:	MSc Research Project		
Supervisor:	Niall Heffernan		
Submission Due Date:	14/07/2023		
Project Title:	Protecting user's data stored locally on smartwatches using Ascon encryption: A Lightweight cryptography approach		
Word Count:	6458	**Page Count: 18**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Noorullah Mohammed Sakhib

Date: 14/07/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□

Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

PROTECTING USER DATA STORED LOCALLY ON SMARTWATCHES USING ASCON ENCRYPTION: A LIGHTWEIGHT CRYPTOGRAPHY APPROACH

Noorullah Mohammed Sakhib
X21225273

ABSTRACT

The advent of smart watches has ushered in a new era of wearable technology, significantly transforming the way we interact with digital information. Smartwatches have gained popularity in recent years due to their various features and functionalities, including step counter, calorie tracking, heartrate monitoring, financial services, and communication. However, these appliances possess limited bandwidth and computational capability, relying heavily on smartphones for connectivity. Smartwatches have become popular for their diverse functionalities as these devices can gather and retain a sizable quantity of personal data, including private information about your health, location, and other sensitive details. Additionally, smartwatches are susceptible to security threats, and if the user’s data that has been stored locally on these devices is not properly protected, it can be compromised. Unfortunately, not all manufacturers of affordable wearable technology have gone far enough to safeguard their clients privacy. To solve this problem, it is necessary to employ a lightweight encryption method, such as Ascon, to protect user data stored on smartwatches without straining the hardware's processing power.

Keywords: Ascon, Smartwatch, Android studio, Emulator, Security, User, Data, Encryption, Decryption.

1. INTRODUCTION

1.1 Background

The use of technology has permeated every area of our daily life. Every person uses a smartphone to carry out a variety of tasks every day. This might take the form of data consumption like as viewing multimedia, sending electronic messages, banking, or engaging in other activities including communication, measuring one's fitness, keeping track of their whereabouts, or arranging tasks and meetings. (Centeno *et al.*, 2019a). With the development of technology, handheld electronic devices such as smart phones have become an integral part of our daily lives. Consumers want these devices to be as portable as possible, and in recent years, smart watches have drawn significant attention due to their ability to perform nearly all a mobile phone's functions, if not all of them.

However, as technology has advanced, the risk connected with these devices has also risen. A breach of this information might cause considerable harm, whether it be financial or reputational loss. This is because these wearable devices hold information, that may be quite sensitive to their users (Al-Sharrah, Salman and Ahmad, 2018a). This information might lead to major discoveries and an improvement in health outcomes as shown in Fig.1 It also raises questions regarding the security and privacy of user data. To safeguard user data from potential assaults, security measures are becoming more and more important as these devices are used more often. Exploiting this information can result in identity theft, data manipulation, and other unlawful behaviours. Keeping information security on shared data is a vital issue, thus it is imperative to solve it.

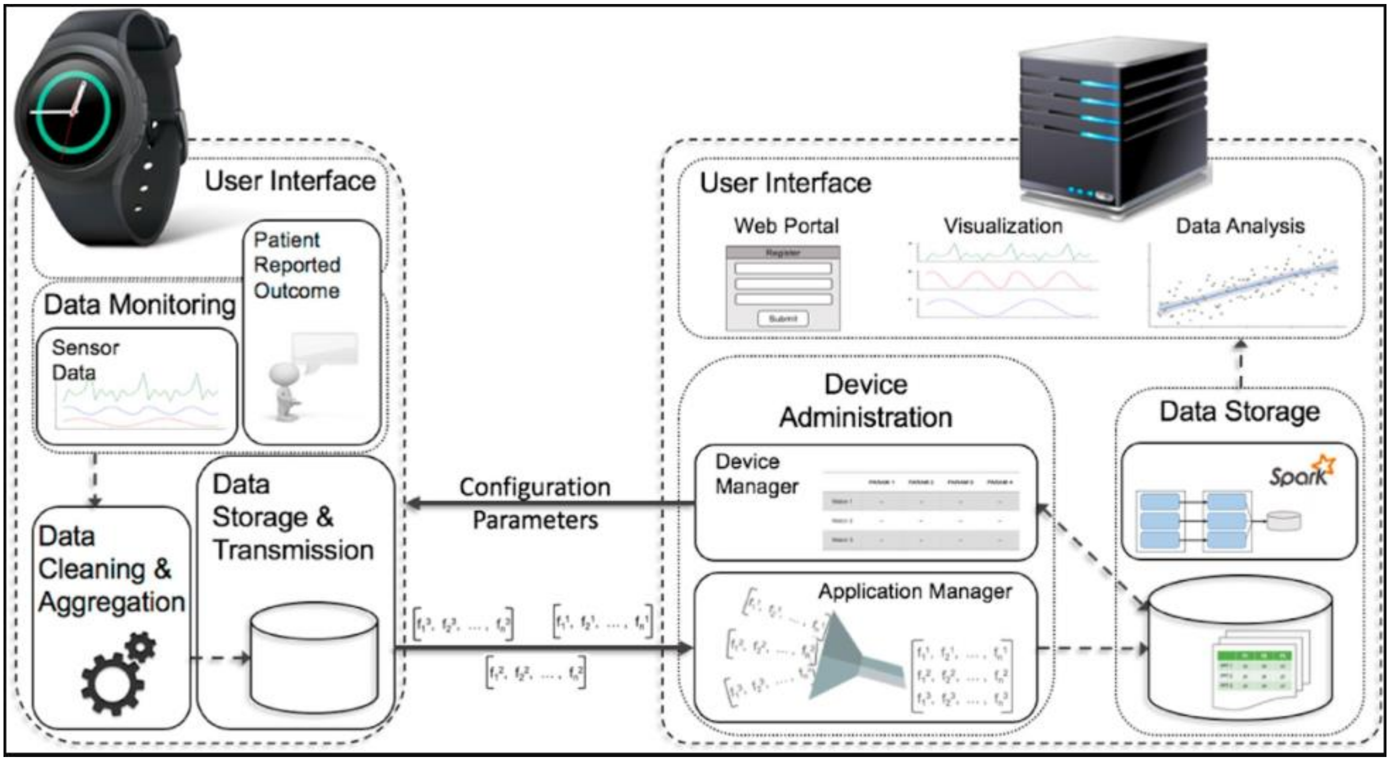


Fig 1: Architecture of Smart watch (Kheirkhahan *et al.*, 2019)

1.2 Motivation

The proliferation of wearable technology has revolutionized the way we interact with and access information. Smart watches have become ubiquitous companions, bridging the gap between traditional timekeeping devices and advanced portable computers. According to (Al-Sharrah, Salman and Ahmad, 2018b) Smart watches have gained its popularity due to its compact size and potential to perform several operations on them such as calling feature, messaging, emailing, calendar dates, gate passes, event tickets, media storage of photos and videos, banking via contactless payment or digital wallets and health informatics such as sleep cycle, blood oxygen level monitoring, calorie monitoring, fitness tracking, footsteps tracker, travel distance and time tracker, sleep cycles, heartbeat, blood pressure, glucose level monitoring, temperature monitoring and health and daily activity tracking as illustrated in Fig 2 It also has emergency assistance features such as “Save our Soul” (SOS) message feature, if the watch detects that the wearer has fallen. In addition, it also has few other features such social media and other notifications by synchronizing with the smartphone applications, location, and tracking features, such as maps, compass, and altimeter. While several devices also provide games, music, photos, and other entertainment options. These devices provide so many features in them, it’s because of the very reason that it has been gaining a rapid acceptance by the consumers.

Fig 2: Capabilities of Smartwatch (Sundaravadivel *et al.*, 2018)

As the usage of smart watches continues to surge, the security and privacy concerns associated with the data they store have become increasingly critical. Thus, some of the key points to consider are:

- **Advantages of wearable devices:** They provide real-time feedback on physical activity and other health-related data, allowing users to self-manage and monitor their progress.
- **Potential for improved health outcomes:** Wearable device data can yield insightful information that can result in more individualized care and improved health outcomes.
- **Privacy and security concerns**: Wearable technology use is growing, which raises questions regarding user data security and privacy. This information needs to be protected against potential assaults and misuse.
- **Exploitation of user data:** Wearable technology's user data can be used for illegal actions including identity theft and data tampering. This emphasizes the significance of data protection and information security.
- **Growing need for security measures**: Strong security measures are becoming increasingly essential as the use of wearable technology grows to protect user privacy and data integrity.

Most of today's smartwatches communicate with the user's mobile phone over Bluetooth Low Energy, leaving users personal sensitive information vulnerable to security attacks. Due to the size and resource constraints in these smart watches, security features have been largely neglected. Given their inherent nature of being constantly connected to smartphones and other devices, these wearables are highly susceptible to unauthorized access, data breaches, and cyber-attacks. As a result, the implementation of robust encryption mechanisms which is light weight and consumes less computational resources is the need of the hour for these devices to be protected.

1.3 Research question

The main intent of this research is to provide an optimistic solution to enhance the security of the smart watch device without compromising on its current computation resources and find a lightweight encryption which would improvise protection of data stored locally on these devices.

- What are the security risks associated with smartwatches? Why is data stored on a smartphone so important?
- How efficiently can a lightweight encryption such as Ascon be used to mitigate the security challenges on a smartwatch and the data stored in them.

1.4 Research Objective

The objective of this research is to find how a lightweight encryption such as ASCON is efficient to secure the data stored on the device. The framework consists of several privacy protection rules and several instruments for implementing those rules into practice. The report emphasizes the significance of user data protection and offers a thorough methodology for doing so. To answer the research question, the study has the following objectives:

- Develop a framework which replicates smart watch environment.
- Use Ascon light weight encryption to perform encryption and decryption of the data.
- Analyse the output to understand how efficient the algorithm is based on CPU, memory, and energy consumption.

2. RELATED WORKS

2.1 Overview of Smartwatch security

As per (Aljabri, Abawajy and Huda, 2023), the growth in IoT devices signifies a substantial expansion of the digital landscape, with an ever-increasing integration and incorporation of smart devices into various aspects of our daily lives. From smart homes and industrial automation to healthcare applications and transportation systems, the proliferation of these interconnected devices is poised to reshape the way we interact with technology and gather data, creating a more interconnected and data-driven world. An anticipated projection by (Ahmad, Laplante and Defranco, 2020) suggests that "by the year 2030, the global count of Internet of Things (IoT) interconnected devices is expected to reach around 500 billion".

Considering the growing popularity of wearable technology, it is essential to address the weaknesses and challenges that develop to ensure the unwavering security and absolute privacy of the data they contain. Smartwatches in particular stand out among these advancements as targets that are open to a variety of possible assaults. (Alshammari and Alshammari, 2022) the process of hacking may reveal the vast amount of data that these gadgets collect and keep. This circumstance emphasizes how important it is to take preventative action to protect the amount of information stored in wearable gadgets. These technologies' vulnerability to attacks only grows as they become increasingly integrated into our daily lives. Determining a multifaceted strategy to address these risks and maintain the integrity of the data they contain is therefore necessary.

It's also critical to recognize that security flaws can occur with these gadgets. If not properly protected, the user data stored locally on these devices can be compromised. Regarding protecting information security and privacy, this poses a growing worry. These gadgets rely largely on mobile devices for connectivity since they have low processing and bandwidth capacities, which creates a critical need. It becomes essential to have strong security systems in place for smart wearable devices to protect user data. Encryption is a well-known and essential tactic for enhancing the security of user data on these wearables (Al-Sharrah, Salman and Ahmad, 2018a). By turning data into a cryptographic code that can only be decoded using a unique key or password, encryption serves as a crucial layer of defence as shown in Fig 3 By using encryption, the information contained in smart wearables is made far more difficult for threat actors to access or steal. This creates a potential barrier that prevents unwanted access to the device's data (Centeno *et al.*, 2019b). Such encryption techniques are crucial for both enhancing data security and preventing any breaches that could compromise the integrity of sensitive user data. Adopting encryption procedures stands out as a proactive solution to safeguard the security and integrity of user data as the wearable technology ecosystem continues to change. As per (Tawalbeh *et al.*, 2020), utilizing robust and reliable algorithms while routinely updating security mechanisms is of the utmost significance. This procedure is necessary to ensure the highest level of security for user data on wearable smart devices. Additionally, it is crucial to fully teach end users of the significance of encryption and proper device security in protecting their information.

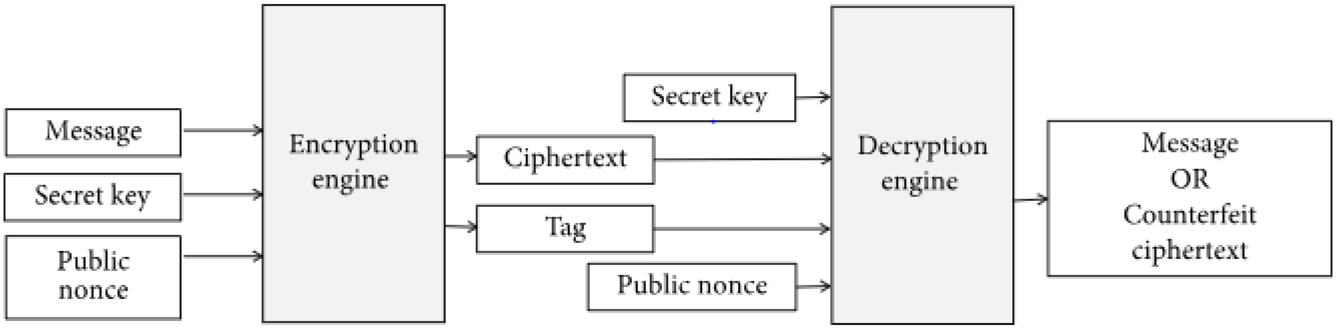


Fig 3 Encryption and Decryption Architecture

Strong and sophisticated algorithms must be incorporated to strengthen the security framework of smart wearables. Regularly reviewing and improving security protocols ensures that any possible weaknesses are quickly fixed, providing a continuously strengthened defence against new threats (Sadkhan and Salman, 2018) (Rofouei *et al.*, 2019). This iterative process considerably enhances user data protection overall and strengthens the reputation of smart wearables as reliable and safe instruments in the current digital environment. An essential part of these efforts is educating end users about the value of encryption and the correct procedures for preserving device security. By providing users with a thorough understanding of encryption's function in data protection, consumers are better equipped to make decisions about how they will use their devices. Users are given the tools they need to actively engage in the protection of their own data when they are informed about best practices, password management, and the need of frequent upgrades. As outlined in the report authored by (Vijayan *et al.*, 2021), wearable technology is still vulnerable to a wide range of possible breaches, including dangers like data theft, illegal access, and intrusions by malicious software. This thorough investigation also identifies a major obstacle in the shape of non-standard security procedures, which presents a huge obstacle to adequately fortification wearable devices against vulnerabilities. The authors propose strict security procedures for wearable technology makers to employ to solve this issue and successfully protect user data from compromise. Another assessment, also conducted by (Vijayan *et al.*, 2021) explores the use of wearable technology in the areas of self-care and healthcare. This investigation highlights the extraordinary data storage capabilities of wearable technology, which can store huge amounts of data, including sensitive and private data. Surprisingly, this study identifies a significant barrier to the use of wearable technology in healthcare as the urgent need for safe data storage and transfer. The consequences might be severe in a hypothetical situation where an attacker acquires access to a user's wristwatch, especially if the sensitive data stored there is insufficiently protected or left unencrypted. The attacker could take advantage of this circumstance to get access to and modify information, possibly planning more complex and harmful assaults.

This emphasizes how urgent it is to address both encryption and strong security measures for use with wearable technology in all contexts. To ensure the security, privacy, and functioning of wearable technology across a range of applications, a multifaceted strategy is essential. This includes data storage and transmission as well as the creation of standardized security standards. Furthermore, an in-depth exploration of wearable technology carried out by (Ometov *et al.*, 2021) gives a thorough review of wearable technology's development across time as well as its most recent developments. The paper mentions some of the features and functionalities of the smart wearable devices. However, wearable devices still lack encryption feature in them, leaving them vulnerable to hacking and other security breaches.

By adding encryption to these wearable devices, my work can help to address this issue and improve security and privacy of user data which is stored locally on these devices.

The relevance of my work lies in addressing the evolving security needs on these devices and making use of encryption techniques to guarantee data privacy and integrity. In addition, selecting a specific encryption technique like Ascon lightweight encryption allows for an in-depth understanding of its implementation and performance on smart wearable devices.

The work is limited to Ascon encryption because Ascon is light weight encryption and the winner of National Institute of Standards and Technology (NIST) lightweight cryptography competition (*Lightweight Cryptography | CSRC*, no date). It covers all the key challenges with reference to memory, power consumption and performance on the devices with resource constraints. Therefore, by using Ascon encryption on smart watches, my work can help to improve the security and privacy of user data stored locally on these devices while minimizing the impact on device performance and battery life. The thorough investigation suggests that the introduction of smart wearables is likely to have an impact on not only people's personal lives but also on the reputation and daily operations of huge enterprises. It's important to note that this assessment raises an important concern and the necessity of developing secure methods for both data transmission and storage which appears to be a crucial obstacle to fully utilizing wearable technologies.

Similarly, a comprehensive evaluation conducted by (Rahmani *et al.*, 2022), on the revolutionary potential of these technological advancements is highlighted by a focus on wearable technology applications in the healthcare industry. The assessment highlights how wearable technology can provide creative answers to the complex problems facing the healthcare industry. The requirement for secure data storage and efficient data transfer does, however, also arise from this investigation. According to the paper, this is still a substantial barrier to properly using wearable technology transformational potential in the healthcare industry. The requirement for secure data storage and efficient data transfer does, however, also arise from this investigation. According to the paper (Kim *et al.*, 2019), this is still a substantial barrier to properly using wearable technology' transformational potential in the healthcare industry.

In summary, these studies show the disruptive and revolutionary potential of wearable technology while also highlighting a persistent issue. This issue relates to the development of trustworthy and safe frameworks for data transmission and storage, which is essential for assuring the moral and effective application of wearable technology in a variety of contexts, including those of the individual, the workplace, and healthcare. Addressing this issue head-on is crucial as wearable technology continues to influence our lives.

2.2 Comparative study on available cryptographic algorithms

Traditional cryptographic algorithms, such as AES and SHA, show a considerable disadvantage in the context of IoT devices due to their inclination to need high levels of processing power and battery life (Hung and Hsu, 2018) (Dobraunig *et al.*, 2021a). They are unfit for incorporation into the IoT devices' resource-constrained environment because of this constraint. The development of lightweight cryptography approaches is a reaction to this problem, seeking to reconcile resource efficiency with strong security. These methods concentrate on coming up with secure solutions that use the least amount of memory, processing, and power.

A core concept of lightweight cryptography is the quest of energy efficiency. This drive is evidenced by research conducted by (P. *et al.*, 2021a), which emphasizes the crucial role energy plays in this setting and places the importance of energy consumption on par with that of power dissipation. Lightweight cryptography methods make use of bilateral key concepts and other clever techniques to optimize energy use, significantly reducing the energy consumption of end devices.

It's important to note that methods that skilfully handle many of the problems often associated with conventional cryptography are combined with lightweight encryption algorithms. These difficulties include issues with memory capacity and energy use. The energy and memory limits are eased by using lightweight encryption algorithms, representing a step towards resolving these ongoing challenges. As a result, the use of energy-efficient lightweight encryption technologies heralds in a new age in sharp contrast to the power-hungry nature of traditional encryption methods. This change not only makes it possible to secure IoT devices, but it also exemplifies how cryptography has advanced via innovation in the context of technology with limited resources.

(Hung and Hsu, 2018) conducted another study in 2018 that digs into the world of IoT devices by examining the effectiveness of a device that has Advanced Encryption Standard (AES) encryption built in. The main goals of this study included a comparison of various key lengths and modes and an assessment of the effects on hardware resource usage. The main objective of this investigation was to strengthen security in embedded systems using AES. An analysis of the Advanced Encryption Standard's (AES) performance dynamics regarding both power use and computing demands served as the study's focus. The investigation's key result is that while being widely used in the IoT industry, AES has a high energy consumption cost. This realization emphasizes the significant amount of power allocated to AES-based IoT device encryption procedures. The study emphasizes an important fact that although AES is a commonly used encryption standard for IoT devices, it is not without drawbacks. Although it unquestionably improves security, there is a corresponding rise in power usage. To achieve a balance between protecting sensitive data and improving the operational sustainability of IoT devices, researchers and practitioners must traverse the complicated interplay between security needs and energy efficiency.

A specific area of cryptography called lightweight encryption purposefully tries to provide strong security while reducing resource requirements. The importance of lightweight encryption approaches has significantly increased considering the growing popularity of smart wearables, which are distinguished by their constrained processing power. These methods act as a crucial barrier, protecting critical information from the grasp of nefarious intruders (Kim and Kim, 2018). The capacity of lightweight cryptographic algorithms to function with low memory use, demand constrained computing resources, and demonstrate decreased energy consumption stands out among its distinguishing characteristics.

(Kim and Kim, 2018) diligently undertook a thorough evaluation of the encryption performance of lightweight cryptography on open and commercial hardware platforms in 2018, demonstrating the method's versatility and promise. The uniqueness of lightweight techniques, which distinguish them from standard approaches, resides in the adjustments they use throughout encryption and decryption procedures. These modifications essentially allow lightweight cryptography to thrive even on constrained systems with limited resources. This includes gadgets like smartwatches and Internet of Things (IoT) gadgets. By using lightweight cryptographic fundamentals, it is possible to connect a greater number of devices, even those with few resources. In addition to promoting connection, this dynamic also encourages creativity among low-resource devices, breaking down boundaries and opening the door for entirely new possibilities for data security. A fascinating confluence is formed by the development of sophisticated lightweight encryption algorithms and the rigorous analysis of how well they operate in low-resource settings. This junction offers a rich environment for research, opening the path for better data security while encouraging the smooth operation of devices with limited resources. In essence, the development of lightweight encryption reflects the technological environment, helping to create a future in which security and usability coexist together.

Ascon stands as a notable inclusion in the conclusive selection of cryptographic algorithms stemming from the CAESAR and NIST Lightweight Cryptography competitions, as documented by (Farahmand *et al.*, 2018). The work of (Dobraunig *et al.*, 2021a) also sheds light on Ascon's significance as a lightweight authenticated encryption technique, a solution that masterfully blends reliability and confidentiality within a given environment. Notably, Ascon has been skilfully designed to excel in efficiency while managing succinct communications in addition to thwarting certain implementation mistakes and assaults. The comprehensive examination of authenticated encryption schemes, categorized and assessed through a systematic literature review, illuminates the pivotal role that Ascon occupies within this domain. As detailed in the research by (Madushan, Salam and Alawatugoda, 2022), Ascon emerges as a prime contender for lightweight authenticated encryption. This sentiment is echoed in an IEEE Conference Publication from 2023 that highlights Ascon's evaluation, particularly in the context of AI-enabled Internet of Things (IoT) devices.

According to (Dobraunig *et al.*, 2021a) "The Ascon suite's design is based on the well-known Ascon-128 and Ascon-128a authenticated encryption paradigms. Newer structures like Ascon-80pq, Ascon-Hash, and Ascon-Xof have also been added to the suite, adding an extra degree of security. Ascon presents itself as a leader in hardware-oriented optimization and operates on a 320-bit permutation structure."

Ascon's dominance in credible contests, support from thorough literature evaluations, and tolerance of changing security paradigms highlight its relevance as the cryptographic field continues to change. Ascon's skill in fusing efficiency, security, and innovation confirms its position as a leading light in the field of lightweight authenticated communications in an age where these three factors are converging (P. *et al.*, 2021a). In accordance with the research conducted by (Dobraunig *et al.*, 2021a), The authors thoroughly assess Ascon v1.2 security while also putting it through a rigorous comparison with several competing cipher suites. Collectively, their results support Ascon v1.2 qualities as a cipher suite that skilfully strikes a balance between security and effectiveness. Their resounding conclusion is that Ascon v1.2 emerges as a lightweight yet reliable cryptographic solution, making it exceptionally ideal for deployment in settings with naturally constrained resources. Given these striking results, it makes sense to use this specific lightweight encryption technique as the cornerstone of our analytical efforts, which are primarily focused on the simulation of a wristwatch.

By deciding to base our research on Ascon v1.2, we make sure that our efforts are supported by a cryptographic framework that best complies with the limitations imposed by resource-limited circumstances. This is especially relevant when considering smartwatch emulation, where the interaction between security and resource efficiency is crucial. The results from (Dobraunig *et al.*, 2021a) reaffirm our choice, casting Ascon v1.2 as a beacon of suitability in safeguarding data within environments where resources play a vital role. As a result, this study ensures the importance that compact yet secure cipher suites, like Ascon v1.2, bring to the forefront in the constantly changing field of cryptography. By utilizing its capabilities for our research, that can derive insights that represent the delicate balance between security, effectiveness, and limited resources—a balance that characterizes the benefits and difficulties of modern digital technology.

3. RESEARCH METHODOLOGY

The idea of "lightweight encryption" stands out as a sign of hope since it provides a strong way to protect the data stored in smartwatches from possible attacks while also reducing any negative impacts on the device's processing capacity. The Ascon lightweight encryption techniques stand out in this environment as a model for this quest. This algorithm has been carefully designed with the goal of striking a balance between operational efficiency and security. As a result, they are especially well-suited for deployment in situations with limited resources (Dobraunig *et al.*, 2021b). This covers the world of Internet of Things (IoT) devices, where it is crucial to optimize resource utilization.

The fundamental purpose of lightweight encryption is to safeguard sensitive data effectively without placing an unnecessary burden on the host device's CPU or memory. Data may be successfully protected against illegal access, interception, and modification by incorporating these encryption techniques into wearable design smoothly. This tactical approach guarantees that the device will continue to operate with agility and efficiency, free from the restrictions that frequently go along with standard encryption solutions. Particularly the Ascon lightweight encryption algorithms personify the implementation of security with effectiveness. They provide a crucial answer for situations where constraints on computing resources are crucial since they were specifically created to manage the difficult balance between comprehensive data security and resource conservation. This algorithm offers an elegant solution in situations where comparable problems exist, such as the IoT environment where devices must operate without interruption despite limited resources. The concept of lightweight encryption stands as a beacon of innovation in a time when data-driven technologies are becoming more and more ingrained in the fabric of our everyday lives. It presents a harmonic strategy that enhances the capabilities of devices while enhancing their resistance against developing threats. It smoothly combines the requirement of data security with the practical reality of resource limitations. The choice of encryption algorithms is validated and verified in large part by the incorporation of smartwatch simulators into our analytical framework. These simulators are essential tools that allow for a thorough evaluation of the encryption schemes, assuring their reliable operation. The importance of this project is shown by the vital part that encryption plays in our study; protecting sensitive data continues to be our top priority.

It is impossible to stress the importance of encryption testing in the context of our investigation. It is crucial to ensure that the chosen encryption approaches not only achieve their intended goals but also display the power and resilience necessary to fend off possible attacks as we navigate the complex environment of data security. The key to this validation procedure is the use of smartwatch simulators, which act as a controlled setting in which the effectiveness of encryption can be constantly evaluated.

The numerous benefits that smartwatch simulators provide increase the accuracy and completeness of our encryption testing. One of these benefits is the simulator's ability to give a comprehensive overview of the encryption strategy being used. This transparency enables us to explore the complex mechanisms underneath the encryption, providing insights into how data is changed and safeguarded. Additionally, these simulators give us the priceless ability to keep an eye on how resources are being allocated during the encryption process. Our assessments are informed by this detailed knowledge of resource usage, which also aids in the optimization of the encryption methods we have selected. In conclusion, the pursuit of lightweight encryption signifies a pivotal stride towards mitigating risks while upholding the operational efficiency of these remarkably portable wearable devices. This proactive approach underscores the commitment to both security and functionality, ensuring that user data remains shielded without compromising the device's overall performance (P. *et al.*, 2021b).

In summary, smartwatch simulators serve as a planned and strategic method for us to carefully assess the effectiveness and security of our encryption techniques. By making use of their strengths, we make certain that the encryption methods we use have the power needed to protect sensitive data while working well with the constrained computing resources present in smartwatch contexts. Our ability to make educated judgments is facilitated by this iterative testing and validation process, which also ensures that our analyses are strong and protected against any weaknesses. For this research we have used Android studio to perform our research and analysis on smartwatches which is our primary target. The analysis of this encryption is also performed on an android emulator to avoid ambiguity, since some of the smartwatches can be operated through a smartphone to store and retrieve the data. In addition, the android emulator is also used to understand how efficiently this encryption will perform on an android device. We have found the code for Ascon encryption from "https://github.com/ascon" which we have utilized in our code to perform encryption and decryption of the data. By embracing lightweight encryption techniques, the potential perils to user data integrity are effectively minimized. This strategic manoeuvre allows for the preservation of the device's operational agility while maintaining a formidable defence against security breaches. The incorporation of such encryption methods speaks to the ingenuity required to address the resource constraints that are inherent to these compact wearable technologies.

The proposition revolves around the adoption of lightweight encryption methodologies. These techniques offer a way to establish robust security measures while simultaneously curtailing the computational and energy expenses associated with encryption. This alignment of security and efficiency stands as a viable response to the challenge at hand. Nonetheless, these intelligent timepieces often grapple with limitations in resources, particularly when it comes to their processing capabilities and memory capacity. To safeguard the sensitive user data that resides within these smart watches, a solution presents itself in the form of a streamlined encryption approach. This approach is tailored to ensure that it doesn't excessively drain the device's already restricted resources.

4. IMPLEMENTATION AND DESIGN

4.1 Implementation process

Leveraging the Ascon encryption algorithm, renowned for its lightweight and high-performance characteristics, ensures robust protection of sensitive information on smartwatches. The development process within Android Studio allows for seamless integration of the encryption functionality into the smartwatch emulator environment. The design emphasizes efficiency, low resource consumption, and real-time encryption to cater to the limited hardware capabilities of smartwatches. When implementing smartwatch encryption using Android Studio, there are several design considerations to keep in mind to ensure the security and usability of the application. Here are some of the key design considerations:

- Ensure that the dataset in used shows a distinct result before and after implementation.
- Ensuring that no other application is consuming resources during the process which could tamper the results.
- To test the application on a variety of dataset to ensure that it works correctly and that the encryption and decryption functions are secure and the results as appropriate.
- Use pre-built or supported tools which illustrates the results throughout its compilation process.
- Ensure that appropriate sanity checks have been done before running the code to ensure a smooth flow of the experiment.

The choice of using the Ascon encryption approach in my research is backed by several compelling reasons, particularly in comparison to other techniques commonly used for smart devices.
Ascon was selected based on its distinguished recognition as the winner of the National Institute of Standards and Technology (NIST) lightweight cryptography competition (Lightweight Cryptography | CSRC, 2017). One of the key advantages of Ascon lies in its lightweight design, tailored to the resource constraints of small devices like smart watches. This design ensures that the encryption process consumes minimal computational resources and power, making it well-suited for small devices with limited capabilities. The flexibility offered by Ascon's code implementation is another compelling factor. Its adaptability to different platforms and programming languages facilitates seamless integration into the smart watch's software ecosystem, making it feasible to implement without any major challenges. In contrast to the research carried out, which revealed a lack of encryption on smart devices since these devices have less resources and computational power. However, as the technology has evolved and the functionalities of these devices have increased with the increase in its resources as well as computational power, it would be the need of the hour to enhance security on the data captured and stored on these devices.

4.2 Design Specification

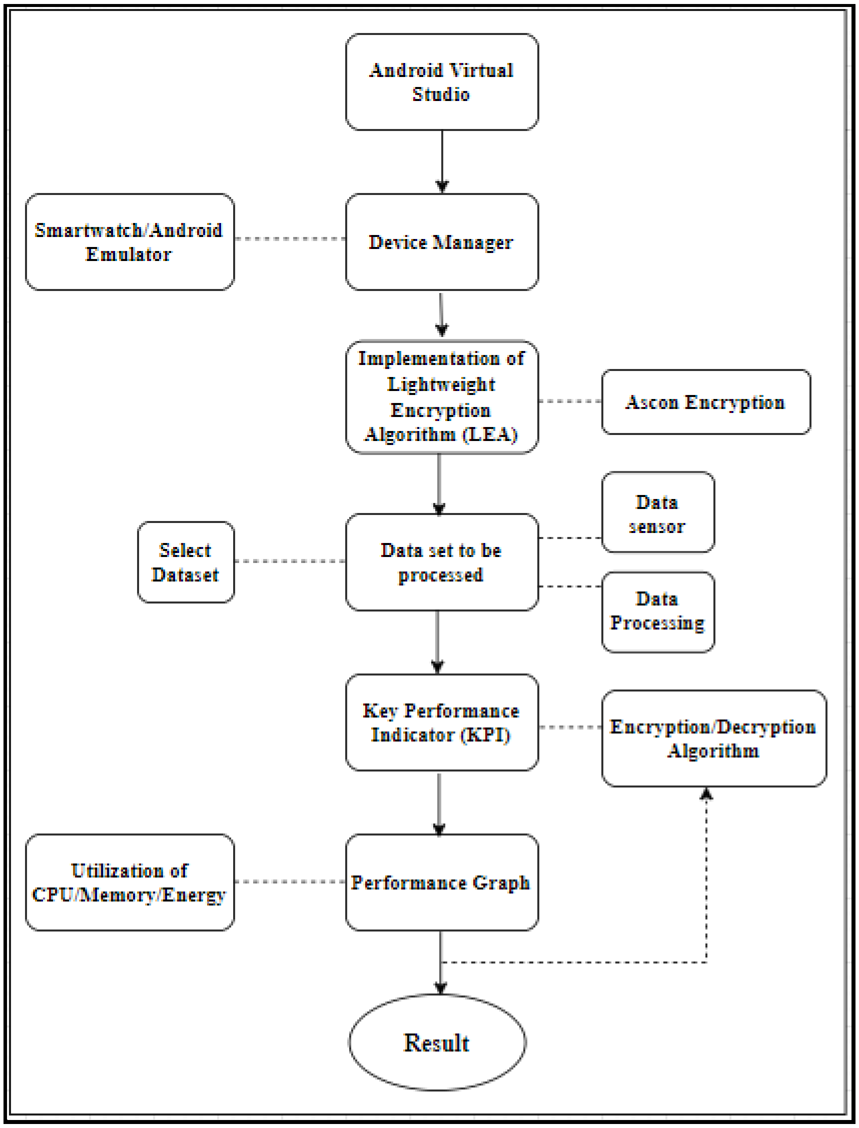

Android Virtual Studio
Device Manager
Smartwatch/Android Emulator
Implementation of Lightweight Encryption Algorithm (LEA)
Ascon Encryption
Select Dataset
Data set to be processed
Data sensor
Data Processing
Key Performance Indicator (KPI)
Encryption/Decryption Algorithm
Utilization of CPU/Memory/Energy
Performance Graph
Result

Fig 4: Flow Diagram of Ascon Light weight encryption on Android Studio

The Fig 4 illustrates the Flow Diagram of the Ascon Lightweight encryption that is implemented to perform the analysis of the dataset on Android studio. The dataset is selected and loaded into the emulator by selecting the device from device manager on android studio and the selected data is processed accordingly. An emulator is initiated via device manager which would run the encryption algorithm. The emulator screen on focus consists of two options i.e., encryption and decryption which when clicked performs the following operation. A key performance indicator which in this case is the logcat and performance graph for the utilization of CPU, Memory and Energy consumed is displayed through the profiler tool. Logcat and profiler are the built-in feature set of Android studio which has been utilized for this analysis. The experiment is performed several times and on several different datasets to understand the efficiency of the algorithm used and if it’s a feasible option to be implemented on a physical device. The experiment has been performed on a controlled environment of Android studio under lab conditions to understand and evaluate the consumption of resources by the emulator. The device performance and utilisation of resources before carrying out the experiment has also been noted to ensure that the results obtained are as expected. The Table 1 illustrates the configuration of the system and the Table 2 Illustrated the configuration lab under which the analyses have been performed.

Table 1: System Configuration

Host System configuration	
Operating System type	**Windows 10 (64-bit)**
Memory	**16 GB RAM**
Processor	**Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz**
GPU	**NVIDIA GeForce 840M (2 GB DDR3 dedicated)**

Table 2: Lab Configuration

Lab Configuration	
Android Studio version	**Android Studio Flamingo 2022.2.1 Patch 2** **https://androidstudio.googleblog.com/2023/05/android-studio-flamingo-patch-2-now.html**
Programming languages	**Kotlin and Java**

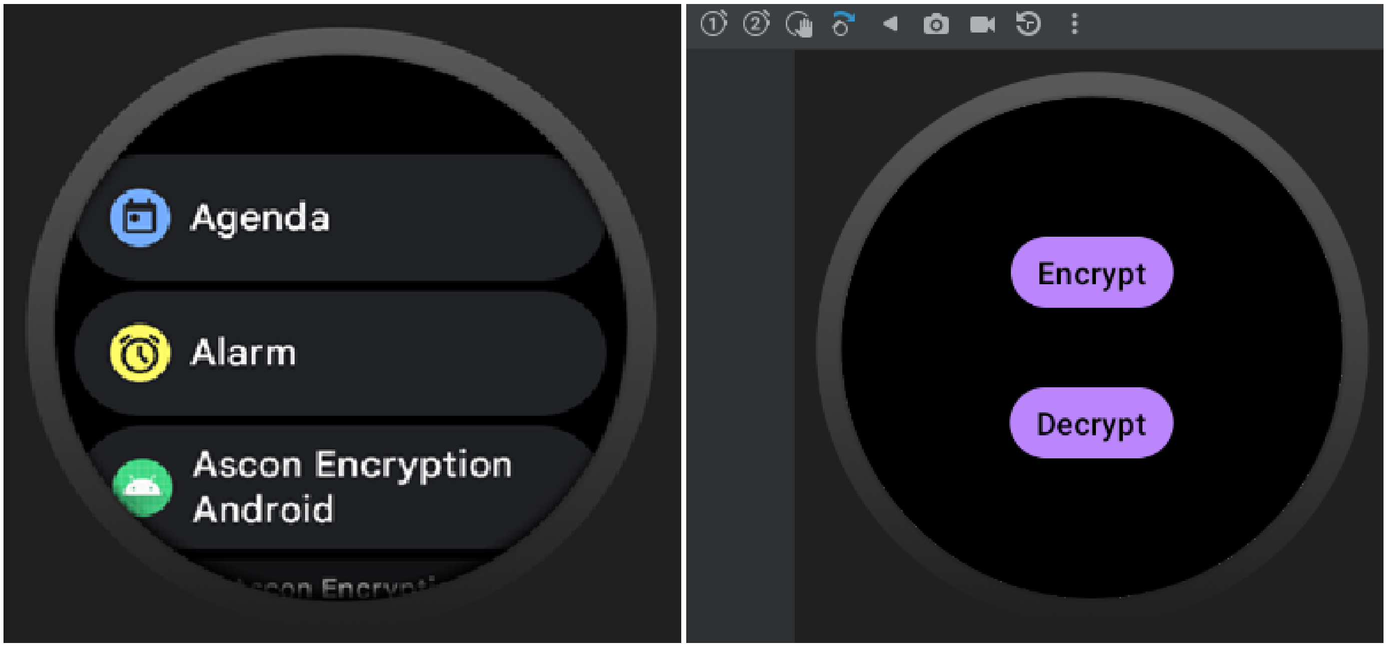


Fig 5: Smartwatch emulator

4.3 Design process

In this research, we have used Ascon 128-bit encryption to perform encryption and decryption of the data. The key point in focus was to ensure that the algorithm is running efficiently on the device and utilizing minimum computational resources and providing faster result. The required result was obtained in a short interval and as expected. The Fig 5 illustrates the design that has been created to perform the encryption and decryption of the selected dataset in a smartwatch emulator using Ascon encryption algorithm which can be selected by clicking on the icon “Ascon Encryption Android” from the smartwatch emulator under device manager. Once clicked, the screen shows the next display which has option to perform encryption and decryption. The dataset is loaded into the android studio for smartwatch emulator and once the “Encrypt” button is pressed, the dataset being encrypted could be analysed through the logcat feature of the android studio application which displays the data being encrypted along with the time taken to perform the operation. The similar operation has been performed to decrypt the data by clicking on the "Decrypt" button present on the face of the smartwatch emulator. A similar approach has also been carried out for the smartphone emulator which can be seen in the Fig 6.

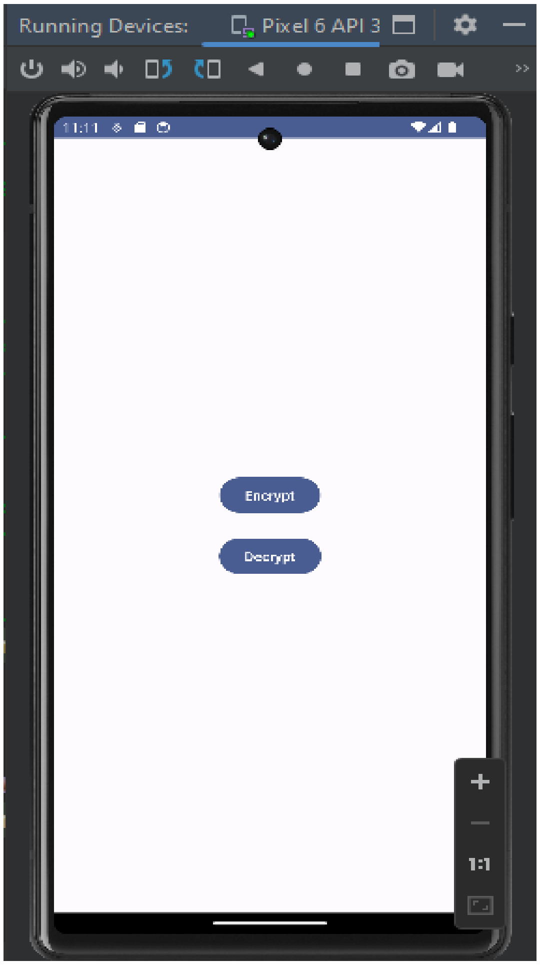
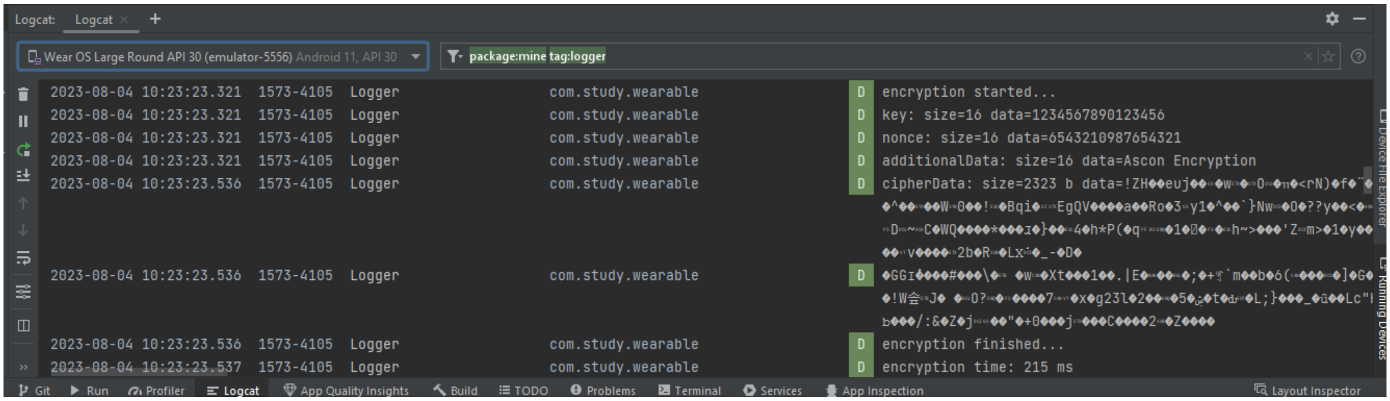


Fig 6: Android emulator

5. EVALUATION AND ANALYSIS

The Fig 7. shows the time duration taken to perform encryption and decryption on the sample data. The output result of data being encrypted can be observed under the logcat feature tab of the android studio. The amount of time taken, the memory utilized, and the energy consumed along with CPU utilization during the encryption and decryption interval can be analysed through the profiler tab. From the sample data file taken and the analysis performed, we can see that the times taken to encrypt and decrypt the data is few milliseconds for a file size comprising of around 2 MB. The CPU, memory and energy consumption has also been significantly low throughout multiple runs that has been performed on several datasets. We have tested the code on .bat, .txt, .doc, .docx, and .zip file types ranging from few hundred KBs and up to 5 MB which comprises of the files that could be used in an actual device.

The experiment has been initially performed on a smartwatch emulator by encrypting the dataset as shown in Fig 7 and the performance of this sample dataset can be seen in Fig 7, Fig 8 and Fig 9 which illustrates the amount of CPU, memory and energy consumed during the experiment being carried out. A similar observation has also been taken into consideration while performing the decryption of the same dataset which can be seen in Fig 10 It can also be observed from Fig 11 that the amount of time taken for decryption is comparatively shorter than the encryption time.


Logcat: Logcat
Wear OS Large Round API 30 (emulator-5556) Android 11, API 30
package:mine tag:logger
Git Run Profiler Logcat App Quality Insights Build TODO Problems Terminal Services App Inspection Layout Inspector
Device File Explorer
Running Devices

```
2023-08-04 10:23:23.321  1573-4105  Logger      com.study.wearable   D  encryption started...
2023-08-04 10:23:23.321  1573-4105  Logger      com.study.wearable   D  key: size=16 data=1234567890123456
2023-08-04 10:23:23.321  1573-4105  Logger      com.study.wearable   D  nonce: size=16 data=6543210987654321
2023-08-04 10:23:23.321  1573-4105  Logger      com.study.wearable   D  additionalData: size=16 data=Ascon Encryption
2023-08-04 10:23:23.536  1573-4105  Logger      com.study.wearable   D  cipherData: size=2323 b data=!ZH��euj���W��O��п�<rN)�f�¨�
                                                                        �^���W0��!�Bqi�EgQV����a��Ro�3y1�^��`}Nw�0�??y��<�
                                                                        D~C�WQ����*���ɪ�}��4�h*P(�q�1����h~>���'Zm>�1�y��
                                                                        ��v����2b�R�Lx�_-�D�
2023-08-04 10:23:23.536  1573-4105  Logger      com.study.wearable   D  �GGɪ����#���\� �w�Xt���1��.|E����;�+`m��b�6(����]�G�
                                                                        �!W슾J� �0?�����7�x�g23l�2���5��t��L;}���_�û��Lc"
                                                                        ь���/:&�Z�j��"�+0���j���C����2�Z����
2023-08-04 10:23:23.536  1573-4105  Logger      com.study.wearable   D  encryption finished...
2023-08-04 10:23:23.537  1573-4105  Logger      com.study.wearable   D  encryption time: 215 ms
```

Fig 7: Logcat output result through Android emulator for data encryption

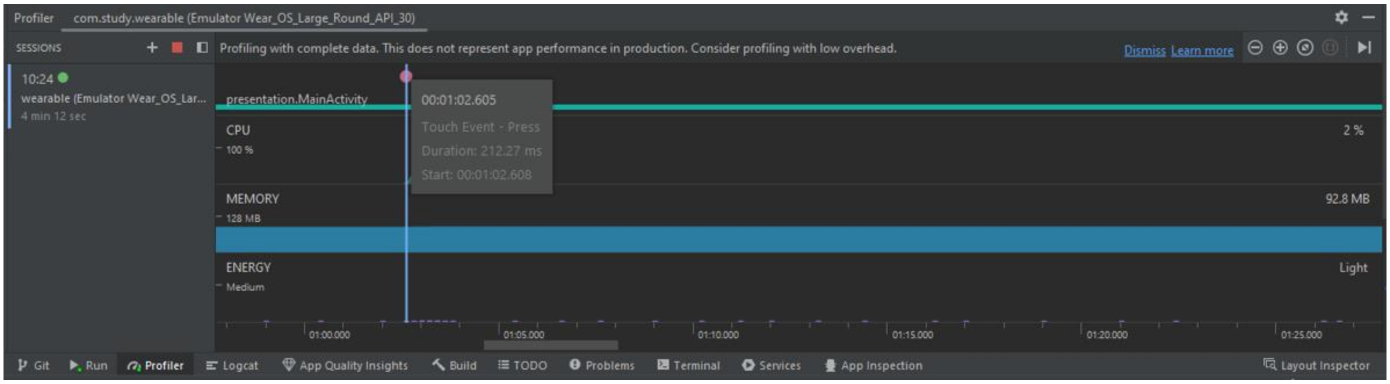

Profiler
com.study.wearable (Emulator Wear_OS_Large_Round_API_30)
SESSIONS
Profiling with complete data. This does not represent app performance in production. Consider profiling with low overhead.
Dismiss
Learn more
10:24
wearable (Emulator Wear_OS_Lar...
4 min 12 sec
presentation.MainActivity
00:01:02.605
Touch Event - Press
Duration: 212.27 ms
Start: 00:01:02.608
CPU
100 %
2 %
MEMORY
128 MB
92.8 MB
ENERGY
Medium
Light
01:00.000
01:05.000
01:10.000
01:15.000
01:20.000
01:25.000
Git Run Profiler Logcat App Quality Insights Build TODO Problems Terminal Services App Inspection Layout Inspector

Fig 8: Performance analysis of Smartwatch emulator for data encryption

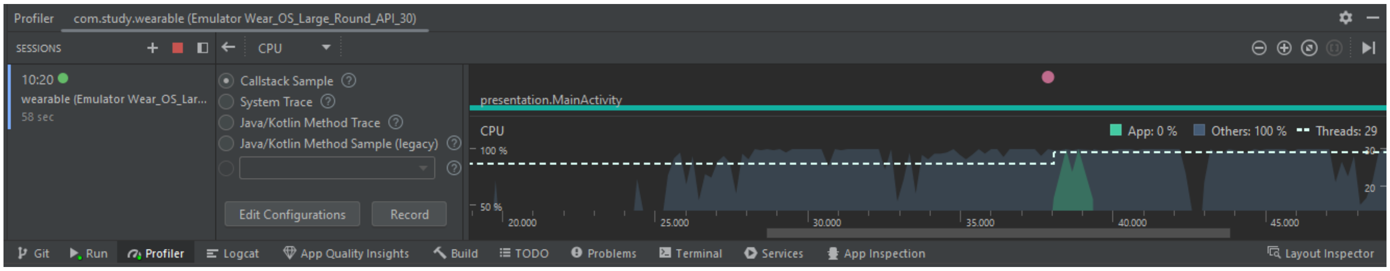
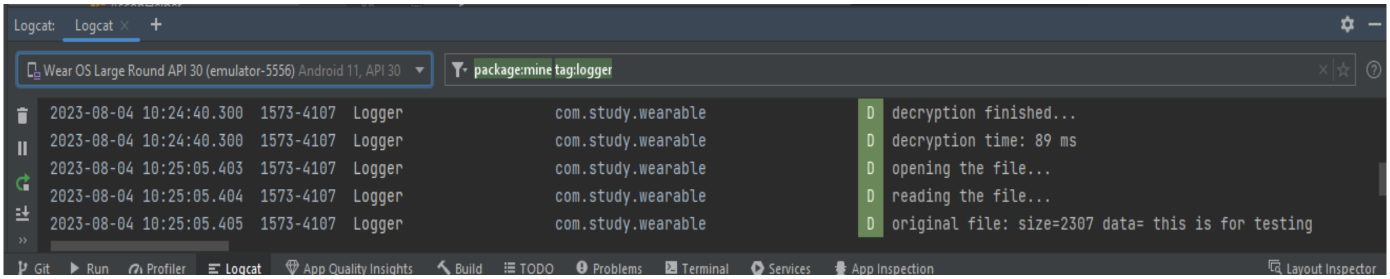
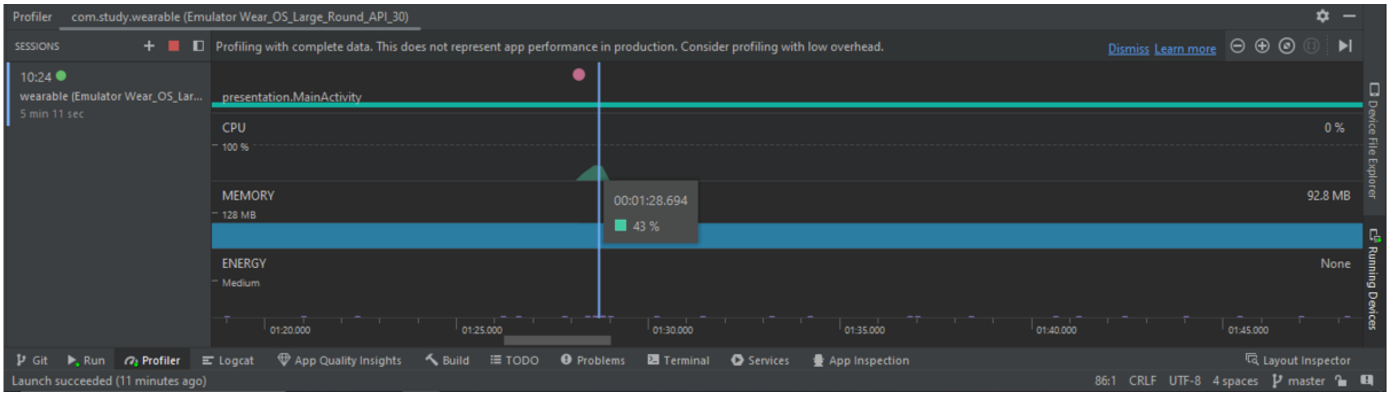

Profiler
com.study.wearable (Emulator Wear_OS_Large_Round_API_30)
SESSIONS
CPU
10:20
wearable (Emulator Wear_OS_Lar...
58 sec
○ Callstack Sample
○ System Trace
○ Java/Kotlin Method Trace
○ Java/Kotlin Method Sample (legacy)
Edit Configurations
Record
presentation.MainActivity
CPU
100 %
50 %
App: 0 %
Others: 100 %
Threads: 29
20
20.000
25.000
30.000
35.000
40.000
45.000
Git Run Profiler Logcat App Quality Insights Build TODO Problems Terminal Services App Inspection Layout Inspector

Fig 9: CPU consumption graph for smartwatch emulator


Logcat: Logcat
Wear OS Large Round API 30 (emulator-5556) Android 11, API 30
package:mine tag:logger
Git Run Profiler Logcat App Quality Insights Build TODO Problems Terminal Services App Inspection Layout Inspector

```
2023-08-04 10:24:40.300  1573-4107  Logger      com.study.wearable   D  decryption finished...
2023-08-04 10:24:40.300  1573-4107  Logger      com.study.wearable   D  decryption time: 89 ms
2023-08-04 10:25:05.403  1573-4107  Logger      com.study.wearable   D  opening the file...
2023-08-04 10:25:05.404  1573-4107  Logger      com.study.wearable   D  reading the file...
2023-08-04 10:25:05.405  1573-4107  Logger      com.study.wearable   D  original file: size=2307 data= this is for testing
```

Fig 10: Logcat output result through Android smartwatch emulator for data decryption

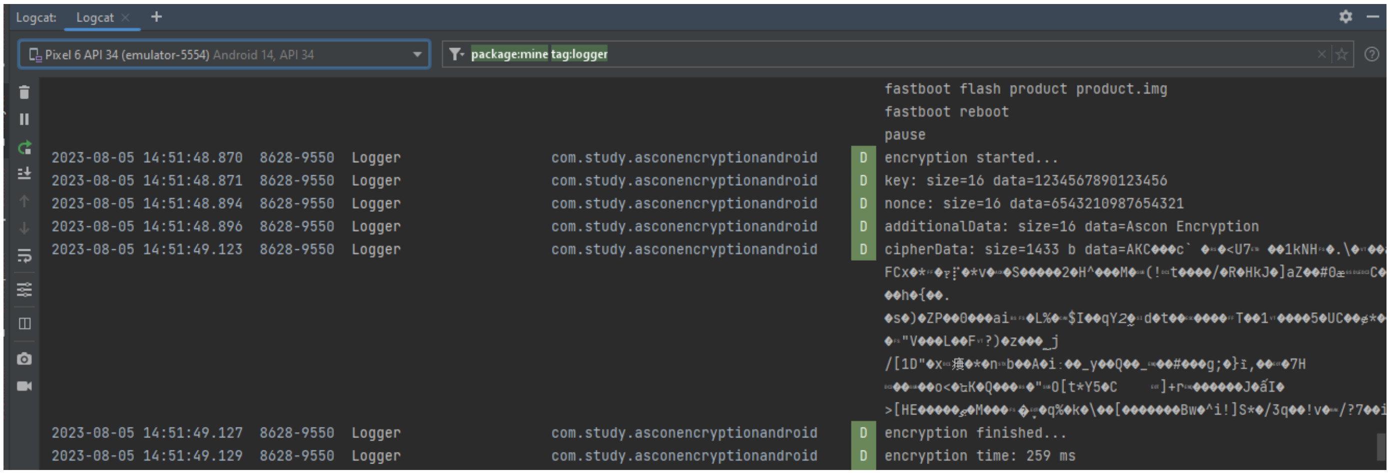


Profiling with complete data. This does not represent app performance in production. Consider profiling with low overhead.

Launch succeeded (11 minutes ago)

Fig 11: Performance analysis of Smartwatch emulator for data decryption

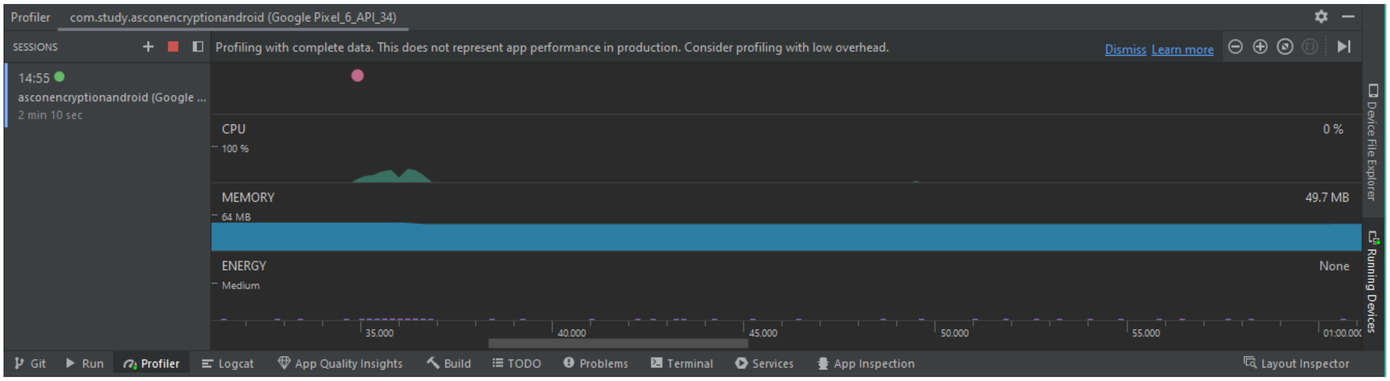
The experiment has also been performed on smartphone emulator to perform a comparative analysis on how effectively the application will perform when a different device is used and as per Fig 12, Fig 13 Fig 14, and Fig 15 it can be clearly observed that the there is a similar performed measures obtained from the device as well. This ensure that the application in consideration is performing as per the requirement without a major change in its efficient or performance.



```
package:mine tag:logger
```

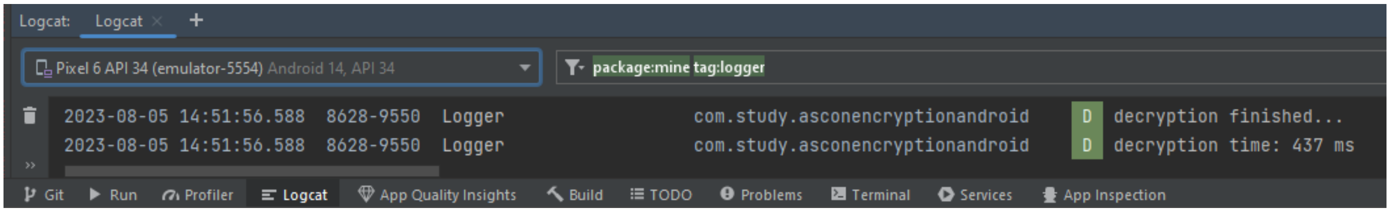
```
                                                                                        fastboot flash product product.img
                                                                                        fastboot reboot
                                                                                        pause
2023-08-05 14:51:48.870  8628-9550  Logger              com.study.asconencryptionandroid  D  encryption started...
2023-08-05 14:51:48.871  8628-9550  Logger              com.study.asconencryptionandroid  D  key: size=16 data=1234567890123456
2023-08-05 14:51:48.894  8628-9550  Logger              com.study.asconencryptionandroid  D  nonce: size=16 data=6543210987654321
2023-08-05 14:51:48.896  8628-9550  Logger              com.study.asconencryptionandroid  D  additionalData: size=16 data=Ascon Encryption
2023-08-05 14:51:49.123  8628-9550  Logger              com.study.asconencryptionandroid  D  cipherData: size=1433 b data=AKC���c` ��<U7 ��1kNH�.\���
                                                                                        FCx�*�ɣ⁞�*v��S�����2�H^���M�(!t����/�R�HkJ�]aZ��#0æC�
                                                                                        ��h�{��.
                                                                                        �s�)�ZP��0���ai�L%�$I��qY2ǫd�t������T��1����5�UC��ȼ*�
                                                                                        �"V���L��F?)�z���_j
                                                                                        /[1D"�x瘐�*�nb��A�i:��_y��Q��_��#���g;�}ĩ,���7H
                                                                                        ����o<�ⱢK�Q����"O[t*Y5�C    ]+r������J�ấI�
                                                                                        >[HE�����ȩ�M����̣�q%�k�\��[�������Bw�^i!]S*�/3q��!v�/?7��i
2023-08-05 14:51:49.127  8628-9550  Logger              com.study.asconencryptionandroid  D  encryption finished...
2023-08-05 14:51:49.129  8628-9550  Logger              com.study.asconencryptionandroid  D  encryption time: 259 ms
```

Fig 12: Logcat output result through Android smartphone emulator for data decryption



Profiling with complete data. This does not represent app performance in production. Consider profiling with low overhead.

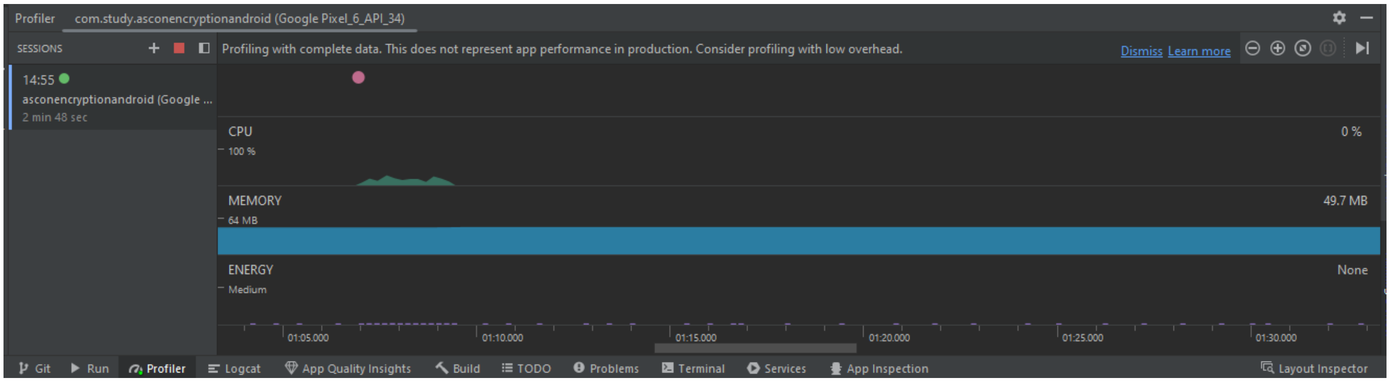
Fig 13: Performance analysis of smartphone emulator for data encryption



package:mine tag:logger

```
2023-08-05 14:51:56.588  8628-9550  Logger        com.study.asconencryptionandroid     D  decryption finished...
2023-08-05 14:51:56.588  8628-9550  Logger        com.study.asconencryptionandroid     D  decryption time: 437 ms
```

Fig 14: Logcat output result through Android smartphone emulator for data decryption



Profiling with complete data. This does not represent app performance in production. Consider profiling with low overhead.

Fig 15: Performance analysis of smartphone emulator for data decryption

6. CONCLUSION AND FUTURE WORKS

Smartwatches have become prevalent in the last few years and can perform almost everything if not all that a mobile phone can perform, which makes it an alternative in the upcoming future for smartphones. However, these devices are susceptible to security risks, and user data that is locally stored on them may be compromised if adequate security measures are not taken. Ascon encryption is a lightweight cryptographic method. Using Ascon encryption, user data saved on smartwatches may be protected without straining the device's computing capabilities. Data security on smart devices may be assured using Ascon, which NIST has chosen as the global standard for lightweight cryptography, making it a reliable choice for this research.

The performance results obtained from our experiment ensure that the experiment was successful in obtaining the desired results without causing an overhead to the resources of the smartwatch device. The measurements and data we've collected from the dataset has confirmed that our goals were accomplished while making the best possible use of the smartwatch's operational and computing capabilities.

The usefulness of Ascon encryption in safeguarding user data on smartwatches and other wearable devices may be investigated further using various types of datasets and environment. The future work could also include increasing security such as adding multifactor authentication and sanity checks on these devices for enhance security.

REFERENCES

1. Ahmad, N., Laplante, P. and Defranco, J.F. (2020) ‘Life, IoT, and the Pursuit of Happiness’, *IT Professional*, 22(6), pp. 4–7. Available at: https://doi.org/10.1109/MITP.2019.2949944.
2. Aljabri, Z., Abawajy, J. and Huda, S. (2023) ‘A Comprehensive Review of Lightweight Authenticated Encryption for IoT Devices’, *Wireless Communications and Mobile Computing*, 2023. Available at: https://doi.org/10.1155/2023/9071969.
3. Alshammari, Manal and Alshammari, Mona (2022) ‘Cyber Security for Connected wearable Devices’, *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022* [Preprint]. Available at: https://doi.org/10.1109/ICBATS54253.2022.9758932.
4. Al-Sharrah, M., Salman, A. and Ahmad, I. (2018a) ‘Watch Your Smartwatch’, *2018 International Conference on Computing Sciences and Engineering, ICCSE 2018 - Proceedings*, pp. 1–5. Available at: https://doi.org/10.1109/ICCSE1.2018.8374228.
5. Al-Sharrah, M., Salman, A. and Ahmad, I. (2018b) ‘Watch Your Smartwatch’, *2018 International Conference on Computing Sciences and Engineering, ICCSE 2018 - Proceedings*, pp. 1–5. Available at: https://doi.org/10.1109/ICCSE1.2018.8374228.
6. Centeno, J.K.M. *et al.* (2019a) ‘Performance Analysis of Encryption Algorithms on Smartwatches’, *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2018-October, pp. 162–166. Available at: https://doi.org/10.1109/TENCON.2018.8650067.
7. Centeno, J.K.M. *et al.* (2019b) ‘Performance Analysis of Encryption Algorithms on Smartwatches’, *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2018-October, pp. 162–166. Available at: https://doi.org/10.1109/TENCON.2018.8650067.
8. Dobraunig, C. *et al.* (2021a) ‘Ascon v1.2: Lightweight Authenticated Encryption and Hashing’, *Journal of Cryptology*, 34(3), pp. 1–42. Available at: https://doi.org/10.1007/S00145-021-09398-9/TABLES/21.
9. Dobraunig, C. *et al.* (2021b) ‘Ascon v1.2: Lightweight Authenticated Encryption and Hashing’, *Journal of Cryptology*, 34(3). Available at: https://doi.org/10.1007/S00145-021-09398-9.
10. Farahmand, F. *et al.* (2018) ‘Improved Lightweight Implementations of CAESAR Authenticated Ciphers’, *Proceedings - 26th IEEE International Symposium on Field-Programmable Custom Computing Machines, FCCM 2018*, pp. 29–36. Available at: https://doi.org/10.1109/FCCM.2018.00014.
11. Hung, C.W. and Hsu, W.T. (2018) ‘Power consumption and calculation requirement analysis of AES for WSN IoT’, *Sensors (Switzerland)*, 18(6). Available at: https://doi.org/10.3390/S18061675.
12. Kheirkhahan, M. *et al.* (2019) ‘A smartwatch-based framework for real-time and online assessment and mobility monitoring’, *Journal of Biomedical Informatics*, 89, pp. 29–40. Available at: https://doi.org/10.1016/J.JBI.2018.11.003.
13. Kim, J.W. *et al.* (2019) ‘Collecting Health Lifelog Data from Smartwatch Users in a Privacy-Preserving Manner’, *IEEE Transactions on Consumer Electronics*, 65(3), pp. 369–378. Available at: https://doi.org/10.1109/TCE.2019.2924466.
14. Kim, Y.S. and Kim, G. (2018) ‘A Performance Analysis of Lightweight Cryptography Algorithm for Data Privacy in IoT Devices’, *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, pp. 936–938. Available at: https://doi.org/10.1109/ICTC.2018.8539592.

15. *Lightweight Cryptography | CSRC* (no date). Available at: https://csrc.nist.gov/projects/lightweight-cryptography (Accessed: 18 September 2023).
16. Madushan, H., Salam, I. and Alawatugoda, J. (2022) ‘A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses’, *Electronics 2022, Vol. 11, Page 4199*, 11(24), p. 4199. Available at: https://doi.org/10.3390/ELECTRONICS11244199.
17. Ometov, A. *et al.* (2021) ‘A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges’, *Computer Networks*, 193, p. 108074. Available at: https://doi.org/10.1016/J.COMNET.2021.108074.
18. P., P. *et al.* (2021a) ‘An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices’, *ICT Express*, 7(4), pp. 487–492. Available at: https://doi.org/10.1016/J.ICTE.2021.03.007.
19. P., P. *et al.* (2021b) ‘An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices’, *ICT Express*, 7(4), pp. 487–492. Available at: https://doi.org/10.1016/J.ICTE.2021.03.007.
20. Rahmani, A.M. *et al.* (2022) ‘The Internet of Things for Applications in Wearable Technology’, *IEEE Access*, 10, pp. 123579–123594. Available at: https://doi.org/10.1109/ACCESS.2022.3224487.
21. Rofouei, M. *et al.* (2019) ‘Resource-efficient computing in wearable systems’, *Proceedings - 2019 IEEE International Conference on Smart Computing, SMARTCOMP 2019*, pp. 150–155. Available at: https://doi.org/10.1109/SMARTCOMP.2019.00045.
22. Sadkhan, S.B. and Salman, A.O. (2018) ‘A survey on lightweight-cryptography status and future challenges’, *International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, pp. 105–108. Available at: https://doi.org/10.1109/ICASEA.2018.8370965.
23. Sundaravadivel, P. *et al.* (2018) ‘Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health’, *IEEE Consumer Electronics Magazine*, 7(1), pp. 18–28. Available at: https://doi.org/10.1109/MCE.2017.2755378.
24. Tawalbeh, L. *et al.* (2020) ‘IoT privacy and security: Challenges and solutions’, *Applied Sciences (Switzerland)*, 10(12). Available at: https://doi.org/10.3390/APP10124102.
25. Vijayan, V. *et al.* (2021) ‘Review of Wearable Devices and Data Collection Considerations for Connected Health’, *Sensors (Basel, Switzerland)*, 21(16). Available at: https://doi.org/10.3390/S21165589.