CHAPTER 1

INTRODUCTION

1.1 Rationale

The Internet of Things (IoT) has had a considerable impact on various sectors, including aquaculture. By providing the ability to monitor real-time water environment conditions and collect data for analysis and prediction, these systems have enhanced operational efficiency and supported environmental sustainability [1] . These systems monitor parameters such as water temperature, pH, and dissolved oxygen (DO) to address the clean water crisis [2]. In Indonesia, a notable example of the widespread adoption of these systems is evident, particularly in the context of aquaculture, given the country's status as a major producer of fish [3]. However, a critical concern that emerges from the utilization of these IoT-based water monitoring systems pertains to the integrity of the data they generate. Ensuring the accuracy and reliability of the information collected poses a significant challenge, underscoring the need for robust data management and analysis to inform effective decision-making processes [4].

However, the limited resources of IoT devices, such as processing power, memory, and energy capacity, present significant challenges, particularly in maintaining the integrity of the data collected. It is of paramount importance to ensure the integrity of the data to guarantee the accuracy, reliability, and utility of the information generated, thereby facilitating informed decision-making in aquaculture management [5]. It is imperative that monitoring data be obtained in real time and maintained in an unaltered state, as the integrity of the data can impact the accuracy of subsequent data analysis. The involvement of the Internet in this system presents a cybersecurity risk, as unauthorized access to sensitive data can compromise the integrity of the monitoring system and result in false alarms or the neglect of threats [6, 7].

The issue of security has become increasingly pertinent with the advent of cyberattacks against IoT devices. In the second quarter of 2024, there was a 30% increase in cyberattacks compared to the first quarter of the same year, representing the highest number of cyberattacks since 2021 [8]. Concurrently, the number of cyberattacks on IoT devices in 2022 reached 10.54 million globally [9]. The water quality monitoring sector, which relies on the IoT for the collection of real-time data, is not immune to this threat. Prior research has demonstrated that IoT-based water quality monitoring systems are susceptible to attacks that can impair operational functionality and compromise data integrity. For instance, botnets may employ IoT devices to launch attacks on water infrastructure, resulting in substantial disruption [10].

One potential solution to overcome this challenge is the utilization of lightweight cryp-

tographic hash functions. The function of a hash is to provide a unique identifier for digital data, thereby ensuring that any changes to the data can be detected [11]. The minimal resource requirements of hash functions make them an ideal solution for resource-constrained IoT devices [12]. The optimal implementation of hash functions allows for the increased efficiency of IoT devices while maintaining the necessary data security to support the aquaculture sector as a whole. Among the various hashing algorithms available, xxHash is known for its speed and efficiency in non-cryptographic applications. However, its standard implementation is found to be lacking in cryptographic robustness, rendering it unsuitable for security-critical use cases such as authentication and secure data storage.Given the limited resources of IoT devices, a viable approach to ensuring data integrity in IoT-based water quality monitoring systems is to optimize xxHash to enhance its security features while maintaining its computational efficiency. xxHash is a non-cryptographic hash algorithm that is widely used for high-speed operations such as data compression, indexing, and integrity checking [13]. However, it is not designed for cryptographic security purposes, so it is not suitable for use cases that require one-way hashing and strong collision resistance, such as password storage or digital signatures [14]. Despite these limitations, xxHash offers notable advantages, positioning it as a compelling choice for IoT applications. It provides high throughput and low memory consumption, making it particularly well-suited for resource-constrained environments such as IoT devices (researchgate).Studies on lightweight hash functions for IoT have demonstrated that xxHash operates efficiently on embedded systems, maintaining high-speed data processing with minimal resource usage, despite its lower avalanche effect compared to cryptographic hash functions. These characteristics underscore the necessity to modify xxHash to enhance its security while preserving its efficiency, thereby ensuring that xxHash fulfills the real-time data integrity requirements in IoT-based water quality monitoring systems [15].

The objective of this research is to develop an optimized and secure hash function, specifically designed for resource-constrained IoT devices. It is anticipated that this hash function will maintain the operational efficiency of IoT devices while simultaneously safeguarding the integrity and security of the data collected. If approached in an appropriate manner, this solution has the potential to facilitate the development of a more reliable IoT-based water quality monitoring system at both the national and global levels.

1.2 Theoretical Framework

The objective of this research is to develop an optimal hash function for resource-constrained IoT devices. The following section presents the theoretical and conceptual frameworks that inform this research project.

1. This research is primarily based on cryptography theory. A hash function is a fundamental component of cryptography, serving to generate a distinctive fingerprint of the

input data. This allows for the detection of any alterations to the data. This concept is closely related to data integrity, which ensures that data is not manipulated during transmission or storage. The hash function employed must satisfy fundamental properties, including memory usage, computational speed, and collision resistance.

2. The theory of algorithm efficiency provides a framework for the design of hash functions that are suitable for the limitations of IoT devices. The efficiency of an algorithm encompasses an analysis of its time and space complexity. This is a crucial aspect to consider when developing hash functions, as it ensures their compatibility with devices that have limited processing power, memory, and energy capacity. This concept facilitates the assessment of the proposed hash function in terms of its capacity to achieve a balance between security and resource efficiency.

3. The concept of IoT security is employed to comprehend the particular requirements and challenges associated with IoT devices, particularly in the context of water quality monitoring applications. IoT devices are frequently the target of cyber attacks due to their high connectivity and limited resources. Accordingly, this theoretical framework offers insight into the potential security threats, including collision attacks, data theft, and information manipulation.

This research employs the theories of cryptography, algorithm efficiency, and IoT security to develop a hash function that is not only resource-optimized but also capable of maintaining data integrity on IoT devices utilized for water quality monitoring. This theoretical framework offers a robust conceptual foundation to inform and guide the research objectives.

1.3 Conceptual Framework/Paradigm

The conceptual framework of this research is designed to identify and explain the relationship between variables relevant to the problem of developing an optimal hash function for IoT devices used in water quality monitoring systems. This approach is designed to provide a visual representation of the interrelationships between the primary elements of the research, thereby facilitating the attainment of the research objectives.Identify and discuss the variables related to the problem, and present a schematic diagram of the paradigm of the research and discuss the relationship of the elements/variables therein.

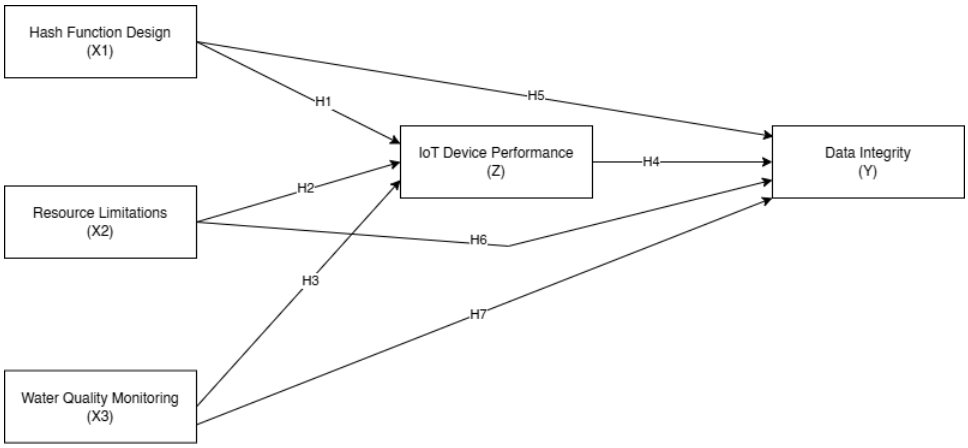

Figure 1.1: Conceptual Paradigm

1. Independent Variables :

   (a) Hash Function Design (X1): The evaluation of the efficiency and security of hash algorithms on IoT devices involves the consideration of throughput, memory usage, and the avalanche effect. Throughput is a metric of data processing speed, memory usage is a measure of resource efficiency, and the avalanche effect ensures that input changes result in a secure hash distribution. The optimization of the hash function in maintaining data integrity in the water quality monitoring system is determined by these three aspects.

   (b) IoT Resource Limitations (X2): External factors such as battery power, memory capacity, and processor speed. These variables are the main limitations that affect the implementation of hash functions.

   (c) Water Quality Monitoring Context (X3): Water quality parameters (such as temperature, pH, turbidity) measured in a real operational environment. This variable introduces additional challenges such as real-time data requirements and unstable network conditions.

2. Variabel Intervening (Z)
   IoT Device Performance: Resource efficiency (memory, power, and computing capacity) and the ability to maintain data integrity. IoT device performance is affected by hash function design, resource limitations, and the context of water quality monitoring.

3. Dependent Variable
   Data Integrity (Y): The ability of the system to ensure that the data generated is accurate, undistorted, and safe from manipulation. Good IoT device performance directly contributes to the achievement of data integrity.

4. Relation between Variables :

(a) H1: Hash function design affects the performance of IoT devices by improving processing efficiency and data security.

(b) H2: IoT resource limitations restrict device performance, so the hash function design should be adapted to these conditions.

(c) H3: The context of water quality monitoring introduces additional challenges, such as real-time requirements, that affect IoT device performance.

(d) H4: IoT device performance directly affects data integrity.

(e) H5 - H7: Hash function design, IoT resource limitations, and water quality monitoring context affect data integrity either directly or through IoT device performance as an intervening variable.

1.4 Statement of the Problem

Ensuring data integrity in IoT-based water quality monitoring systems poses significant challenges, particularly due to the limited computational resources of IoT devices. Traditional cryptographic hash functions, while secure, often impose high computational costs that are unsuitable for resource-constrained environments [16]. For this reason, the development of an efficient, lightweight hashing algorithm is crucial to maintaining data integrity without compromising device performance.

A primary concern is optimizing hashing throughput to ensure that data is processed swiftly, thereby minimizing latency in real-time monitoring applications.Studies indicate that slow data processing can hinder the effectiveness of IoT-based environmental monitoring systems, potentially leading to delays in detecting critical water quality fluctuations [17]. Furthermore, it is imperative to minimize memory consumption to align with the constraints of low-power IoT devices, as excessive resource usage can reduce battery life and overall system efficiency [12].

Another critical aspect is the Avalanche Effect, which determines how significantly small input changes impact the output hash. Enhancing this effect in the modified xxHash can improve its resistance to data manipulation attempts, thereby strengthening data security [5, 18]. Finally, it is essential to evaluate how modifications to xxHash influence the overall efficiency of IoT devices in water quality monitoring applications, ensuring that security enhancements do not compromise system performance [19].

By addressing these challenges, the objective of this research is to develop and evaluate an optimized, lightweight hashing algorithm tailored for IoT-based water quality monitoring, balancing computational efficiency and data integrity.

1.5 Objective and Hypotheses

The objective of this research is to modify xxhash, which will be implemented as a lightweight hash function for IoT Aquaculture. The efficacy of the modifications will be assessed through a comprehensive evaluation of three distinct matrices: throughput, memory utilization, and avalanche effect. This evaluation will serve to ascertain the effectiveness of the algorithm in preserving data integrity within IoT devices characterized by constrained resources. The central focus of this research is the evaluation of the performance of the modified xxHash hash function for IoT devices with limited resources. The following hypotheses have been formulated:

H1: xxHash modification will increase hashing throughput

H2: The modified xxHash will reduce memory consumption, making it more efficient for resource-constrained IoT devices.

H3: The modified xxHash will exhibit better Avalanche Effect values, thereby improving its security.

In accordance with extant research on lightweight hashing algorithms for the Internet of Things (IoT), it is hypothesized that modifying xxHash will enhance its efficiency and security in IoT-based water quality monitoring systems. Specifically, it is anticipated that the modified xxHash will improve hashing throughput, reduce memory consumption, increase the Avalanche Effect, and enhance overall device efficiency.

1.6 Assumption

This research is based on several key assumptions that support the development of hash functions for IoT devices in water quality monitoring applications:

1. IoT devices for water quality monitoring have limited resources, including processing power, memory capacity, and energy, so they need efficient and lightweight algorithms.
2. The designed hash function can maintain data integrity by detecting changes in the collected data in real-time, which is an important requirement in water quality monitoring systems.
3. The optimally designed hash algorithm can improve the resource efficiency of IoT devices without compromising the security level.
4. Cybersecurity threats to IoT devices, such as data collision attacks and information manipulation, are a significant and growing problem as IoT adoption increases in various sectors.

5. Cybersecurity threats to IoT devices, such as data collision attacks and information manipulation, are a significant and growing problem as the adoption of IoT in various sectors increases.

1.7 Scope and Delimitation

1.7.1 Scope

This research project is concerned with the development of optimal and secure hash functions for resource-constrained IoT devices, with a particular focus on applications in water quality monitoring. The research encompasses the design, implementation, and assessment of hash algorithms that enhance resource efficiency (e.g., memory, power, and processing time) while maintaining robust security against cyber threats. The water quality monitoring system that was the subject of the research is capable of monitoring key parameters such as temperature, pH, and turbidity in real time. Furthermore, the research entails the examination of hash algorithms under simulated conditions and their implementation on actual IoT devices, with the objective of assessing their efficiency and security. A comparison is made with existing hash functions, such as BLAKE2 and SHA-3, in order to assess the advantages of the proposed hash function.

1.7.2 Delimitation

1. Key Variables: The research only focuses on the two main aspects of resource efficiency and data security without considering other factors such as interoperability between IoT devices or network challenges.

2. Location: Device testing was conducted on an IoT-based water quality monitoring system designed for laboratory and simulated environments, without direct implementation at industrial production scale or specific geographic locations.

3. Time Frame: This research is conducted within a one-year time frame, which includes the design, implementation, testing, and analysis stages of the designed hash function.

4. Technology Limitations: This study does not cover IoT devices with high specifications, as the focus of the research is on devices with limited resources.

1.7.3 Justification

This scope and restrictions were set to keep the research focus on developing hash functions relevant to resource-constrained IoT devices, according to the needs of the water quality monitoring sector. Restrictions on laboratory testing and simulation were necessary to control variables and ensure reliable results. A time frame of one year was considered sufficient to achieve the research objectives without compromising the quality of the results.

1.8 Significance of the Study

This research has significant contributions in several aspects, both from a scientific point of view and practical applications. Theoretically, this research adds new knowledge in the field of cryptography and IoT technology by developing a hash algorithm specifically designed for resource-constrained devices. The proposed hash algorithm offers better efficiency in memory usage, power, and processing time, while maintaining a high level of security. The findings provide a basis for further research on hash function optimization for other IoT applications beyond water quality monitoring. Practically, this research is beneficial to various user groups:

1. Aquaculture and Water Management Industry: This research provides solutions that can improve the reliability of IoT-based water quality monitoring systems, helping to detect and address water contamination more efficiently and safely.

2. IoT Technology Developers: The proposed hash algorithm can be adopted for other IoT devices with limited resources, thus expanding its benefits in sectors such as health, transportation, and energy.

3. Academics and Researchers: This study serves as an important reference for further research related to algorithm efficiency and data security in IoT devices, as well as the development of innovative solutions in the context of cryptography.

4. Government and Policy Makers: This study can support efforts to improve water quality and environmental sustainability by providing more reliable technologies for water resources management.

With more conclusive and relevant findings, this research is expected to make a real contribution to the development of IoT technology, while addressing the challenges of maintaining the efficiency and security of IoT devices in the water quality monitoring sector.