International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

A State-of-the-Art Survey for IoT Security and Energy Management based on Hashing Algorithms

Teba Mohammed Ghazi Sami[1], Subhi R. M. Zeebaree[2], Sarkar Hasan Ahmed[3]
[1]Computer Science Department, Faculty of Science, University of Zakho, Duhok, Iraq; teba.sami@uoz.edu.krd
[2]Energy Eng. Dept., Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq; subhi.rafeeq@dpu.edu.krd
[3]Network Department, Sulaimani Polytechnic University, Sulaimani, Iraq; sarkar.ahmed@spu.edu.iq

Abstract

The Internet of Things (IoT) has developed as a disruptive technology with wide-ranging applications across several sectors, enabling the connecting of devices and the acquisition of substantial volumes of data. Nevertheless, the rapid expansion of networked gadgets has generated substantial apprehensions pertaining to security and energy administration. This survey paper offers a detailed examination of the present state of research and advancements in the field of Internet of Things (IoT) security and energy management. The work places special emphasis on the use of hashing algorithms in this context. The security of the Internet of Things (IoT) is a crucial element in safeguarding the confidentiality, integrity, and availability of data inside IoT environments. Hashing algorithms have gained prominence as a fundamental tool for enhancing IoT security. This survey reviews the state of the art in cryptographic hashing techniques and their application in securing IoT devices, data, and communication. Furthermore, the efficient management of energy resources is essential to prolong the operational lifespan of IoT devices and reduce their environmental impact. Hashing algorithms are also instrumental in optimizing energy consumption through data compression, encryption, and authentication. This survey explores the latest advancements in energy-efficient IoT systems and how hashing algorithms contribute to energy management strategies. Through a comprehensive analysis of recent research findings and technological advancements, this survey identifies key challenges and open research questions in the fields of IoT security and energy management based on hashing algorithms. It provides valuable insights for researchers, practitioners, and policymakers to further advance the state of the art in these critical IoT domains.

Keywords: IoT, Security, Energy Management, Hashing Algorithms, SHA family.

1. Introduction

The Internet of Things (IoT) has transformed the way we perceive and interact with the digital world, fostering unprecedented connectivity and data-driven insights across various domains. As IoT deployments continue to proliferate, encompassing smart homes, industrial automation, healthcare systems, and beyond, the need for robust security mechanisms and efficient energy management strategies has become more pressing than ever [1]. This state-of-the-art survey delves into the realms of IoT security and energy management, with a specific emphasis on the pivotal role played by hashing algorithms in addressing these critical challenges. IoT is a dynamic ecosystem comprising an extensive network of interconnected devices, sensors, and actuators that communicate and collaborate to collect, process, and share data. This interconnectedness has ushered in an era of unprecedented convenience, automation, and data-driven decision-making across sectors such as healthcare, transportation, agriculture, and smart cities. However, this proliferation of IoT devices also presents multifaceted security and energy management concerns that necessitate immediate attention [2].

Security is paramount in IoT systems, where data privacy, device integrity, and network resilience are of utmost importance. The vast array of interconnected devices and the potential vulnerabilities they introduce create a complex threat landscape. Unauthorized access, data breaches, and cyber-attacks not only jeopardize sensitive information but can also compromise the safety of individuals and the functionality of critical systems. To address these challenges, robust security measures are indispensable. Cryptographic hashing algorithms have emerged as a fundamental building block for IoT security [3]. These algorithms play a pivotal role in ensuring data confidentiality, integrity, and authenticity. By converting data into fixed-size hash codes, hashing algorithms enable secure data transmission, user authentication, and tamper detection. Furthermore, they support efficient encryption, digital signatures, and data deduplication, all of which are crucial in safeguarding IoT ecosystems. In tandem with security concerns, efficient energy management is a critical consideration in IoT deployments. Many IoT devices are battery-powered, making energy conservation paramount for prolonging device lifespan and reducing environmental impact [4]. Hashing algorithms contribute significantly to energy management by enabling data compression, reducing the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

computational load, and enhancing the efficiency of encryption and authentication processes [5][6].

This state-of-the-art survey embarks on an exploration of the current landscape of IoT security and energy management, shedding light on the prominent role of hashing algorithms in addressing these challenges. It provides an in-depth analysis of cryptographic hashing techniques, their applications in securing IoT ecosystems, and their contributions to energy-efficient IoT systems. Moreover, it identifies key research directions and unresolved issues in these domains, aiming to guide researchers, practitioners, and policymakers toward a more secure and sustainable IoT future. As IoT continues its exponential growth and integration into everyday life, understanding the intricacies of IoT security and energy management becomes indispensable [7]. This survey seeks to contribute to the ongoing discourse by consolidating and synthesizing the latest research and innovations in these vital areas, ultimately fostering a more resilient, secure, and energy-conscious IoT landscape [8].

2. Background Theory

Because of the breakthroughs brought about by the Fourth Industrial Revolution, the Internet of Things (IoT) has been able to successfully help in the integration of real-world industrial environments with the virtual world of computer systems. This has been made possible by the advancements that have been made possible by the Fourth Industrial Revolution. The Internet of Things (IoT) came into being as a result of the technological advancements that were made feasible as a result of the Fourth Industrial Revolution. Because of this scenario, it is necessary for there to be a huge number of interconnected systems, each of which has to have a unique identity that enables them to communicate and interact with the other interconnected systems. In contrast to the current state of affairs in actual industrial settings, this is the situation. In addition, these systems have the capability of transmitting data over the network without the need for communication between people or between humans and computers. In addition, the incorporation of contemporary technologies such as Artificial Intelligence (AI), Big Data Analytics (BDA), Machine Learning (ML), and several other growing tools made it feasible to make efficient use of the data that was obtained from a range of sources located within the network [9]. The most recent breakthrough in internet technology is known as the Internet of Things, or IoT for short. It makes it possible to connect a broad range of devices, each of which may have a different number of available resources. These may include devices that have little resources as well as devices that have a restricted supply of resources. According to the findings of the studies that have been carried out in this area, the Internet of Things (IoT) makes it feasible to transform physical items into their digital counterparts [10].

As a direct consequence of the expanding scope of these applications and the escalating rate of their invention, there has been a perceptible rise in the number of cyberattacks that particularly target Internet of Things (IoT) applications. This has led to an increase in the overall number of IoT-specific cyberattacks. Both the businesses that manufacture the devices and the individuals who use them are finding it more challenging to ensure the safety of Internet of Things (IoT) devices [11]. This issue, which arises from the extensive use of homogenous sensor nodes in the IoT, is closely connected to the dearth of safe devices that exist inside the Internet of Things (IoT). In the context of the Internet of Things (IoT), heterogeneity refers to the presence of a wide variety of interfaces, frameworks, and laws, in addition to a plethora of different types of physical resources. Some examples of these types of resources include differing degrees of processor compute power and storage capacity [12]. It is well knowledge that one of the most serious threats to data security is posed by the predisposition of extra apps to fall prey to a variety of vulnerabilities [13]. The primary reason for concern is that there aren't any of the more traditional kinds of safety precautions in place. A future in which Internet of Things (IoT) devices will blend in seamlessly with their surroundings and result in the generation of enormous volumes of data is conceivable and may be envisioned. It is crucial that the data be processed and kept in a safe way, as this will ensure that the data retains both its meaningfulness and its value. Because of this, it is very important for anybody who is interested in building applications for the Internet of Things (IoT) to perform research on the special security problems offered by IoT, which are different from those encountered in conventional networks [14].

It has been determined that the management of energy in IoT networks is a key component for increasing power efficiency and elongating the length of time that IoT devices may continue to operate correctly. This conclusion was reached as a result of the findings of the previous statement. In the context of applications that make use of the Internet of Things (IoT), there has been a perceptible increase in the amount of energy that is needed. Energy management is a crucial issue in this specific context since there is the potential for significant energy savings and an efficient reduction in the severity of energy crises [15]. This is the primary reason why there is so much cause for concern about energy management. The user has provided a reference to a number; however, this reference does not have any supporting material or context associated with it. Recent years have witnessed a dramatic acceleration in the rate of urbanization, which has necessitated the deployment of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

measures that are sustainable, efficient, and intelligent in order to solve a variety of issues, including transportation, governance, environmental concerns, and general quality of life in general [16]. This has necessitated the deployment of measures that are sustainable, efficient, and intelligent in order to solve these issues. The Internet of Things (IoT) is able to provide support for a wide range of cutting-edge as well as general applications that are important to the growth of smart cities. The simultaneous growth in the number of IoT devices and the specifications of those devices has led to a rising tendency in the energy consumption of Internet of Things (IoT) applications, which has witnessed an upward trend in the recent years [17]. This trend has been observed in recent years. Therefore, it is essential that the solutions that make up smart cities have the capacity to effectively gather energy and appropriately handle the challenges that are involved with doing so. This is because smart cities are becoming more important. It is widely agreed upon that the concept of energy management ought to act as the foundation for the development of intricate energy systems inside smart cities [18].

When seeking to solve the energy problems that are caused by Internet of Things (IoT) networks, it is standard procedure to make use of a broad number of different strategies that have shown to be effective. The following strategies fall within this category: The development of algorithms, protocols, and hardware solutions with the objective of decreasing the amount of energy that is used by networks and lengthening their lifespans is given priority by initiatives aimed at saving energy. The purpose of these initiatives is to reduce the amount of energy that is consumed by networks. The low energy capacity of IoT devices, which are supposed to run constantly for long periods of time without the need for the batteries to be changed, has turned out to be a significant obstacle for the Internet of Things (IoT), which is a major drawback of the IoT. In addition, there has been a significant increase in the number of devices that are linked to IoT networks. This is due to the fact that the Internet of Things (IoT) is gaining more and more attention. Because of this, the carbon footprint of IoT networks has significantly increased in recent years. Both academic scholars and industry professionals are finding that the emergence of Green-IoT and energy management of IoT has become a fascinating and engaging subject of study [19]. Green-IoT stands for "Internet of Things" and energy management of IoT. The term "Green-IoT" refers to the Internet of Things (IoT) that is run by alternative or renewable forms of electricity. Because there is not currently a technology that is readily deployed, easily maintained, and can be acquired at a low cost, the widespread adoption of these systems has been somewhat hampered as a result. Data storage, data management, and data analysis are all made more difficult by the enormous volume of data that is acquired from a variety of urban areas spread throughout a nation. The use of technology that is associated with the Internet of Things (IoT) and the utilization of big data can turn out to be an effective technique for overcoming the existing difficulties. The technologies that go into making up the Internet of Things (IoT) have the potential to create a pervasive computing platform that makes it feasible to detect, monitor, and exert control over the amount of energy that is consumed by home appliances on a vast scale. This would make it possible to reduce overall energy consumption. The data gathering is being handled via an extensive variety of wireless sensors [20] that have been put in residential units.

Over the course of the last several years, it has been abundantly evident that a number of hashing algorithms that were originally assumed to be dependable have severe faults that render them unsuitable for assuring the continuous safety of cryptographic systems. These issues include the inability to properly handle collisions, which is a common kind of attack against cryptographic systems. As a result of continuous advancements in computer power, a variety of cryptographic attacks that were formerly thought to exist only in the world of theory are now within the grasp of those who would intentionally inflict damage. These attacks were previously supposed to be impossible. Recent significant advancements in the field of quantum computing predict that in the not too distant future, there will be an enhanced capacity to launch assaults against hashing algorithms that are more successful. This is based on the idea that quantum computers would be able to solve certain problems that were previously unsolvable. As a consequence of this, the creation of novel hashing algorithms that provide enough cryptographic resilience in the face of contemporary assaults made feasible by supercomputers and quantum computers is an imperative need. Utilizing effective cryptographic hash algorithms makes it feasible to protect the data even in the face of ongoing increases in computing power that may be made available to potential adversaries [21]. This is because these adversaries are unlikely to be able to get their hands on such capacity.

A mathematical operation is said to be a hash function if it generates an output with a size that is both stated and fixed, in addition to accepting data of any quantity as its input. An in-depth analysis of the standard hash function is the first step towards discovering cryptographic hash functions. Examples of hash algorithms that are used often in the modern world include the Message-Digest Algorithm 5 (MD5) and several iterations of the Secure Hash Algorithm (SHA). The integrity of the data must be preserved at all costs in order for the system to be considered highly secure [22]. When users interact with a cryptographic hash function system, they are presented with the option to produce a hash value for the message that they are

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

sending. The fundamental objective of the system is to make it much easier to discover any unlawful modifications that have been done to files; this is one of the benefits that the system provides. It is of the highest need to take safeguards in order to maintain the security of vital computer systems and sensitive data. It is possible to verify the origin of data by combining hash functions with other forms of cryptography that are already well-established. Several distinct approaches are possible for achieving this goal. When hashing methods are employed in combination with encryption, the result is the creation of one-of-a-kind message hash values that may be used to determine the origin of the data [23].

The Secure Hash algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), which was the institution responsible for developing the algorithm in 1993. In the years that followed, in 1995, NIST made improvements to the method in order to address and eliminate many problems that had been identified in the manner that it was first put into practice. These weaknesses had been uncovered in the way that it was initially implemented. In the year 2001, a proposal was made for an entirely new hashing algorithm that was going to be referred to as SHA-2. The approach that is employed in this case makes use of bigger digital messages, which both raises their resilience to probable assaults and permits their use with larger data chunks. This is how the method gets over the limitations that smaller digital messages have. All of the SHA functions, including SHA-224, SHA-256, SHA-384, and SHA-512, have the same characteristics. The key characteristics that set these functions apart from one another are their relative sizes, particularly those of the operators, the initiators, and the final message expression. [24]. The user has provided a numerical reference of [25], and it is being used here. There are many different iterations of applications that include hashing as a method for increasing the amount of security that they provide for their users. The hashing technique is an effective approach for validating and confirming that the data supplied by a user is sent by a legitimate entity, or that the information that was received is genuine and has not been changed in any way. This may be done by comparing the data that was received with the data that was submitted by the user. There have been a number of approaches developed with the intention of obtaining hash values. Some of these approaches have been deemed insufficient and, as a result, have been disregarded, while others have been commonly accepted as meeting or exceeding certain criteria. Data integrity may be checked with the use of hash value comparisons. For creating hash values, the standards that are universally recognized are MD and SHA (which contains SHA-1 and SHA-2), respectively. MD and SHA both include SHA-1 and SHA-2. Because technological progress is an ongoing process, it is required to either create brand-new techniques or discover ways to improve upon those that are currently in use in order to stay up with the most recent needs. In order to do so, it is necessary to either invent brand-new methods or find ways to improve upon those that are already in use. A specific kind of cryptographic procedure known as a hash algorithm compresses the contents of an input message of any length into a numerical number that is referred to as a hash value. This value may be used in the process of validating the authenticity of the first message. The primary characteristic that distinguishes hash algorithms from one another is the degree of complexity that they bring to the task of locating two distinct messages that generate the same hash result. This is one of its primary distinguishing characteristics. The usual operation that the hash algorithm performs is shown in Figure (1) [26], which may be found below.

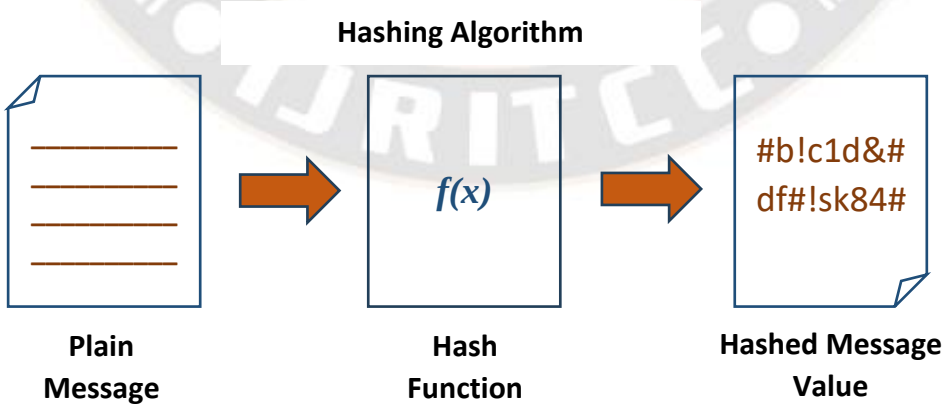

Figure (1): A Typical Process of Hash Algorithm.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

3. Literature Review

The field of IoT device security and energy management has seen a surge in research efforts, aiming to fortify the resilience and efficiency of these devices. Many studies have delved into cryptographic solutions and energy-aware algorithms. Cryptographic approaches bolster data protection and secure communications, ensuring the integrity and confidentiality of transmitted information, and optimize power consumption, extending the operational life of IoT devices. In this chapter, a literature survey is presented of previous works that Enhancing IoT Devices Security and Energy Management based on secure hashing algorithm.

Zhang, et al. [27], 2019, centered on Bitcoin's pivotal role in blockchain technology and the critical challenge of hash function computation within its proof-of-work mechanism. It primarily focused on optimizing FPGA implementation of the hash function, starting with the determination of the algorithm's iteration bound using iteration bound theory. Subsequently, it employed techniques such as carry-save adder and retiming to align the critical path's computation time with the iteration bound. Further optimizations were made by considering the constant input component and result requirements to reduce the hash function calculation cycles. They concluded with simulation results demonstrating the enhanced efficiency of hash function calculations. Additionally, the paper introduced the iteration bound theory as a foundational concept for SHA-256 optimization on FPGA, accompanied by a corresponding block diagram. they emphasized improvements in computational efficiency tailored to Bitcoin mining scenarios, and the efficiency gains were validated through simulation experiments, indicating significant enhancements in hash function calculation efficiency without substantial increases in resource utilization.

Maliberan, et al. [28], 2019, suggested to use a modified form of the SHA-1 algorithm, in which the hash size would be extended from the standard 160 bits to a value of 1280 bits. This improvement was accomplished by assigning 32 buffer registers, each of which consisted of 5 bytes, to the variables A, B, C, and D. This allowed for a significant increase in storage capacity. Within each cycle of the compression function, the process of expanding comprised the construction of four registers. This procedure was carried out for a total of eight times, making up the expansion process. Empirical testing has shown, and this is significant, that efforts to break the hash code generated by the modified SHA-1 algorithm using strong online cracking tools, brute force assaults, and rainbow table attacks were unsuccessful. This noteworthy result indicates an increase in the security of the modified SHA-1 algorithm compared to its original counterpart, notably in protecting online applications against a variety of dangers, including flaws in login authentication procedures. In particular, this improvement can be seen in safeguarding web applications against the threat of phishing attacks. This method exhibited a significant increase in the degree of hash security that is necessary for protecting online applications.

Cortez, et al. [29], 2020, examined the security capabilities of the modified SHA-256 algorithm in safeguarding data from attacks, particularly focusing on length extension. They implemented various input message techniques within the padding scheme and additional operations in the cryptographic hash function to bolster the hash's resistance to the attacks. Randomness tests, including Run Test, demonstrated a uniform random distribution of the generated hashes. These findings suggested that the modified SHA-256 algorithm offered robust security, making it challenging to break, and future research could explore its resilience against other common hashing algorithm attacks.

Martino, et al. [30], 2020, introduced a versatile HW accelerator designed to bolster SHA-256 performance while accommodating the specific limitations and requirements of the IoT domain. Experimental results revealed the accelerator's ability to empower resource-constrained IoT devices, enabling them to effectively engage in complex tasks associated with blockchain applications. They underscored the imperative need to tailor HW acceleration solutions to IoT's unique constraints, offering a promising avenue for enhancing IoT security and facilitating the adoption of blockchain technology in diverse IoT applications.

In the Bitcoin network, the double SHA-256 computation was a major energy-consuming process, making power reduction and processing rate enhancement a critical research focus. Pham, Hoai Luan, et al. [31], 2020, presented a novel HW architecture called the compact message expander (CME) double SHA-256, which combined resource sharing and fully unrolled data path techniques to achieve high data rates and low power consumption. The CME algorithm leveraged the specific characteristics of double SHA-256 input data, reducing HW costs and power consumption. Comparative analysis demonstrated that the CME algorithm reduced the requirement for XOR gates, adders, and registers significantly. This advancement was particularly relevant in the context of Bitcoin mining, as it addressed energy efficiency and processing speed concerns. Furthermore, they emphasized the broader applicability of blockchain technology beyond Bitcoin, signaling the need for flexible and programmable accelerators capable of handling various cryptography hash functions, opening new avenues for research in the blockchain domain.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

Smolarz, Andrzej, et al. [32], 2021, addressed the field of modern cryptography, and information security played a crucial role in addressing risks within digital operations in cyberspace. Hash functions were pivotal among information security technologies, efficiently processing limited-length critical data to generate fixed-size digital codes, known as hashes or digests. These functions served classic purposes, including data integrity verification and authentication of user messages. However, as the volume of risk-dependent data processing grew, the throughput of hash functions became a paramount consideration. SHA-3, the latest addition to the SHA family, introduced by NIST in August 2015, differed internally from its predecessors. It stood as a generally accepted hashing standard and boasted the fastest implementation of the SHA-512 (SHA-3 variant) cryptographic algorithm, offering adequate bandwidth for safeguarding risk-dependent critical data. Analyzing the role of cryptographic hash functions in safeguarding such data and efficiently compressing critical messages in risk-dependent computer systems revealed their promising potential in modern cryptography. These crypto-resilient functions excelled at protecting limited-length critical information by producing fixed-size digital codes. As the need to secure risk-dependent critical data intensified, the throughput of hash functions gained prominence, making the modification of hash algorithms to enhance throughput a pressing concern within contemporary information security research.

Bemida, et al. [33], 2021, resulted in the creation of an updated version of the SHA-512 algorithm, which was developed for the exclusive purpose of password hashing. Adjustments were made to the message scheduling, the creation of the hash, and the compression function as part of the revisions. In addition, the number of iterations has been decreased in order to increase the computational efficiency as well as the resistance against possible assaults. Following the implementation of the changes, the algorithm produced an avalanche percentage of 50.84%, which is higher than the target goal of 50%. In addition to this, it was resistant to attacks using brute force, rainbow tables, and dictionaries. The original SHA-512 algorithm had an average elapsed time of 5,384 milliseconds, but the modified version had an observed average elapsed time of 3,485 milliseconds. This indicates that the modified version is much faster than the original version. In light of this, the new SHA-512 algorithm is both effective and resilient as a method for hashing passwords. In compared to the original algorithm, it displays increased productivity and a greater resistance to attacks.

Quilala, et al. [34], 2022, advanced document integrity verification using Quick Response (QR) codes through the integration of a modified SHA-1 hashing algorithm and an updated encryption method, modified Blowfish, guaranteeing both data integrity and security during transmission. The developed SW underwent rigorous testing against user requirements and exhibited commendable levels of acceptability, accuracy, and heightened security. While the SW showcased a low error rate of 3.33%. Additionally, exploring the implementation of cost-effective blockchain technology in educational institutions presented a promising avenue for further investigation, potentially bolstering the system's capabilities and overall performance.

Pham, Hoai Luan, et al. [35], 2022, the Multimode SHA-2 Accelerator (MSA) was developed with the purpose of boosting the flexibility and effectiveness of SHA-2 cryptographic algorithms, which are an important component in a broad range of various applications. The Multimode SHA-2 Accelerator (MSA) was built with the intention of enhancing the versatility and efficacy of SHA-2 cryptographic algorithms. The MSA made use of three efficient methodologies: a multimode processing element architecture, which made it easier to compute a variety of SHA-2 functions; a three-stage arithmetic logic unit pipeline architecture, which reduced the number of critical paths and requirements for hardware resources; and nonce generator and nonce validator architectures, which enhanced memory access and mining performance in blockchain applications. The MSA was able to effectively perform its objectives in large part because to the contributions of each of these architectures in particular. The Field Programmable Gate Array (FPGA) manufactured by Xilinx called the Alveo U280 was put through extensive testing on its hardware, which produced remarkable results in terms of the device's overall performance, hardware efficiency, and adaptability. These outcomes were above and above what was possible with the previous designs. The fact that the MSA reached a record-breaking level of energy efficiency, clocking in at a maximum of 38.05 Mhps/W, should be brought to everyone's attention since it is vital. This speed was 543.6 times greater than the most recent iteration of the RTX 3090 GPU, and it was also 29 times faster than the most recent iteration of the Intel i9-10940X central processor unit. In addition, the authors emphasized how essential it is for future research to include support for more cryptographic hash algorithms like SHA-3, BLAKE, and MD-5. This was a point that was driven home repeatedly. This is done in order to accommodate the ever-evolving requirements of blockchain mining and data security applications.

Mohanty, Mohan Debarchan, et al. [36], 2022, presented a modified SHA-256 encryption algorithm to enhance security in medical insurance data processing, mitigating fraud risks. The modified algorithm generated a long key and combined it for robust encryption, applicable to both insurance and medical data. Results demonstrated the efficacy of deep-learning models in admission decision-making, while patient data were

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

secured through 256-bit hash encryption, offering a smart and secure medical management system benefiting both medical personnel and patients. This approach also improved disease detection efficiency and enhanced health insurance data security, making it a valuable tool for effective healthcare services and data protection.

Suhaili, et al. [37], 2022, focused on the implementation of the SHA-256 (Secure Hash Algorithm-256) hash function. They introduced the concept of the unfolding transformation to augment the throughput of the SHA-256 design, effectively reducing the number of clock cycles from 64 to 34 and enabling the generation of up to four parallel inputs for output in a single cycle. ModelSim simulations validated the Verilog code, while HW implementation on an Altera DE2-115 FPGA board attested to the effectiveness of the proposed unfolding techniques. The results demonstrated a significant throughput improvement of 4196.30 Mbps for the SHA-256 unfolding factor four design, showcasing its potential in enhancing hash function performance. Additionally, while area implementation remained a challenge, the combination of pipelining and unfolding techniques held promise for future security applications, making this design valuable for various cryptographic applications and innovations.

Uganya, et al. [38], 2023, The Multiple-Node Accessibility Shortest route algorithm, also known as MECC-MSS, is a proposed method with the goal of finding the shortest path between nodes in order to offer accessibility to multiple nodes. The system made it possible to carry out several transactions by using a number of different keys, and it had the additional feature of increasing the size of the input key to a maximum of 512 bytes. Several different Secure Hash Algorithms (SHAs), such as SHA-224, SHA-256, SHA-384, SHA-512, MD5, SHA3-224, SHA3-256, SHA3-384, and SHA3-512, were used in order to conduct the performance analysis of the approach that is now under consideration. In order to analyze the statistical performance, a one-way analysis of variance (ANOVA) test was used. This test examined both the accuracy and the time complexity of the process. A high degree of accuracy was proven using the MECC-MS method, which had a precision of 90.85%. In addition to this, the temporal complexity of the system was just 1.4 nanoseconds, which is a fairly low value. The significance level was lower than 0.05, which indicates that these findings are statistically significant. The findings of the statistical study allow one to draw the conclusion that the technique that was recommended had a noticeably higher degree of accuracy and demonstrated decreased time complexity in comparison to other cryptographic hash algorithms. This conclusion can be reached as a consequence of the findings.

4. Discussion and Comparison

Table (1) illustrates a detailed comparison among the previous works. These works collectively address various aspects of hash functions, including optimization for specific applications, security enhancements, and efficiency improvements, catering to diverse domains such as cryptocurrency, web security, IoT, and healthcare.

Table (1): Comparison among the previous works.

Reference	Implemented Fields	Hashing Algorithm	Length (bits) output	Block Size(bits)	Word Size (bits)	# Iterations	# K Constant	# H Valued	Significant Satisfied Aims
[27], 2019	security	SHA-256	256	512	32	61	64	8	The paper proposed an FPGA-based SHA256 implementation with improved computational efficiency for Bitcoin mining, using the iteration bound theory and other optimizations.
[28], 2019,	security, integrity	SHA-1	1280	512	32	8	4	3 2	Modified SHA1 hash code remains uncracked against brute force, online cracking tools, and rainbow table attacks, enhancing web application security.
[29], 2020	security	SHA-256	256	1024	64	32	64	8	Randomness tests, including Run Test, demonstrated a uniform random distribution of the generated hashes. These findings suggested that the modified SHA256 algorithm offered robust security, making it challenging to break,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

[30], 2020	security	SHA-256	256	512	32	64	64	8	Experimental results revealed the accelerator's ability to empower resource-constrained IoT devices, enabling them to effectively engage in complex tasks associated with blockchain applications.
[31], 2020	energy	double SHA-256	256	1024	32	64	64	8	CME algorithm reduces XOR gates, adders, and registers, improving energy efficiency and processing speed for Bitcoin mining and beyond.
[32], 2021	security, integrity	SHA-512	512	1024	64	80	16	8	Hash functions in risk-dependent computer systems have promising potential in modern cryptography, protecting limited-length critical information. Modifying hash algorithms to enhance throughput is a pressing concern in information security research.
[33], 2021	security	SHA-512	256	512	64	64	64	5	the difference between the modified and original SHA-512 algorithms was assessed in terms of runtime execution and time complexity.
[34], 2022	integrity, security	modified SHA-1 and blowfish algorithms	192	-	-	-	-	-	The developed SW underwent rigorous testing and exhibited high acceptability, accuracy, and security, with a low error rate of 3.33%. Exploring the implementation of cost-effective blockchain technology in educational institutions is a promising avenue for further investigation, as it could bolster the system's capabilities and overall performance.
[35], 2022	security, energy	SHA-2, SHA-256d	256	1024	32-64	64	64 - 80	8	the proposed MSA is significantly better than the Intel i9-10940X CPU and RTX 3090 GPU in energy efficiency .Overall, our accelerator supports only the hash functions of the SHA-2 family.
[36], 2022	healthcare, security	SHA-256	256	512	32	64	64	8	Deep-learning models for admission decision-making with patient data security improve disease detection, enhance health insurance data security, and benefit both medical personnel and patients.
[37], 2022	security	SHA-256	256	512	32	18	64	8	The results demonstrated a significant throughput improvement of 4196.30 Mbps for the SHA-256 unfolding factor four design, showcasing its potential in enhancing hash function performance
[38], 2023	security	MECC-MS	-	4096	-	-	-	-	MECC-MS hash algorithm achieves significantly better accuracy (90.85%) with less time complexity (1.4 nanoseconds) than other cryptography hash algorithms.

Zhang, et al. [27], 2019: focused on optimizing the hash function computation within Bitcoin's proof-of-work mechanism using FPGA implementation. It emphasizes improvements in computational efficiency tailored to Bitcoin mining scenarios, resulting in enhanced hash function calculation efficiency. Maliberan, et al. [28], 2019: introduced a modified SHA-1 algorithm with an expanded hash size to enhance security for web applications. It effectively resists various attacks, making it a significant improvement in hash security. Cortez, et al. [29], 2020:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

examined the security capabilities of the modified SHA-256 algorithm, particularly in safeguarding data from length extension attacks. It demonstrates robust security and uniform random distribution of generated hashes. Martino, et al. [30], 2020: introduced a hardware accelerator for SHA-256, tailored for resource-constrained IoT devices. The focus is on enhancing blockchain applications in the IoT domain, considering unique constraints. Pham, Hoai Luan, et al. [31], presented a novel hardware architecture for double SHA-256 computation, addressing power reduction and processing rate enhancement, particularly relevant in Bitcoin mining. It emphasizes the need for flexible accelerators for various cryptographic hash functions.

Smolarz, Andrzej, et al. [32], discussed the importance of hash functions in modern cryptography and information security, with a focus on throughput. It highlights the role of SHA-3 in efficiently processing limited-length critical data. Bemida, et al. [33], 2021: presented a modified SHA-512 algorithm for password hashing, enhancing efficiency and resistance against attacks compared to the original algorithm. Quilala, et al. [34], 2022: integrated a modified SHA-1 hashing algorithm and modified Blowfish encryption into Quick Response (QR) codes for document integrity and security. It explores the potential use of blockchain technology in educational institutions. Pham, Hoai Luan, et al. [35], 2022: introduced the Multimode SHA-2 Accelerator (MSA) for SHA-2 cryptographic functions, emphasizing performance, efficiency, and flexibility, including support for various cryptographic hash algorithms. Mohanty, Mohan Debarchan, et al. [36], 2022: presented a modified SHA-256 encryption algorithm for securing medical insurance data, enhancing security and efficiency in healthcare data management. Suhaili, et al. [37], 2022: focused on optimizing the SHA-256 hash function with unfolding techniques to improve throughput. The design shows promise for various cryptographic applications. Uganya, et al. [38], 2023: proposed the MECC-MSS algorithm for finding the shortest path between nodes with multiple transactions and keys. It achieves high accuracy and low time complexity compared to other cryptography hash algorithms.

5. Conclusion

In conclusion, the academic publications give a comprehensive view of hash functions' dynamic domain and numerous practical applications. The above studies illustrate the necessity of hash functions in satisfying modern cryptography and information security needs. They investigate several topics, including bitcoin hash function calculation, FPGA Bitcoin mining, and online application security. The study also tests cryptographic algorithms' resilience, notably the modified SHA-256 algorithm's length extension resistance. Hardware accelerators for low-resource IoT devices demonstrate the importance of hash functions. The focus on energy efficiency and processing speed in Bitcoin mining, particularly in hardware design, emphasizes the need for adaptable accelerators that can handle a variety of cryptographic hash algorithms. Hash functions are crucial to information security due to their use in modern cryptography and ability to handle sensitive data. The improved SHA-512 algorithm enhances password hashing and boosts its resilience to attacks, meeting the growing requirement for secure authentication. This research examines how blockchain technology might improve data security in educational institutions by combining updated hashing algorithms and encryption methods into document integrity verification. The Multimode SHA-2 Accelerator highlighted the need of adaptive cryptographic hardware. Healthcare data management is more secure and efficient with updated SHA-256 encryption.

References

[1] H. Kopetz and W. Steiner, "Internet of things," in Real-time systems: design principles for distributed embedded applications: Springer, 2022, pp. 325-341.

[2] M. Rupesh and N. A. Selvan, "Design of IoT based smart energy meter for home appliances," in Journal of Physics: Conference Series, 2021, vol. 1964, no. 5: IOP Publishing, p. 052001.

[3] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. C. Bălan, E. Tuyishime, and R. Acheampong, "Cybersecurity challenges in IoT-based smart renewable energy," 2023.

[4] Sami, Teba Mohammed Ghazi, Subhi RM Zeebaree, and Sarkar Hasan Ahmed. "A Comprehensive Review of Hashing Algorithm Optimization for IoT Devices." International Journal of Intelligent Systems and Applications in Engineering 11.6s (2023): 205-231.

[5] R. C. Motta, K. M. de Oliveira, and G. H. Travassos, "An evidence-based roadmap for IoT software systems engineering," Journal of Systems and Software, vol. 201, p. 111680, 2023.

[6] Sadeeq, Mohammed AM, et al. "Internet of Things security: a survey." 2018 International Conference on Advanced Science and Engineering (ICOASE). IEEE, 2018.

[7] Ageed, Zainab Salih, et al. "A state of art survey for intelligent energy monitoring systems." Asian Journal of Research in Computer Science 8.1 (2021): 46-61.

[8] J. C. M'Kaila and L. Rajabion, "A Strategic Approach to IoT Security by Working Towards a Secure IoT Future," International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), vol. 7, no. 1, pp. 1-18, 2023.

[9] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, and R. Nordin, "Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

algorithms," Wireless Communications and Mobile Computing, vol. 2021, pp. 1-23, 2021.

[10] J. Jebrane and S. Lazaar, "A performance comparison of lightweight cryptographic algorithms suitable for IoT transmissions," General Letters in Mathematics (GLM), vol. 10, no. 2, 2021.

[11] N. A. M. Alhammadi and K. H. Zaboon, "A review of IoT applications, attacks and its recent defense methods," Journal of Global Scientific Research, vol. 7, no. 3, pp. 2128-2134, 2022.

[12] Sadeeq, Mohammed Mohammed, et al. "IoT and Cloud computing issues, challenges and opportunities: A review." Qubahan Academic Journal 1.2 (2021): 1-7.

[13] K. Janani and S. Ramamoorthy, "IoT security and privacy using deep learning model: a review," in 2021 International conference on intelligent technologies (CONIT), 2021: IEEE, pp. 1-6.

[14] N. Lata and R. Kumar, "Security in internet of things (IoT): challenges and models," Mathematical Statistician and Engineering Applications, vol. 71, no. 2, pp. 75–81-75–81, 2022.

[15] E. Leloglu, "A review of security concerns in Internet of Things," Journal of Computer and Communications, vol. 5, no. 1, pp. 121-136, 2016.

[16] A. H. Bagdadee, L. Zhang, and M. Saddam Hossain Remus, "A brief review of the IoT-based energy management system in the smart industry," Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 443-459, 2020.

[17] Rashid, Zryan N., et al. "Distributed and Parallel Computing System Using Single-Client Multi-Hash Multi-Server Multi-Thread." 2021 1st Babylon International Conference on Information Technology and Science (BICITS). IEEE, 2021.

[18] T. V. K. Nguyen, "From theory to practice: towards scalable and smart energy monitoring based on the Internet of Things," Macquarie University, 2023.

[19] S. Benhamaid, A. Bouabdallah, and H. Lakhlef, "Recent advances in energy management for Green-IoT: An up-to-date and comprehensive survey," Journal of Network and Computer Applications, vol. 198, p. 103257, 2022.

[20] A.-R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. AliKarar, "A smart home energy management system using IoT and big data analytics approach," IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 426-434, 2017.

[21] L. V. Cherckesova, O. A. Safaryan, N. G. Lyashenko, and D. A. Korochentsev, "Developing a New Collision-Resistant Hashing Algorithm," Mathematics, vol. 10, no. 15, p. 2769, 2022.

[22] Sadeeq, Mohammed AM, and Subhi Zeebaree. "Energy management for internet of things via distributed systems." Journal of Applied Science and Technology Trends 2.02 (2021): 59-71.

[23] P. P. Pittalia, "A comparative study of hash algorithms in cryptography," International Journal of Computer Science and Mobile Computing, vol. 8, no. 6, pp. 147-152, 2019.

[24] A. Sideris, T. Sanida, and M. Dasygenis, "Hardware acceleration of SHA-256 algorithm using NIOS-II processor," in 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2019: IEEE, pp. 1-4.

[25] Sami, Teba Mohammed Ghazi, Subhi RM Zeebaree, and Sarkar Hasan Ahmed. "A Novel Multi-Level Hashing Algorithm to Enhance Internet of Things Devices' and Networks' Security." International Journal of Intelligent Systems and Applications in Engineering 12.1s (2024): 676-696.

[26] B. U. I. Khan, R. F. Olanrewaju, M. A. Morshidi, R. N. Mir, M. L. B. M. Kiah, and A. M. Khan, "Evolution and analysis of secured hash algorithm (SHA) family," Malaysian Journal of Computer Science, vol. 35, no. 3, pp. 179-200, 2022.

[27] X. Zhang and H. Hu, "Optimization of hash function implementation for bitcoin mining," in 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019), 2019: Atlantis Press, pp. 448-452.

[28] E. V. Maliberan, "Modified SHA1: a hashing solution to secure web applications through login authentication," International Journal of Communication Networks and Information Security, vol. 11, no. 1, pp. 36-41, 2019.

[29] D. M. A. Cortez, A. M. Sison, and R. P. Medina, "Cryptanalysis of the Modified SHA256," in Proceedings of the 2020 4th High Performance Computing and Cluster Technologies Conference & 2020 3rd International Conference on Big Data and Artificial Intelligence, 2020, pp. 179-183.

[30] R. Martino and A. Cilardo, "Designing a SHA-256 processor for blockchain-based IoT applications," Internet of Things, vol. 11, p. 100254, 2020.

[31] H. L. Pham, T. H. Tran, T. D. Phan, V. T. D. Le, D. K. Lam, and Y. Nakashima, "Double SHA-256 hardware architecture with compact message expander for bitcoin mining," IEEE Access, vol. 8, pp. 139634-139646, 2020.

[32] A. Smolarz et al., "Using hash functions to protect critical messages from changes in risky computing systems," in CITRisk, 2021, pp. 434-444.

[33] P. J. F. Bemida, A. M. Sison, and R. P. Medina, "Modified SHA-512 Algorithm for Secured Password Hashing," in 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 2021: IEEE, pp. 1-9.

[34] T. F. G. Q. Rogel LadiaQuilala, "Document verification using quick response code with modified secure hash algorithm-1 and modified blowfish algorithm," Indonesian Journal of Electrical Engineering and Computer Science, vol. 28, pp. 470-479, 2022, doi: 10.11591/ijeecs.v28.i1.

[35] H. L. Pham, T. H. Tran, V. T. D. Le, and Y. Nakashima, "A high-efficiency FPGA-based multimode SHA-2 accelerator," IEEE Access, vol. 10, pp. 11830-11845, 2022.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v11i10.8488
***Article Received:** 27 July 2023 **Revised:** 14 September 2023 **Accepted:** 02 October 2023*

[36] M. D. Mohanty et al., "Design of Smart and Secured Healthcare Service Using Deep Learning with Modified SHA-256 Algorithm," in Healthcare, 2022, vol. 10, no. 7: MDPI, p. 1275.

[37] S. Suhaili and N. Julai, "FPGA-based Implementation of SHA-256 with Improvement of Throughput using Unfolding Transformation," Pertanika Journal of Science & Technology, vol. 30, no. 1, 2022.

[38] G. Uganya and R. Baskar, "Modified Elliptic Curve Cryptography Multi-Signature Scheme to Enhance Security in Cryptocurrency," Computer Systems Science & Engineering, vol. 45, no. 1, 2023.