Power System Technology
ISSN:1000-3673

Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

An Improved Variable Length Lightweight DESSHA for IoT-Enabled Smart Devices

Shafaan Khaliq Bhatti[1], Khalid Mahmood Aamir[1], Misbah Jabeen[1]

[1] Department of Information Technology, University of Sargodha,

Sargodha, 40162, Punjab, Pakistan

ABSTRACT

Amidst the accelerating scenarios of cybersecurity and increasing concerns regarding data integrity organizations seriously seek strong and scalable frameworks as safeguard against sensitive data to keep it unmodified from illegitimate access. To ensure consistent performance and optimization in resource utilization over various types of devices security and scalability are of utmost requirements. Data integrity has become challenging issue in resource constrained devices as used in IoT. IoT has become one the major components in automation of healthcare, smart home and smart agriculture. This study proposes a DES based Scalable Hashing Algorithm (DESSHA) for smart devices using IoT. DESSHA due to its close alignment with theoretical values of all security test including sensitivity, confusion diffusion, uniform distribution and collision resistance with scalability. It provides message authentication for nearly all types of smart devices on IoT, especially for smart agriculture and E-Commerce purposes. Our analysis demonstrates that DESSHA provides a high level of security for message authentication for IoT enabled devices.

Keywords:-DESSHA, Cryptography, Hashing, SHA 256, Smart devices, Security of IoT.

1. INTRODUCTION

Data security has become increasingly important as computer technology has become more widely used. The use of the internet and mobile devices has increased greatly, particularly in studies in areas such as Smart devices on IoT, e-commerce, banking, finance, security, and education [1]. The advancement of technology like software defined networks [2] and software programs utilized today has made it possible for hostile consumers to intercept information at various stages of data transmission[3]. As a result, it is far more critical than ever for any company or individual to protect their sensitive and important documents. To maintain a superior line of defense, security constantly looks for how to keep information safe from unauthorized intrusion[4]. Encryption is a means of preserving data such that it remains unmodified and secure at some point throughout the transfer of information from the sender to the intended recipient [5]. Many encryption technologies have been developed to assure data security and protection [6]. To properly develop and execute security, we must be one step forward, or consider along the same lines as, cyber criminals [7]. Maintaining secrecy against

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

outsiders has always been a problem, and encryption can assist to keep exchanges of confidential messages hidden. Cryptography encompasses a wide range of procedures, such as microdots, combining words with visuals, and further inventive methods of preventing information from being captured by other parties [8]. Cryptography is used to exchange and process information safely and effectively, without a third-party interception. Encryption, hashing, and steganography are examples of such procedures [9].

Cryptographic hash functions are a method for ensuring the integrity of a document. A cryptographic hash function algorithm compresses a message to create a fingerprint for data integrity purposes [10]. Hash functions are versatile cryptographic building blocks used to ensure data validity and digital signatures. Their main fields of application are password protection, message authentication, digital signatures, certificates, and cryptocurrencies like Bitcoin [11].

The Secure Hash Algorithm (SHA), a family of cryptographic hash functions, was released in 1993 under the title Secure Hash Standard. SHA-1 input can accept up to 64 bits and output can be up to 160 bits long. Because the number of input constraints minimizes collisions that may occur when using these algorithms, this has become one of the algorithm's strengths. SHA-1 processes input in 512-bit blocks and then divides it into 16 sunblock’s of 32 bits each [12]. Because of advancements in the field of cryptography, particularly the introduction of the AES encryption standard, which offers better security with three key sizes of 128, 192, and 256 bits, the security of SHA-1 is no longer considered adequate [13]. In response, the NSA launched a project to create new hash functions with key sizes of 128, 192, and 256 bits that would provide comparable security to AES. This project resulted in the creation of the Federal Information Processing Standard hash family, which includes three new hash functions: SHA-256, SHA-384, and SHA-512 [14]. SHA-256 algorithm has two steps: preprocessing and hash computation. Padding a message and parsing the padded message into m-blocks are examples of pre-processing. The initialization values are configured to be used in the hash computation. The size of the hash value affects the security of the SHA-256 hash function [15].

Cryptographic Hash Functions serve a dual purpose: they can be used for data validation as well as user/device validation [16]. This is done by implementing digital signature schemes[17]. Without using Hash, the signature will be the same size as the message. Hash functions are widely used in backend databases not only for password management but also for index preparation, which speeds up record selection [18]. Table 1 shows currently available hashing algorithms.

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

Table 1: Existing Hashing Algorithms

Algorithm	Output size (bits)	Collision resistance	Preimage resistance	Speed
SipHash [19]	64-512	Strong	Strong	Fast
GOST [20]	256	Strong	Strong	Medium
BLAKE2 [21]	512	Strong	Strong	Fast
Whirlpool [22]	512	Strong	Strong	Medium
Tiger [23]	192	Strong	Strong	Fast
RIPEMD [24]	128-256	Weaker than SHA-256	Weaker than SHA-256	Medium
SHA-1 [25]	160	Weaker than SHA-256	Weaker than SHA-256	Fast
SHA-256 [26]	256	Stronger than SHA-1	Stronger than SHA-1	Fast
MD5 [27]	128	Weaker than SHA-1	Weaker than SHA-1	Fast

Data hiding and completeness are extremely critical. To address this issue, a combined DES and SHA-1 encryption system founded on the VC + + environment was created by Zhang et al [28]. The system offers a wide range of practicality since it uses the 3DES and RSA procedures for data encryption and the SHA-1 algorithm to confirm data integrity.

Ambedkar et al proposed an algorithm [29] each round used twenty-one steps to create a 64-bits fixed size hash code that is independent of any initial value. As a result, it is extremely difficult to reassemble the original message because no publicly known initial value was used. Logical operations are used and a three-bit circular left shift operation during hash function processes.

The paper is structured as follows: Section 2 outlines the proposed methodology, Section 3 details the experimental setup and results, and the final section contains the conclusion and suggestions for future work.

2. PROPOSED METHODOLOGY

In the current era of digitization, IoT has become the major factor to revolutionize the device automation with the use of internet. Use of IoT is spreading all over including, healthcare, home automation and in smart agriculture. These IoT devices can be controlled and operated by smart devices having low computation and memory resources. Use of sensor and actuators require high velocity of data transmission over the links. Data and commands need to be secured to avoid control, monitoring and operation of IoT devices by adversary.

In this research proposed algorithm, DES based Scalable Hashing Algorithm (DESSHA) offers highly secure cryptographic scheme to secure data transmission in terms of strong data integrity. DESSHA uses block processing mechanism of Data Encryption Standard (DES), a modern symmetric encryption algo. To maintain high security it uses expansion table, S-

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

Boxes and permutation table to deceive adversary while maintaining high security for the resource constrained IoT devices. DESSHA is able to produce secure hashes of input blocks of size as required by smart devices in any length to achieve scalability.

Figure 1: DESSHA Hashing

Figure 1 illustrates formal process of creating hash from the plaintext using DESSHA (hash function) to produce a fixed length hash (hexadecimal values). Input file is divided into blocks of 56 bits each, padded with zeroes if required.

Figure 2 illustrates the overall working of proposed framework for DESSHA, defined buffers g_1, g_2, g_3 and g_4 are initialized with particular hexadecimal values. Additionally, the corresponding g values are concatenated to form the buffers h_0 and h_1. The inputs for the block processing function are h_0, h_1, and a key. Block processing performs all the standard operations of DES including several rounds of permutations, use of S-Boxes and series of XOR operations to make it undiscoverable using usual statistical calculations.

By using the left extractor '[' and right extractor ']', it separates the left and right 32 bits of the input block. Then, by conducting XOR operations with '[' and ']', respectively, the values of h_0 and h_1 are updated. Finally, g_1, g_2, g_3 and g_4 are concatenated to create the final encrypted text $\mathcal{H}$. Using specified buffers and block processing procedures, this procedure demonstrates the conversion of input data into encrypted blocks composed of hexadecimal hash values. Depending upon the register size of device left extractor '[' and right extractor ']' is able to produce variable length of hashes as cipher text. For a resource constrained smart device with register size 16 bits or 8 bits DESSHA will produce hash of 16 bits or 8 bits. While other state of the art algorithms like SHA family lacks the flexibility to produce variable length of hashes.

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

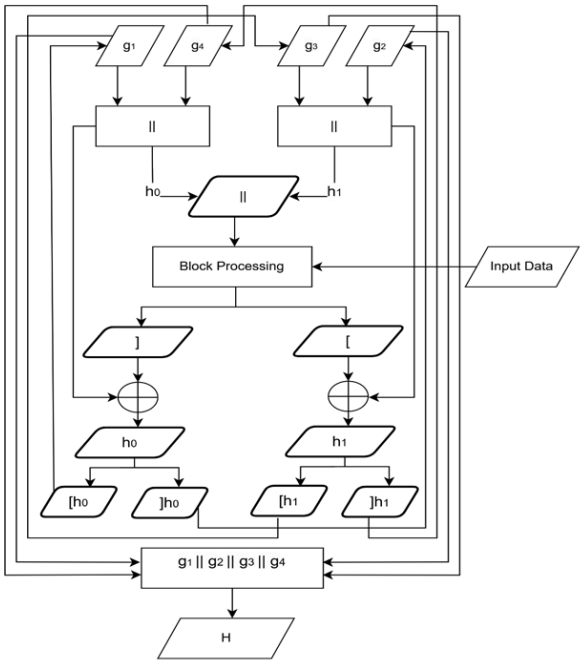

Figure 2: Proposed Framework for DESSHA

Algorithm: DESSHA

We define stream concatenation and stream extraction.

- Stream Concatenation:

Let x and y be two streams of lengths m and n respectively where $m, n \in \mathbb{Z}^+$. Concatenation operator is denoted by $||$ is defined as

$$x \,||\, y = x2^n + y$$

- Definition of Stream Left Extractor:

Let x be a bit stream x of length $2k$, where $k \in \mathbb{Z}^+$. Stream left extractor, denoted by [(left bracket), is defined as:

$$[x = \lfloor x.2^{-k} \rfloor$$

- Definition of Stream Right Extractor:

Let x be a bit stream x of length $2k$, where $k \in \mathbb{Z}^+$. Stream right extractor, denoted by] (right bracket), is defined as:

$$]x = x - 2^k.[x$$

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

Let g_1, g_2, g_3 and g_4 be same some constants.

$$h_0 = g_3 \,||\, g_2 \qquad h_1 = g_1 \,||\, g_4$$

$$h = h_o \,||\, h_2$$

let $\mathcal{B}$ defined a block processing function and b be a block

$$\rho = \mathcal{B}(b)$$

where ρ is the processed block.

$$\rho_L = [\rho$$

$$\rho_R =]\rho$$

We update g_1, g_2, g_3 and g_4 as follows

$$g_1 = [h_0$$

$$g_2 =]h_0$$

$$g_3 = [h_1$$

$$g_4 =]h_1$$

Hash digest $\mathcal{H}$ is computed as

$$\mathcal{H} = g_1 \,||\, g_2 \,||\, g_3 \,||\, g_4$$

Initial values of g_i $(i = 1,2,3,4)$ are:

$$g_1 = x6A09$$

$$g_2 = xE667$$

$$g_3 = xBB67$$

$$g_4 = xEE85$$

3. RESULTS & DISCUSSION

There are a large number of resource constrained system which necessitate the strong cyber controls. Agriculture is considered as backbone of any country. IoT has reached out to facilitate the farmers to make it smart agriculture which is composed of several sensors and actuators. Initializing it from monitoring the crop facilitates to maintain several parameters including temperature, humidity, water level, nutrient levels (nitrogen, phosphorus, and potassium), and the conditions of irrigation components (fan, watering pump, and water

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

pump. Farmers will be able to increase production of crops with smart and automated decision making from the data being generated and processed by IoT components in smart agriculture.

Due to its vital role in intelligent decision-making data is of high importance to maintain high security to protect it against malfunctioning of equipment form adversary. Agriculture possesses paramount importance in society forming foundation of food security, this research takes initiative to secure data of smart agriculture system.

3.1 Dataset:

Cryptographic hash functions are used to maintain data integrity of data being sent over the medium. In this research DESSHA is applied to a dataset *IoT Agriculture 2024* [30]. Dataset is composed of several modern sensors and controller readings recorded in smart greenhouse at Tikrit University, Iraq. The dataset includes 13 different sensor readings over 37,923 rows for better management of IoT components. Table 2 shows minimal view of the dataset.

Table 2: Dataset - IoT Agriculture 2024

date	tempreature	humidity	water_level	N	P	K	Fan_actuator_OFF	Fan_actuator_ON	Watering_plant_pump_OFF	Watering_plant_pump_ON	Water_pump_actuator_OFF	Water_pump_actuator_ON
08-02-24 6:10	41	63	100	255	255	255	0	1	1	0	1	0
08-02-24 6:15	41	59	100	255	255	255	0	1	1	0	1	0
08-02-24 6:20	41	62	100	255	255	255	0	1	1	0	1	0
08-02-24 6:05	40	60	100	255	255	255	0	1	1	0	1	0
08-02-24 6:00	39	61	100	255	255	255	0	1	1	0	1	0
18-01-24 6:02	38	64	100	255	255	255	0	1	1	0	1	0
18-01-24 6:07	38	65	100	255	255	255	0	1	1	0	1	0
18-01-24 6:12	38	64	100	255	255	255	0	1	1	0	1	0
18-01-24 5:02	37	62	100	255	255	255	0	1	1	0	1	0
18-01-24 5:07	37	63	100	255	255	255	0	1	1	0	1	0

3.2 Security Analysis

Cybersecurity of IoT devices is dependent upon the strong hashing algorithms. To assess the strength of hashing algorithm certain situations are imperative to be analyzed such as minimal changes in input to produce highly changed, random and unstructured cipher text. Following is some of the detailed criteria to evaluate effectiveness of data integrity of sensors data using DESSHA compared against theoretical values.

- Sensitivity of Hash

Sensitivity of hash is implementing single bit changes to an input message and supposed to produce altogether a highly dissimilar hash as the hash generated by original message. In our experiment DESSHA is applied to original message m_1 to compute it hash as shown in figure 3 (a). To showcase DESSHA's sensitivity single bit changes are made in m_1 in three different

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

cases: (b) flipping a single bit at random position to make it m_2; (c) insertion of single bit at random position in bit string of original message to yield m_3 and (d) deletion of single bit at random position of m_1 to produce m_4. Table 3 clearly exhibits close alignment between mean values and variances of all three situation when compared with theoretical values achieving robustness and high sensitivity of DESSHA.

In addition, all 4 sections of figure 3 demonstrates 64-bit hashes of original and modified messages. The comparison highlights the altered bit positions in the hashes, marked with an asterisk (*) at approximately 50% changed position of bits in hashes.

Table 3: Results of Sensitivity Testing

	Experimental Values			**Theoretical Values**		
	Bit Flipped	**Bit Inserted**	**Bit Deleted**	**Bit Flipped**	**Bit Inserted**	**Bit Deleted**
mean	0.4365	0.4981	0.5008	0.5	0.5	0.5
variance	0.00314	0.0043	0.0040	0	0	0

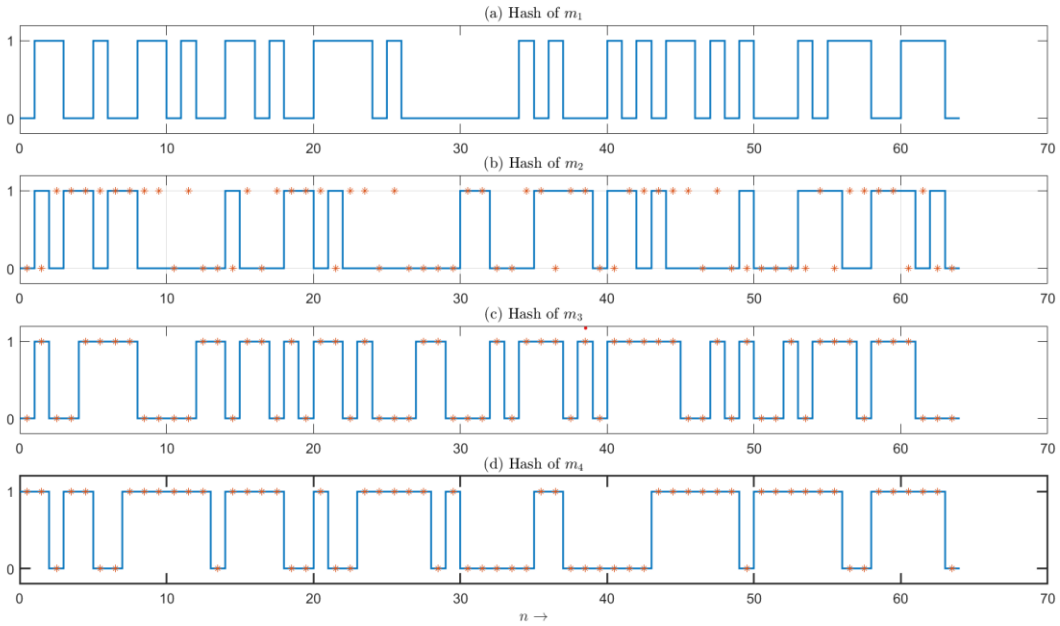

Figure 3: Sensitivity of Hashes

- Confusion Diffusion

In order to mislead the adversary, it is essential to distort the relationship between plaintext and ciphertext (confusion) and guaranteeing the slight changes in input to produce large

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

number of changes in ciphertext (diffusion). In table 4 DESSHA recurrently shows that mean of bits changed $\bar{B}$ and the mean bit change probability P are very close to theoretical values. An important factor, confusion-diffusion measure I_{dc} presenting strength of DESSHA on closely comparable values of experimental output and theoretical results.

Table 4: Confusion Diffusion Analysis

	Experimental Values	Theoretical Values
Mean of bits changed ($\bar{B}$)	27.9330	32
Mean of bit change Probability (P)	0.4365	0.5
SD of bits changed (ΔB)	11.3440	0
SD of bit change Probability (ΔP)	0.1772	0
Confusion-Diffusion Measure (I_{dc})	0.1204	0

- Uniform Distribution

Over the full bit stream of hash there are fair chances for every bit to be either 1 or 0, referred as uniform distribution. Attacker needs to process all possible options to break hash function which applies avalanche effect. In Figure 4, bit flip probabilities are very small in variance making it challenging to cryptanalyst as revealed in comparison of experimental and theoretical values.

Table 5: Uniform Distribution

	Experimental Values	Theoretical Values
Average Probability that a bit flips in hash (Q)	0.5005	0.5
$\|Q - 0.5\|$	0.0635	0
SD Probability that a bit flips in hash (ΔQ)	0.0055	0

Smaller the $|Q - 0.5|$ and ΔQ, better is the avalanche effect.

Directing to table 5 the average probability of bit flips Q is nearly identical to the theoretical value of 0.5, which is proving uniform distribution. The minimal deviation $|Q - 0.5|$ and low standard deviation of bit flip probability ΔQ highlight the consistency and effectiveness of the system's avalanche effect.

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

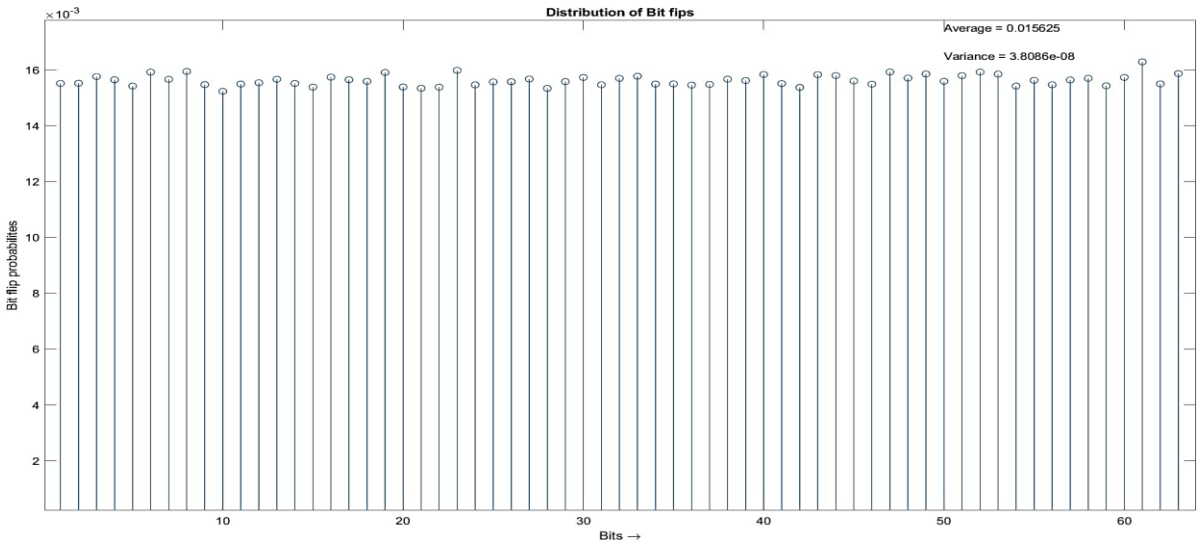

Figure 4: Uniform Distribution

- Collision Resistance

The major challenge in hash function is to guarantee computationally impractical to produce identical hash for any two distinct inputs. In figure 5, DESSHA's probability distribution is compared with theoretical predictions. There is very small difference between experimental and theoretical values which makes our algorithm highly resistant to collision. Consequently, proving it highly secure for the IoT devices to preserve data integrity.

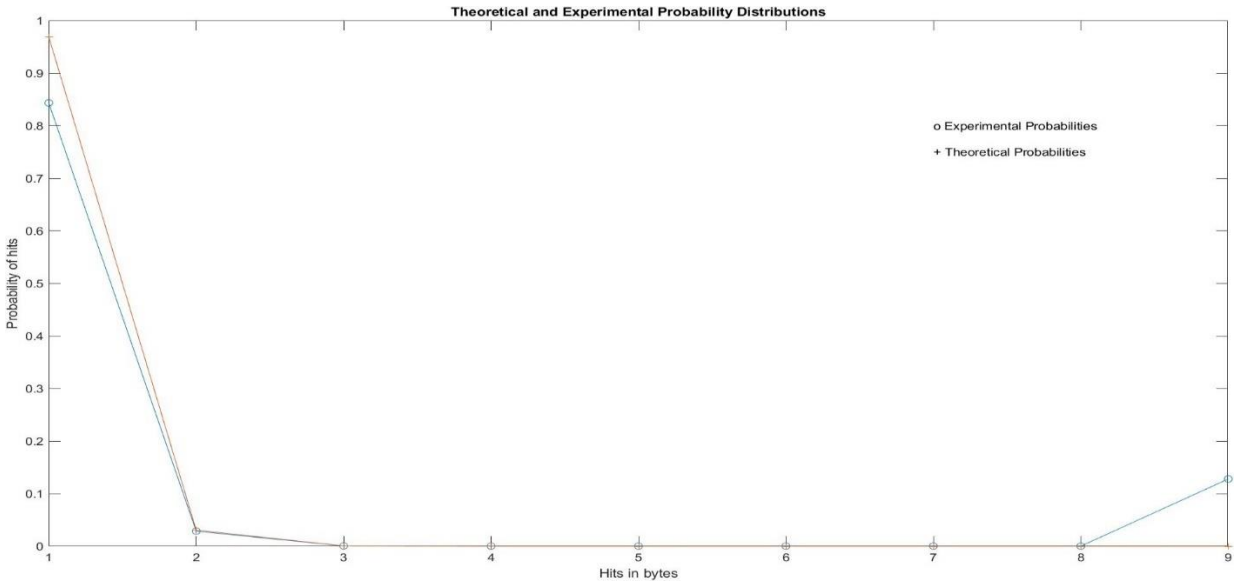

Figure 5: Collision Resistance

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

the uniform distribution property of a hash function could be evaluated using |Q−50%|

Bhattacharya distance is a statistical measure to quantify the similarity or dissimilarity between two probability distributions, expressed as $D = (P^e||P^t)$ where P^e is probability distribution achieved on experimental setup whereas P^t is theoretical probability distribution. Smaller the value of D better the strict avalanche effect achieved that is $D = 0.0684$.

The absolute difference per byte between hash of original message $\mathcal{H}$ and hash of modified message $\overline{\mathcal{H}}$ can denoted as D_{byte}. Using DESSHA we obtained mean of D_{byte} as $\overline{D}^e_{byte} = 74.5496$ which is very close to mean of theoretical value as $\overline{D}^t_{byte} = 85.33$ that shows that DESSHA is capable of collision resistance.

3.3 Scalability

Let m represent the register size of any IoT device. Scalability enables the computation of hash values up to a size of 64n ≤ m, where n denotes the scalability factor. Our test results demonstrate that our proposed algorithm exhibits scalability, making it suitable for deployment across a wide range of smart devices in IoT. This scalability advantage is particularly noteworthy when compared to SHA-1 and SHA-256, which lack scalability. Figure 6 illustrates the comparison of DESSHA (Scalable), SHA-1 (Fixed), and SHA-256 (Fixed) hash sizes in the context of a 64-bit register. DESSHA demonstrates linear scalability, whereas SHA-1 and SHA-256 maintain constant hash sizes of 160 bits and 256 bits, respectively.

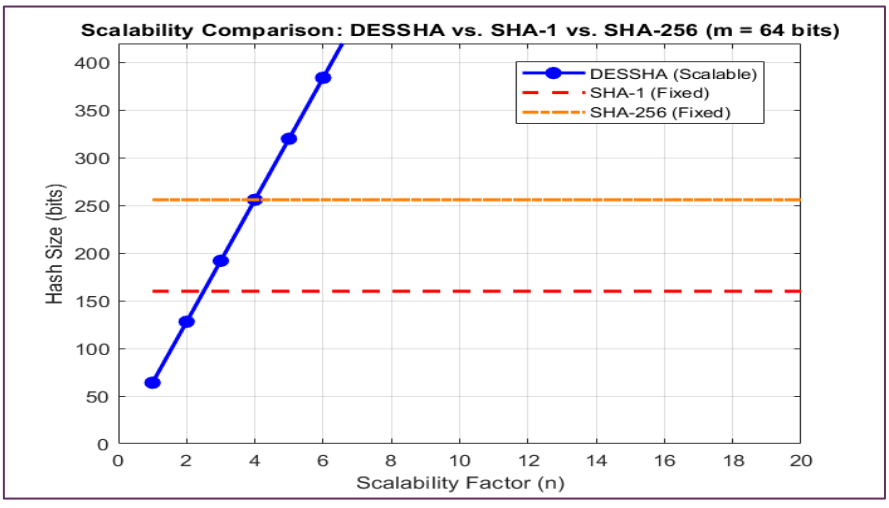

Figure 6: Visualization of Scalability in DESSHA vs SHA-1 vs SHA-256

4. Conclusion and Future Work

In the age digitalization and automation cybersecurity has become obligatory and challenging job. Data is being generated and sent at very large speed in IoT systems. Cryptographic hash

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

functions are one of the perfect security mechanisms to keep information safe. In this research a novel algorithm DESSHA is proposed which resistant to many statistical attacks and scalable to many smart devices. DESSHA is useful in message authentication for various types of smart devices, specifically for smart agriculture and E-commerce purposes. Our analysis presents that DESSHA has an ability to secure message with level of effectiveness closely aligned to theoretical approach in hash sensitivity, confusion diffusion, uniform distribution and collision resistance.

As the deployment of IoT systems are increasing everyday more security will be needed. DESSHA contributes its effectiveness on several type of IoT systems including smart home, healthcare as well as in industrial control systems in future.

References:

[1] S. K. Bhatti, M. I. U. Lali, B. Shahzad, F. Javid, F. U. Mangla, and M. Ramzan, "Leveraging the Big Data Produced by the Network to Take Intelligent Decisions on Flow Management," *IEEE Access*, vol. 6, pp. 12197–12205, 2018, doi: 10.1109/ACCESS.2018.2808358.

[2] M. I. Lali, M. M. Bilal, M. S. Nawaz, M. Deen, B. Shahzad, and S. Khaliq, "Effect of Input-Output (IO) Buffering to Minimize Flow Control Blocking in Software Defined Networking," *The Nucleus*, vol. 53, no. 3, Art. no. 3, Sep. 2016.

[3] P. Liang, L. Yang, Z. Xiong, X. Zhang, and G. Liu, "Multi-Level Intrusion Detection Based on Transformer and Wavelet Transform for IoT Data Security," *IEEE Internet Things J.*, pp. 1–1, 2024, doi: 10.1109/JIOT.2024.3369034.

[4] "Hybrid homomorphic-asymmetric lightweight cryptosystem for securing smart devices: A review - Mathews - 2024 - Transactions on Emerging Telecommunications Technologies - Wiley Online Library." Accessed: Mar. 21, 2024. [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/ett.4866

[5] "Efficient chaos-based image encryption approach for secure communication." Accessed: Mar. 21, 2024. [Online]. Available: https://www.spiedigitallibrary.org/journals/journal-of-electronic-imaging/volume-30/issue-2/023026/Efficient-chaos-based-image-encryption-approach-for-secure-communication/10.1117/1.JEI.30.2.023026.short#_=_

[6] S. Ameer, J. Benson, and R. Sandhu, "Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 5, pp. 4032–4051, Sep. 2023, doi: 10.1109/TDSC.2022.3216297.

[7] "An Efficient Privacy-Preserving Credit Score System Based on Noninteractive Zero-Knowledge Proof | IEEE Journals & Magazine | IEEE Xplore." Accessed: Mar. 21, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/9312961

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

[8] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet Things*, vol. 22, p. 100759, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[9] J. Liu, Y. Wang, Q. Han, and J. Gao, "A Sensitive Image Encryption Algorithm Based on a Higher-Dimensional Chaotic Map and Steganography," *Int. J. Bifurc. Chaos*, vol. 32, no. 01, p. 2250004, Jan. 2022, doi: 10.1142/S0218127422500043.

[10] S. McKeown, P. Aaby, and A. Steyven, "PHASER: Perceptual hashing algorithms evaluation and results - An open source forensic framework," *Forensic Sci. Int. Digit. Investig.*, vol. 48, p. 301680, Mar. 2024, doi: 10.1016/j.fsidi.2023.301680.

[11] S. Gangadharaiah and P. Shrinivasacharya, "Secure and efficient public auditing system of user data using hybrid AES-ECC crypto system with Merkle hash tree in blockchain," *Multimed. Tools Appl.*, Feb. 2024, doi: 10.1007/s11042-024-18363-0.

[12] 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 SECURE HASH ALGORITHM (SHA) FAMILY," *Malays. J. Comput. Sci.*, vol. 35, no. 3, Art. no. 3, Jul. 2022, doi: 10.22452/mjcs.vol35no3.1.

[13] "Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications | IEEE Journals & Magazine | IEEE Xplore." Accessed: Mar. 22, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9923931

[14] S. Zhou, P. He, and N. Kasabov, "A Dynamic DNA Color Image Encryption Method Based on SHA-512," *Entropy*, vol. 22, no. 10, Art. no. 10, Oct. 2020, doi: 10.3390/e22101091.

[15] B. Rahul, K. Kuppusamy, and A. Senthilrajan, "Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm," *Multimed. Tools Appl.*, vol. 82, no. 28, pp. 43729–43758, Nov. 2023, doi: 10.1007/s11042-023-15289-x.

[16] S. K. Bhatti, K. M. Aamir, and M. Deriche, "A Scalable DES Based Hashing Algorithm," in *2023 24th International Arab Conference on Information Technology (ACIT)*, Dec. 2023, pp. 1–5. doi: 10.1109/ACIT58888.2023.10453719.

[17] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput. Appl.*, vol. 32, no. 3, pp. 639–647, Feb. 2020, doi: 10.1007/s00521-018-3915-1.

[18] N. Andola, S. Prakash, V. K. Yadav, Raghav, S. Venkatesan, and S. Verma, "A secure searchable encryption scheme for cloud using hash-based indexing," *J. Comput. Syst. Sci.*, vol. 126, pp. 119–137, Jun. 2022, doi: 10.1016/j.jcss.2021.12.004.

[19] Z. Niu, S. Sun, Y. Liu, and C. Li, "Rotational Differential-Linear Distinguishers of ARX Ciphers with Arbitrary Output Linear Masks," in *Advances in Cryptology – CRYPTO*

Power System Technology
ISSN:1000-3673
Received: 22-05-2024 Revised: 05-06-2024 Accepted: 22-06-2024

2022, Y. Dodis and T. Shrimpton, Eds., Cham: Springer Nature Switzerland, 2022, pp. 3–32. doi: 10.1007/978-3-031-15802-5_1.

[20] A. Sadeghi-Nasab and V. Rafe, "A comprehensive review of the security flaws of hashing algorithms," *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 2, pp. 287–302, Jun. 2023, doi: 10.1007/s11416-022-00447-w.

[21] S. Atiwa, Y. Dawji, A. Refaey, and S. Magierowski, "Accelerated Hardware Implementation of BLAKE2 Cryptographic Hash for Blockchain," in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Aug. 2020, pp. 1–6. doi: 10.1109/CCECE47787.2020.9255709.

[22] Z. Zhang, S. Sun, C. Wang, and L. Hu, "Classical and Quantum Meet-in-the-Middle Nostradamus Attacks on AES-like Hashing," *IACR Trans. Symmetric Cryptol.*, vol. 2023, no. 2, Art. no. 2, Jun. 2023, doi: 10.46586/tosc.v2023.i2.224-252.

[23] S. Malaysha, M. Moreb, and A. Zolait, "Detecting Network Traffic-based Attacks Using ANNs," *Int. J. Comput. Digit. Syst.*, vol. 13, no. 1, pp. 131–137, Jan. 2023, doi: 10.12785/ijcds/130110.

[24] G. Wang, F. Liu, B. Cui, F. Mendel, and C. Dobraunig, "Improved (semi-free-start/near-) collision and distinguishing attacks on round-reduced RIPEMD-160," *Des. Codes Cryptogr.*, vol. 88, no. 5, pp. 887–930, May 2020, doi: 10.1007/s10623-020-00718-x.

[25] A. Koutra and V. Tenentes, "Multi-Vt-Based Energy Efficiency Optimization for ASIC Designs of the Double Secure Hash Algorithm Toward a Sustainable Bitcoin Network," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 71, no. 3, pp. 1596–1600, Mar. 2024, doi: 10.1109/TCSII.2024.3350035.

[26] T. Sureshkumar, R. Sivaraj, and M. Vijayakumar, "Design and implementation of a framework for blockchain based security using IoT," *J. Intell. Fuzzy Syst.*, vol. 44, no. 1, pp. 905–918, Jan. 2023, doi: 10.3233/JIFS-220366.

[27] A. Renklier and S. Öztürk, "Image authentication and recovery: Sudoku puzzle and MD5 hash algorithm based self-embedding fragile image watermarking method," *Multimed. Tools Appl.*, vol. 83, no. 5, pp. 13929–13951, Feb. 2024, doi: 10.1007/s11042-023-15999-2.

[28] J. Zhang and X. Jin, "Encryption system design based on DES and SHA-1," *Proc. - 11th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. DCABES 2012*, pp. 317–320, 2012, doi: 10.1109/DCABES.2012.42.

[29] N. Bisht, B. Pandey, and S. K. Budhani, "Comparative performance analysis of AES encryption algorithm for various LVCMOS on different FPGAs," *World J. Eng.*, vol. 20, no. 4, pp. 669–680, Jan. 2022, doi: 10.1108/WJE-05-2021-0281.

[30] "Smart_Irrigation_system." Accessed: March. 15, 2024. [Online]. Available: https://kaggle.com/code/manjunadh7117/smart-irrigation-system