Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things

Monika Parmar[1]
Chitkara University School of Engineering and Technology
Chitkara University, Himachal Pradesh, India

Harsimran Jit Kaur[2]
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

***Abstract*—Cryptography algorithms play a vital role in Information Security and Management. To test the credibility, reliability of metadata exchanged between the sender and the recipient party of IoT applications different algorithms must be used. The hashing is also used for Electronic Signatures and based on how hard it is to hack them; various algorithms have different safety protocols. SHA-1, SHA-2, SHA3, MD4, and MD5, etc. are still the most accepted hash protocols. This article suggests the relevance of hash functions and the comparative study of different cryptographic techniques using blockchain technology. Cloud storage is amongst the most daunting issues, guaranteeing the confidentiality of encrypted data on virtual computers. Several protection challenges exist in the cloud, including encryption, integrity, and secrecy. Different encryption strategies are seeking to solve these problems of data protection to an immense degree. This article will focus on the comparative analysis of the SHA family and MD5 based on the speed of operation, its security concerns, and the need of using the Secure Hash Algorithm.**

Keywords*—*Blockchain Technology; IoT; Secured Hash Algorithms; IoT Security; SHA; MD5

I. Introduction

The Internet of Things is a connecting network of multiple things that are not only connected to one other but are also connected to the Internet. The basic services of IoT are rapidly increasing owing to its enormous range of applications by providing scalable solutions with lowered expenditure [1]. These scalable solutions always need fast and efficient authorization, information protection, confidentiality, intrusion responsiveness, fast implementation, and self-maintenance. Through implementing blockchain technology, certain specifications can be provided to the IoT solution of a business.

Blockchain is a program with a vast variety of implementations, typically related to cryptography. Besides that, it has subsequently been recently implemented as a distributed and permanent ledger that enables the phase of transfer registration and consultation. One should think about transactions happening in banking sectors as blockchain network transactions as a hypothetical example [2]. These days, to transact currency, the individual is dependent on banking and perhaps other reputable financial institutions. The payment respondents confirmed that the entity handling the transfer has the requisite infrastructure to ensure that it is conducted efficiently and, quite notably, in a secure way. Besides that, as in the event of unforeseen failure, these intermediate institutions can collapse and therefore the faith is violated and so will be the transactions and products entrusted to them [3]. In distributed ledger technology, the confidence element is taken into account through the use of encrypted structures to include the statistical evidence of the total transaction performance. This testimony is unequivocally valid that the members in a blockchain are equipped with safety and integrity.

IoT systems can exchange data with others, to improve the knowledge of all members of the network and the surroundings. The IoT operation consists of a mixture of Interconnection, actuators, programmable controllers, and sensors [4]. Methods of a certain level IoT are applied at a quick speed with ideas such as smart homes, smart cities, and wearable devices which map out their characteristics prospective and efficient usage. Provided that blockchain is a hierarchical ledger system and also the IoT framework is naturally decentralized, it can be concluded that, in a real possibility, their synergy can be advantageous, thereby adding to the protection and accountability of IoT transactions. In view to improve the effectiveness of applications, Blockchain uses a technology in which computers consume large quantities of resources and processing power. IoT, on the contrary, is a network of objects that usually have a comparatively fewer number of resources, but it may even be of significant impact to merge these solutions [5]. The goal of this study is to explain the application of blockchain technologies in IoT applications, and even the effect on resource-constrained systems of many hash functions. At first, as we seek to explain how the system performs and the mechanisms involved, the blockchain concept will be explored in specific. This study investigated certain hashes methods that have been submitted by academics, but the majority of them have not been checked against blockchain and IoT threats. Section II summarizes the literature review of cryptographic hash functions in blockchain technology. Section III introduces the Blockchain technology and Cryptographic Hash functions, Section IV addresses the potential threats in blockchain and IoT, Blockchain Implementation to IoT is depicted in Section V, Section VI analyzes the proposed scheme for an effective hash function, and Section VII comprises the result and conclusion.

II. Literature Review

Zeyad et al. [6] suggested the Pros and Cons of the optimization techniques and the impact on the performance level by performing experimental setup for SHAs by FPGA optimization methods.

B.P. Kosta et al. [7] demonstrated a Strong and a Secure lightweight cryptographic hash function is proposed in which each 512-bit of a data is compressed to 256-bit. Afterward, it is divided further into 8 blocks having 32-bits each.

F. Pfautsch et al. [8] validated the SHA-1 and SHA-3 hash functions because of the brute force threats on UltraScale+ FPGA dual-core systems. They have evaluated the passwords with 6 characters in 3 minutes time span and because of high complexity, the time raises by 5.5 for the SHA-3 Hash Algorithm.

N. Khan et al. [9] surveyed a thorough and in-depth survey of traditional authentication and the hash function is performed in this article, supported by a reasonable contrast of the period and computer processes usage of such methodologies.

C. White et al. [10] suggested Blockchain technology and picture hashes are used to create an image verification system. The concept developed in this paper, however, needs to be refined, as it tends to strive in some circumstances. This research demonstrates whether blockchain can be used to authenticate images, especially through picture hashing. Other findings provide the fact that in certain instances, utilizing adjacent frames hash operations around the same time will enhance efficiency, but that each type of cryptocurrency experiment will have its own distinct set of data.

Table I and Table II summarize the literature review for the given context.

III. Blockchain Technology and Cryptographic Hash Functions

A Peer to Peer network may be a decentralized computing model if any of its technical services, such as computing power, space, and scanners, are shared by its members. To provide the infrastructure and information provided on the platform, these common services are essential. Blockchain is a distributed platform with no data analysis resources and no users to order them [12]. A node, therefore, depicts a system member. Every member has the authority to function as a server as well as the client, leading to the absence of a hierarchical system between them and providing the identical function in all networks. A protection scheme should be perceived when blockchain technology is decentralized because, unlike a centralized system where there is a single point of failure, is not the case here and can be targeted, thus it is tougher to interpret the information. This characteristic, even then, is not adequate to secure information passes through the system security and reliability. Blockchain is based on encryption to accomplish that. Generally, the cryptographic hash functions are of various types that provide different bit values depending on the type of hash and the same is depicted in Fig. 1.

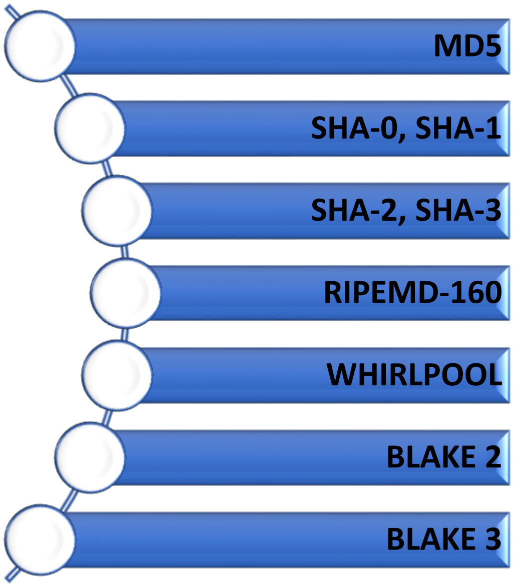


Fig. 1. Types of Cryptographic Hash Function.

Typically, two cryptographic methods are used for the blockchain framework: private and public key for the hash functions. The public key, which confirms the authenticity of whoever made the transfer, has to be used for exchanges to be digitally authenticated. It relies on a key to encipher and a dissimilar key to decipher [13]. Two very different keys are conceptually difficult to find, understanding only the encryption techniques used to produce them. This ensures the security and authenticity of the information if somebody confirms their transfer through its secret key since decrypting is only primarily driven by that of the hash value that is public in nature.

When the decoding results are positive, clients realize that the author of the secret key is someone who validated the agreement, and the information is not compromised or altered, else the decoding will not be efficient. The conversion of some form of data into a sequence of words is translated by these mechanisms. The same knowledge will still lead to almost the same key, and the slightest shift in the source information will create a hash that varies from the previous one. It's a minor processing operation to create a hash, but the reverse does not occur. It is virtually impossible to execute the reverse process to retrieve the actual data once the hash data is known [14]. As soon as the new block is generated, these hash functions are being utilized to confirm the block. Each block is connected to the previous block with the hash key and if someone wants to intrude in between, the hash value will change and will no longer be the same value in the blockchain. So there the frauds can be detected. hen an intruder happens to alter a block that is a member of a blockchain, together with its key, its value will alter in that way that this will not fit with the hash value present over the upcoming block in the chain.

The SHA functions in the SHA family comprise SHA-0, SHA-1, SHA-2, and SHA-3; while there are functionally distinct ones from that very same group. SHA-0 had several bugs and was not very common So, SHA-1 was subsequently developed in 1995 to fix suspected SHA-0 vulnerabilities. Of the current SHA algorithms, SHA-1 might be the most commonly used one for SSL authentication. It has many variations in bits, for example, SHA-224, SHA-256, SHA-384, and SHA-512. It is based on the number of hash bits in the hash function. However, SHA-2 is a good cryptographic algorithm but it follows the same architecture as SHA-1 [15]. NIST introduces another algorithm that is Keecak algorithm considered as the SHA-3 Hash function. It presents various advantages, including efficient quality and reasonable tolerance for threats.

However, SHA-2 is a good cryptographic algorithm but it follows the same architecture as SHA-1. NIST introduces another algorithm that is Keecak algorithm considered as the SHA-3 Hash function. It presents various advantages, including efficient quality and reasonable tolerance for threats.

IV. Potential Threats in Blockchain and IoT

Each technology comes with its pros and cons so is blockchain technology. Several threats that deal with blockchain technology include double-spending threats, threats involved in mining, threats in wallets, threats based on the network, and threats in the smart contracts. Each above mentioned has many threats/attacks associated with it that can have a significant impact on the blockchain network and is shown in Fig. 2. Whenever a network infrastructure is affected, a double-spending threat can occur and virtual currency is generally seized. To make it appear valid, the hacker will indeed send a duplicate copy of the currency or could expunge the transfer of funds entirely. However, it is not widespread, double-spending does happen. This type of threat includes a 51% attack in which a node miner or team of miners on a public ledger tries two times to invest one's digital currency on that public ledger [16]. They are trying to invest twice in them; thus, the title double-spending attack is given. This is not always aimed at doubling crypto spending, but almost always discrediting a particular crypto or blockchain technology by influencing its credibility.

It informs us that more successful clustering power contributes to greater protection against a 51 percent attack while testing the Proof of Work (PoW) algorithm [17]. However, small-size blockchains that run on PoW could be slightly more prone to this kind of attack, given that the intruder does not cope with even more computing power which is the reason that 51% of attacks tend to happen on smaller blockchains whenever these occur in any way. The Bitcoin blockchain still hasn't experienced a 51 percent intrusion yet.

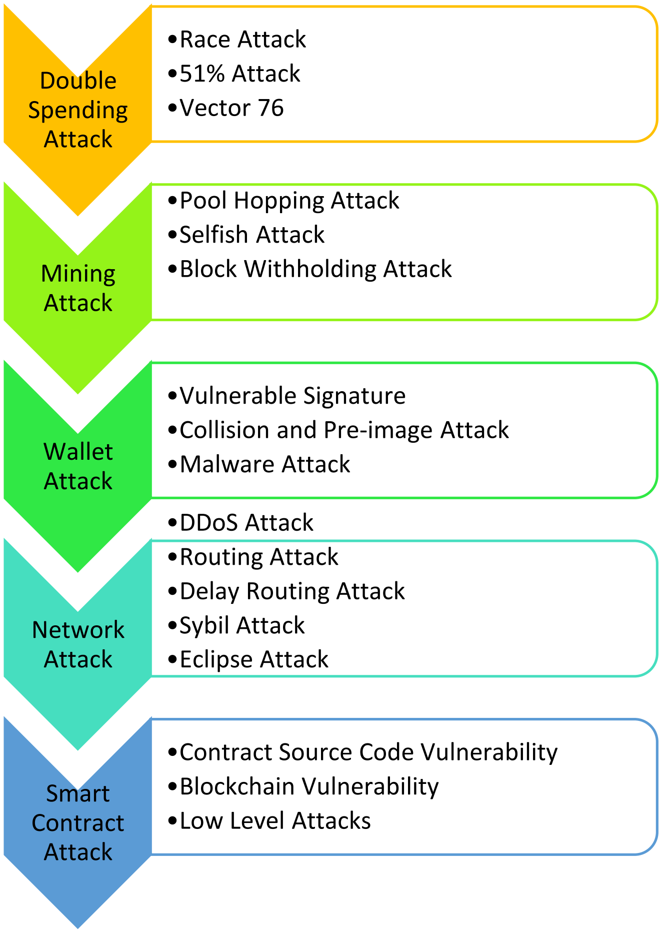


Fig. 2. Threats at Blockchain Levels.

Whenever an intruder makes two opposing transfers, a race attack will be launched. The first-ever transfer would be sent to the individual who, instead of any wait for clarification of the transfer, confirms the transfer (and delivers a service, for example). At the same instance of time, a different transfer is distributed to the server that returns the equal amount of digital currency to the intruder, ultimately rendering the very first transactions null. A decentralized wallet that helps customers to exchange and handle cryptocurrency, as well as ether, is called a blockchain wallet. This wallet is created by Blockchain which is an e-wallet that helps users to manage and move bitcoins [18]. A pre-image threat on cryptographic operations in hashing aims to locate a document that seems to have a particular hash code. A hash of cryptography can withstand threats upon the pre-image. Network attacks include DDoS attacks, Sybil attacks, Routing threats, etc. In general, a DDoS attack may burden a network with new chunks of information inside a network, which would compel a blockchain to function slowly to use its computing capacity. It is a Denial-of-Service intrusion and is a tactic to interrupt connectivity to a network interface or internet platform by normal nodes. Usually, this is done by overburdening the endpoint with a large amount of activity or by injecting fake requests that enable the targeted system to fully fail or collapse. Sybil attacks are prominent in P2P systems where several nodes are successfully run simultaneously by a network interface and compromise the power in credibility schemes [19]. The primary purpose of this threat is to obtain the bulk of the power in the systems to enable unlawful acts in the framework. Such numerous false profiles tend to be legitimate specific attributes for the system. The absence of smart contract technology requirements passes more of the pressure to the organization as it opens its connection details to possible damage. As when the event reveals, the contract applied cannot reflect the agreeing partners' real purpose. In IoT, some architectural levels layers include the Physical layer, Network layer, Middleware, and Application layer [20]. On each layer of IoT, there are different threats and are shown in Fig. 3.

As IoT is growing at a rapid so its challenges include security issues in many IoT applications, it is cost and traffic, increased load capacity on Cloud Service and services insufficiently, Issues in System infrastructure/Architecture, and manipulating information [21]. Table I shows the challenges towards IoT applications, various attacks included, and the possible blockchain solution for the same.

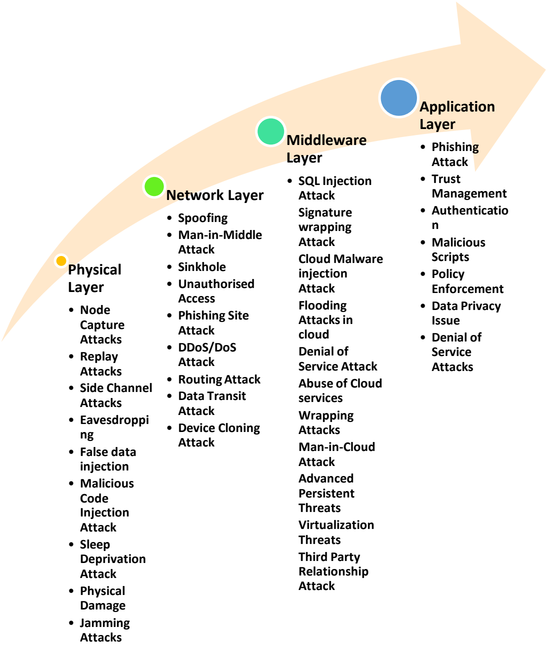


Fig. 3. Security Threats at IoT Architectural Levels.

TABLE I. CHALLENGES OF IOT APPLICATIONS AND THE POSSIBLE BLOCKCHAIN SOLUTION

Challenge Towards IoT	Inclusion Attacks	Specification	Possible Blockchain Solution
Security Issues in IoT Applications	• Node Capturing • SQL Injection Attacks • Man-In-Middle-Attack • Data Thefts • Sniffing Attacks	IoT applications are prone to exposure to personal information.	For this issue, permission type blockchain can be used that can enhance security[15].
Cost and Traffic	• Phishing Site Attack • Booting Attacks • Data Transit Attacks • Routing Attacks • Access Control Attack	To handle exponential growth in IoT devices	It can be solved by the decentralization feature of the blockchain. In this, central servers are not being used as every node can directly communicate to each other [27] [28] [29].
Increased load capacity on Cloud Service and services insufficiently	• DDoS/DoS Attack • Firmware Updates • Service Interruption Attacks • Flooding Attack in Cloud	Owing to security issues/threats or the attacks on the cloud, the services from the cloud discontinues	Each file is updated separately as a ledger on every node/device on the network so single point failure is not possible in such a case [31].
Issues in System infrastructure/Architecture	• Side-Channel Attacks • Eavesdropping and Interferences • Sleep Deprivation Attacks • Secure On-Boarding • Extra Interfaces • Reprogram Attacks	Every section in IoT are prone to single point failure and it affects the systems and whole infrastructure	Verification of data is done with the help of encryption techniques utilizing the blockchain[28].
Manipulating Information	• False Data Injection Attack • Malicious Code Injection Attack • Access Attack • Signature Wrapping Attack • End-to-End encryption	Information is deliberately taking out from IoT units and manipulating the information maliciously.	A blockchain ledger is updated at every node so if there is any malicious node that updates the information, other nodes will decline that[30].

V. Blockchain Implementation to IoT

Today many IoT implementations rely on a centralized server/client model, in which clients link across the Network to services virtualized on to the cloud. While these methods are feasible, as IoT expands a new mechanism is required. Decentralized alternatives have been suggested yet Peer to Peer alone cannot assure security and confidentiality [32]. Blockchain has the power to respond to a number of the problems that come from the use of IoT: IoT implementations are costly because of the expense of central server management in the cloud. To improve protection and loyalty, accountability is important. An open-source approach is desired and should be considered in the development of the next version of IoT products. Since IoT usually requires a central agency, the central level failure problem is prevalent. Factors such as time synchronization, registries, anonymity, and reliability are tough to control reliably [33]. IoT applications are renowned for moderate computational power and also energy efficiency. This system may not be able to use the highest cryptographic algorithms since it takes much longer to access. As per storage is concerned, all nodes hold a backup of all dealings which has existed in the database since its development. The scale would grow as time has gone through or IoT devices might not even be capable of storing it [34]. The problems of ledger extended to IoT originate in its minimal investment. Although the computing capacity is limited, these machines can still execute activities as long as protocols and frameworks designed for them are utilized [35].

So, hash algorithms have to be checked thoroughly for their performance level. A comparative analysis of blockchain and IoT-based systems is being presented in Table II.

TABLE II. A Comparative Analysis of an Existing Survey on Blockchain and IoT based Systems

**** represents covered partially, ✔ represents covered in detail, and ✗ represents not covered in the literature**

Application Criteria	Year of publication	Major Inclusion	Considered Factors	Discussion on Storage Issues	Discussion on Security Issues
Blockchain-based IoT applications	2019 [11]	Overview of Opportunities and challenges of IoT and Blockchain is provided	• Interoperability • Security and privacy of IoT	**	**
	2018[12]	Detailed discussion on blockchain techniques, applications, and challenges	• Consensus algorithms • Security issues in blockchain	✗	✔
IoT storage optimization	2017[13]	A detailed analysis of optimizing the level of performance in distributed storage onto the cloud.	• Improvement in transmission efficiency. • Distributed cloud storage • The adaptive network coding scheme	✔	✗
	2020[14]	An in-depth approach for optimizing the data access storage architecture in the Internet of Things, in which factors of data access storage distribution are fully considered, and secured hashing is being used to configure the data for storage optimization.	• Data processing efficiency • Time consumption for reading the files • File download efficiency	✔	✗
Blockchain-based IoT storage optimization	2017[15]	A brief discussion on lightweight BC-based architecture for IoT that virtually eliminates the overheads of classic BC.	• Block validation processing time • PoW • BC-based smart home	✔	**
	2019[16] [26]	An investigation about lightweight blockchain management with a superior reduction in resource usage and also save the significant information about IoT framework.	• WSN • CPS • PoS consensus mechanisms • Mobility based blockchain management	✔	✗
Blockchain for IoT security	2017[9] [23] [24]	A comprehensive case study of smart home	• Security analysis • DDoS attack • Packet overhead • Energy consumption	✗	✔
	2020[18] [25]	Detailed insights of a software-defined blockchain architecture to realize the configurations for blockchains. Also, a consensus function virtualization approach with application-aware workflow is proposed.	• Consensus algorithms • SDN • Throughput of transactions • Energy consumption • Consensus switch accuracy	✗	✔
Security issues of IoT	2019 [17] [19]	A comprehensive survey of security, issues, challenges, and considerations of IoT	• Physical attacks • Networks attacks • Software attacks • Encryption attacks	✗	✔

	2020 [21] [22] [36]	A discussion about security, privacy, and trust in the Internet of Things	• Secured middleware • Mobile security in IoT • Public key cryptography (PKC)	✗	✔
Comparative analysis of a secured hash algorithm for IoT applications	This article	Detailed insights about cryptographic hash algorithms for Blockchain and IoT	• Threats to IoT • Performance checks for various cryptographic algorithms • The practical applicability of blockchain • Secured strategies	✔	✔

VI. Proposed Scheme for Effective Hash Function

In the proposed scheme, three levels of comparison are being carried out that is based on the output size bits of the hash algorithm, size of the file and time to execute these files through a hash function, and based on the speed performance of various hash algorithms. Six different iterations are taken to compare the time execution of hash algorithms. For the six iterations, two major cases are being taken that include a short sequence of data that is to be hashed and a large sequence of data that is to be hashed and the comparison is in between MD5, SHA-1, SHA-256, and SHA-512. Fig. 4 depicts the three levels of comparison for the hash algorithm.

Based on the output size (in bits), different hash algorithms are analyzed. It is depicted in Fig. 5 that the more the number of hash bits, the higher the security. So, from this, it is shown that SHA-512 and SHA-256 have comparable output bits.

Also, the file size for execution is an important factor while deciding the secured hash algorithm. For a file of size 1KB, 5Kb, and 10 KB, the time taken for execution is depicted in Fig. 6 below. So, for large-size files, SHA1 is taking less time as compared to SHA2 and SHA3.

Also, hash algorithms can be compared based on their speed, and accordingly, a particular hash is selected. In this, six iteration were taken for the two major cases and that includes a small sequence having immutable universally unique identifier string, immutable universally unique identifier including system current time, and random immutable universally unique identifier with system current time and large sequence that will include two immutable universally unique identifiers, two immutable universally unique identifier with current system time, and three random immutables universally unique identifier with current system time. The setup is implemented in java with these six iterations and outcomes from several samples are collated and evaluated. There are six primary instances and are mentioned in Table III.

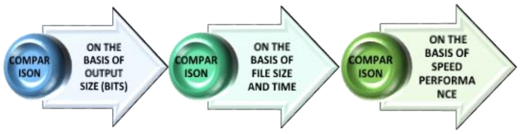

COMPAR ISON
ON THE BASIS OF OUTPUT SIZE (BITS)
COMPAR ISON
ON THE BASIS OF FILE SIZE AND TIME
COMPAR ISON
ON THE BASIS OF SPEED PERFORMA NCE

Fig. 4. Three Levels of Comparison of Hash Algorithms.

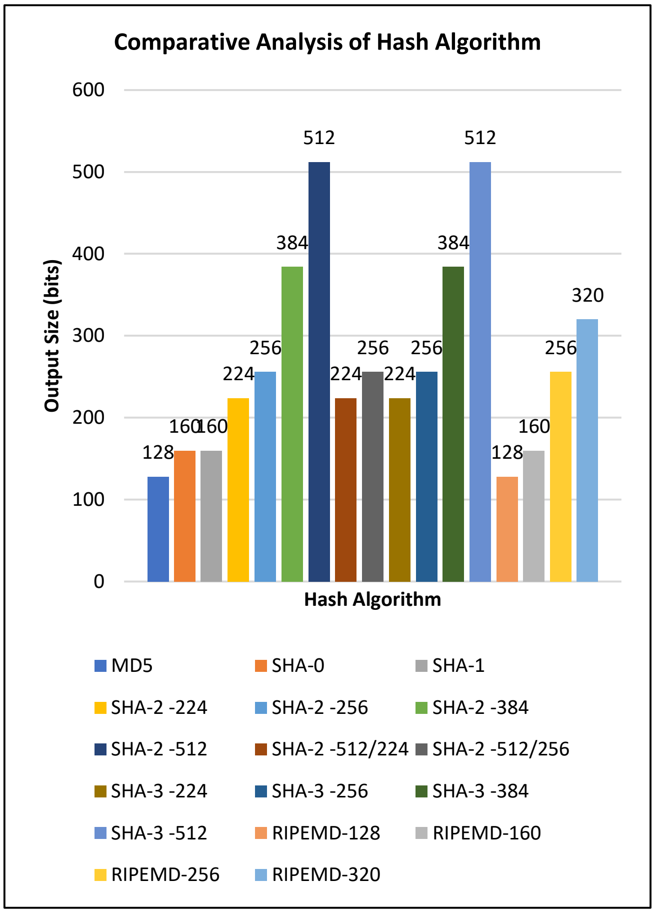
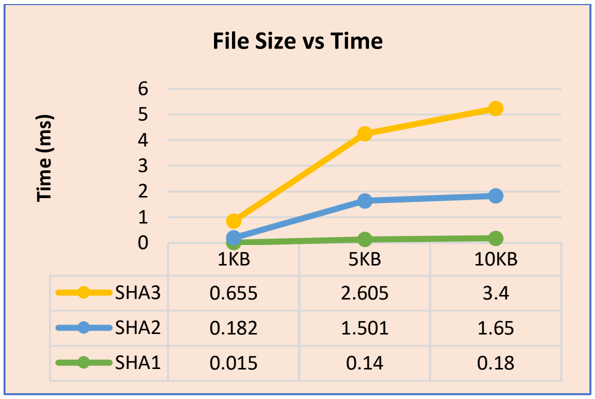


Fig. 5. Comparative Analysis of Hash Algorithm based on Output Size (Bits).



	1KB	5KB	10KB
SHA3	0.655	2.605	3.4
SHA2	0.182	1.501	1.65
SHA1	0.015	0.14	0.18

Fig. 6. Comparative Analysis of Hash Algorithms based on File Size.

TABLE III. SIX ITERATIONS EXECUTION TIME FOR SMALL AND LARGE SEQUENCE

	SMALL SEQUENCE (ms)			LARGE SEQUENCE (ms)		
HASH ALGORITHM	**ITERATION 1**	**ITERATION 2**	**ITERATION 3**	**ITERATION 4**	**ITERATION 5**	**ITERATION 6**
MD5	542	715	1425	798	892	1606
SHA-1	458	466	1146	601	716	1319
SHA-256	513	492	1120	639	750	1339
SHA-512	379	469	1172	593	750	1349

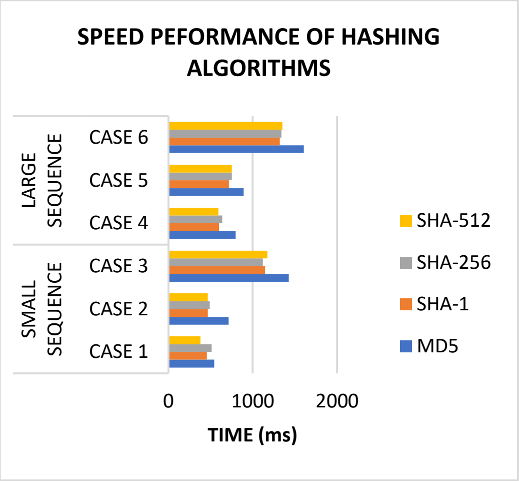


Fig. 7. Comparative Analysis of Speed Performance for Hash Algorithms.

From the above cases, it is being concluded and shown in Fig. 7 that MD5 is faster in speed response than SHA-1 with 29.57% for small sequences and fasters 25.04% for large sequences. Also, SHA-1 is slow as compared to SHA-256 with 2.59% for small sequences and a 3.37% slower use level when selecting secured hash algorithm. MD5 is faster in speed response than SHA-1 with 29.57% for small sequences and fasters 25.04% for large sequences. Also, SHA-1 is slow as compared to SHA-256 with 2.59% for large sequences. SHA-256 is 5.2% faster than SHA-512 for small and faster than SHA-512 with 1.34% for large sequences. Also, out of all, SHA-1 is the fastest with 708.3 ms for small sequences and 909.3 ms for long sequences. For future work the Hybrid Cryptographic Hash Function could be suggested for a security evolved approach which would increase network consensus, however, the ledger node's confidence in current IoT devices cannot be guaranteed, and reaching a consensus would consume a large number of wireless communications.

VII. CONCLUSION

Blockchain systems can supply IoT through a distributed ledger system to exchange data in a secure nature intimidating the centralized power model that remains presently on IoT. In cryptographic currencies, the Internet of Things, chain management, financing, information exchange, and other areas, Blockchain is broadly adopted. In blockchain systems, although, there seems to be safety issues of different extents. A cryptographic hash is used to validate the authenticity and validation of transmissions in a variety of ways. MD5, SHA-1, SHA-2, and SHA-3 have all become the industry norms. The majority of them were discovered to be either usable or inefficient in terms of time. This study investigated certain hashes methods that have been submitted by academics, but the majority of them have not been checked against blockchain and IoT threats. Therefore, hash performance plays a crucial role in blockchain as well as in IoT. So, this paper focuses on the different cryptographic hash algorithms and it is conferred that it is indeed safe to limit MD5 and SHA-1 because they have been vulnerable and not secured. However, if the performance is considerably better than stable SHA-2 family for a specific scenario and protection is not so necessary, they can be selected. It is dependent on the use level when selecting a secured hash algorithm. SHA-1 is the fastest with 708.3 ms for small sequences and 909.3 ms for long sequences.

REFERENCES

[1] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, no. March, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.

[2] F. Lin et al., “Survey on blockchain for internet of things,” J. Internet Serv. Inf. Secur., vol. 9, no. 2, pp. 1–30, 2019, doi: 10.22667/JISIS.2019.05.31.001.

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” IEEE Access, vol. 6, no. c, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[4] K. Biswas and A. B. Technology, “Securing Smart Cities Using Blockchain Technology,” 2016 IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City; IEEE 2nd Int. Conf. Data Sci. Syst., pp. 1392–1393, 2016, doi: 10.1109/HPCC-SmartCity-DSS.2016.0198.

[5] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain Based Data Integrity Service Framework for IoT Data,” 2017, doi: 10.1109/ICWS.2017.54.

[6] M. Abu-elkheir, M. Hayajneh, and N. A. Ali, “Data Management for the Internet of Things: Design Primitives and Solution,” pp. 15582–15612, 2013, doi: 10.3390/s131115582.

[7] Zeyad A. Al-Odat, Mazhar Ali, Assad Abbas, and Samee U. Khan. 2020. Secure Hash Algorithms and the Corresponding FPGA Optimization Techniques. ACM Comput. Surv. 53, 5, Article 97 (October 2020), 36 pages. doi:https://doi.org/10.1145/3311724.

[8] B.P Kosta, and P.S. Naidu " Design and Implementation of a Strong and Secure Lightweight Cryptographic Hash Algorithm using Elliptic Curve Concept: SSLHA-160 ",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 2, 2021.

[9] Pfautsch, Fr., Schubert, N., Orglmeister, C., Gebhart, M., Habermann, P. & Juurlink, B., (2020). The Evolution of Secure Hash Algorithms. PARS-Mitteilungen: Vol. 35, Nr. 1. Berlin: Gesellschaft für Informatik e.V., Fachgruppe PARS. (S. 5-15).

[10] N. Khan, N. Sakib, I. Jerin, S. Quader and A. Chakrabarty, "Performance analysis of security algorithms for IoT devices," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 2017, pp. 130-133, doi: 10.1109/R10-HTC.2017.8288923.

[11] White, C., Paul, M. and Chakraborty, S., 2020. A Practical Blockchain Framework using Image Hashing for Image Authentication. arXiv e-prints, pp.arXiv-2004.

[12] L. Wan, D. Eyers, and H. Zhang, “Evaluating the impact of network latency on the safety of blockchain transactions,” Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 194–201, 2019, doi: 10.1109/Blockchain.2019.00033.

[13] J. Li, J. Wu, and L. Chen, “Block-secure: Blockchain based scheme for secure P2P cloud storage,” Inf. Sci. (Ny)., vol. 465, pp. 219–231, 2018, doi: 10.1016/j.ins.2018.06.071.

[14] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," Int. Conf. Adv. Commun. Technol. ICACT, pp. 464–467, 2017, doi: 10.23919/ICACT.2017.7890132.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[16] K. Hossain and S. Roy, "A Data Compression and Storage Optimization Framework for IoT Sensor Data in Cloud Storage," 2018 21st Int. Conf. Comput. Inf. Technol., pp. 1–6, 2018.

[17] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, vol. 2018-July, no. i, 2018, doi: 10.1109/ICCCN.2018.8487348.

[18] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., no. January 2019, pp. 151–157, 2019, doi: 10.32628/cseit195137.

[19] J. Li, Y. Liu, Z. Zhang, J. Ren, and N. Zhao, "Towards Green IoT Networking: Performance Optimization of Network Coding Based Communication and Reliable Storage," IEEE Access, vol. 5, pp. 8780–8791, 2017, doi: 10.1109/ACCESS.2017.2706328.

[20] M. Wang and Q. Zhang, "Optimized data storage algorithm of IoT based on cloud computing in distributed system," Comput. Commun., vol. 157, no. February, pp. 124–131, 2020, doi: 10.1016/j.comcom.2020.04.023.

[21] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," Proc. - 2017 IEEE/ACM 2nd Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2017 (part CPS Week), pp. 173–178, 2017, doi: 10.1145/3054977.3055003.

[22] A. R. Shahid, N. Pissinou, C. Staier, and R. Kwan, "Sensor-Chain : A Lightweight Scalable Blockchain Framework for Internet of Things," 2019 Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, pp. 1154–1161, 2019, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00195.

[23] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[24] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT," IEEE Netw., vol. 34, no. 1, pp. 69–75, 2020, doi: 10.1109/MNET.001.1900179.

[25] A. Gajbhiye and D. Sen, "Attacks and Security Issues in IoT Communication : A Survey," pp. 1688–1693, 2020.

[26] F. Buccafurri, G. Lax, L. Musarella, and A. Russo, "Ethereum transactions and smart contracts among secure identities," CEUR Workshop Proc., vol. 2334, pp. 5–16, 2019.

[27] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, and S. Tai, "Blockchain-based data provenance for the internet of things," ACM Int. Conf. Proceeding Ser., 2019, doi: 10.1145/3365871.3365886.

[28] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment," 2018 IEEE Int. Conf. Inf. Reuse Integr., pp. 15–22, 2018, doi: 10.1109/IRI.2018.00011.

[29] D. Liu, J. Ni, C. Huang, X. Lin, and X. Shen, "Secure and Efficient Distributed Network Provenance for IoT: A Blockchain-based Approach," IEEE Internet Things J., vol. 4662, no. c, pp. 1–1, 2020, doi: 10.1109/jiot.2020.2988481.

[30] K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-layer energy optimization for IoT environments: Technical advances and opportunities," Energies, vol. 10, no. 12, 2017, doi: 10.3390/en10122073.

[31] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, An Overview of Blockchain Security, vol. 2. Springer Singapore, 2019.

[32] Y. Qian et al., "Towards decentralized IoT security enhancement: A blockchain approach," Comput. Electr. Eng., vol. 72, pp. 266–273, 2018, doi: 10.1016/j.compeleceng.2018.08.021.

[33] H. Kim, S. H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," IEEE Access, vol. 7, no. September, pp. 136481–136495, 2019, doi: 10.1109/ACCESS.2019.2940052.

[34] R. Yasaweerasinghelage, M. Staples, and I. Weber, "Predicting Latency of Blockchain-Based Systems Using Architectural Modelling and Simulation," Proc. - 2017 IEEE Int. Conf. Softw. Archit. ICSA 2017, no. October, pp. 253–256, 2017, doi: 10.1109/ICSA.2017.22.

[35] Y. Xu and Y. Huang, "Segment blockchain: A size reduced storage mechanism for blockchain," IEEE Access, vol. 8, pp. 17434–17441, 2020, doi: 10.1109/ACCESS.2020.2966464.

[36] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," J. Netw. Comput. Appl., vol. 149, p. 102481, 2020, doi: 10.1016/j.jnca.2019.102481.