IMPLEMENTATION OF HASHING ALGORITHM FOR RESILIENT COMMUNICATION USING BLOCKCHAIN TECHNOLOGY

Malini Ramesh[1], Padmashree.M[2], Lavanya.E[3], Geeta.D.D[4]

[1,2,3,4] *School of Electronics and Communication Engineering, Reva University, (India)*

ABSTRACT

Authentication and resilience in data transfer is the primary focus in ever increasing network protocols. In this regard, hash functions are considered as the fundamental units of message integrity and security. Several types of Hash functions are developed to enhance the level of confidential data flow within the network. In this paper we are discussing about secure hashing technique for data transfer (peer to peer) on a decentralized blockchainbased platform.

Keywords: *Authentication, Blockchain, Integrity, Security, Resilience.*

I. INTRODUCTION

The growth of communication protocols often require a secured way of data transmission and this relies on cryptography, a technique that ensures secure mechanism. Development of Hash function in this regards fulfills certain security issues [1]. Although there are different types of Hash function which were already developed [2], few of them were found irresistible towards attacks. Hashing methodology thus employed, includes the usage of hash function that takes an arbitrary length of input and transforms that to a shorter fixed length value termed as hash. The input could be a single character or a string whereas the output is called as "message digest".

Two widely used families of Hash function are MD and SHA families, recent attacks on MD5 and SHA1 often provided the way for the development of more secure Hashing algorithm. Thus emergence of blockchain along with hash functions in the field of bitcoin or cryptocurrencies[3] enhanced the view of security. Thus, extending this level of secured data transfer is the main objective of this paper.

This paper describes the importance of data integrity and security within emergent fields like robotic and sensor network, where confidentiality of data plays a major role.

Therefore, Section-II explains the related work in brief, also explains the fundamental aspects and types of secured Hash function. Further Blockchain technology with basic principles is discussed. Section III provides methodology for implementation of a trusted system using Blockchain. In Section IV, the results analysis have been discussed. In Section V, the scope for future work and section VI concludes this paper.

II. RELATED WORK

With the expansion of network protocols the need for more reliable, integrated network is increasing enormously. The problem lies in the up-gradation of security policies considering all relevant aspects of confidentiality, integrity and availability [1][2]. Majority of hash- function are designed based on Merkle-Damgard construction [3]. General purpose hash functions were then designed, considering the key characteristics or properties of Merkle-Damgard approach, where padding, appending, initialization of buffer are few steps involved in the design. To include security aspects a key was also be used. EMD (Enveloped Merkle Damgard) and RMX are other kinds of hashing techniques[4].

2.1 Fundamental aspects of secured Hash function:

The impact of following three properties of hash function described below enhances the secure aspects of data transfer.

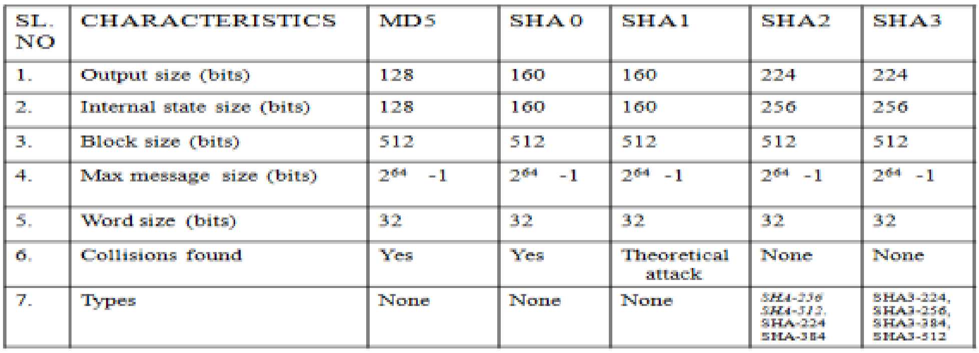
2.1.1 Pre-image resistant: The hash function is said to be pre-image resistant, if for any given h, it is computationally infeasible/hard to determine y, such that H(y)=h. It is also termed as One-way property.

2.1.2 Second pre-image resistant: As per the second pre-image resistant property, for any given x, it is very hard to find y ≠x, with H(y) = H(x).It is also termed as weak collision resistant property.

2.1.3 Collision-Resistant: The property of collision-resistant states That, it is difficult to find any pair(x,y), such that H(x)=H(y).This property is also termed as Strong collision resistant.

2.2 Types of Hash functions

Table.1 Representing the characteristics of different types of hash functions.



SL. NO	CHARACTERISTICS	MD5	SHA 0	SHA1	SHA2	SHA3
1.	Output size (bits)	128	160	160	224	224
2.	Internal state size (bits)	128	160	160	256	256
3.	Block size (bits)	512	512	512	512	512
4.	Max message size (bits)	2^{64} -1	2^{64} -1	2^{64} -1	2^{64} -1	2^{64} -1
5.	Word size (bits)	32	32	32	32	32
6.	Collisions found	Yes	Yes	Theoretical attack	None	None
7.	Types	None	None	None	SHA-256 SHA-512, SHA-224 SHA-384	SHA3-224, SHA3-256, SHA3-384, SHA3-512

2.2.1 SHA-0: NIST, the US National Institute of Standards and Technology, published a new message digest standard, termed as Secure hash Algorithm, with SHA-0 being the first member of the SHA family. The SHA-0 compression function is built upon Davis-Meyer Construction [5]. The attacks on SHA-0 provided way for the establishment of SHA-1 and its successors, revealing that the collision security strength is significantly less, than an ideal hash function (2^{36} compared to 2^{80}).

2.2.2 SHA-1: It is similar to the MD family of hash functions. The key difference between MD5 and SHA-1 is that the MD family of hash functions uses more bits compared to SHA-1, due to this reason SHA-1 is considered as more secure than MD5. SHA-1 produces message digest of 160 bits i.e. 32 bits more than the message digest produced by MD5, further the attacks on SHA-1 proved that the collision of full SHA-1 could be found in around 2^{51} hash functions, which in turn was considered as inefficient in preventing the collision attacks, as it provides less collision resistance than expected. Hence, SHA-2 family of algorithm emerged, to provide better results.

2.2.3 SHA-2: SHA-2 family of hashes gathers different size of hashes and also different block sizes, known as *SHA-256* and *SHA-512*. They do differ in the word size i.e. SHA-256 uses 32-bit words and SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256. The popular one among all the four is SHA-256. It provides better results regarding the prevention of collision attacks, and it also uses 64 to 80 rounds of cryptography operations.

2.2.4 SHA-3: A hash function formerly called *Keccak*, also termed as the latest hash function, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family. The variants of SHA-3 do include – SHA3-224, SHA3-256, SHA3-384, SHA3-512 (fixed size output length) and also includes sponge functions termed as SHAKE256, SHAKE512 (variable output length). Enabling high security margin makes it fundamentally different from SHA-2.

2.3 Blockchain Technology:

Blockchain is a new approach which is based on the technique of Bitcoin, digital currency with each block containing a list of transactions, referencing to the preceding block and by creating a chain like structure as shown in Figure1. Blockchain has the characteristics of decentralization, stability, security and non-modifiability [6][7].

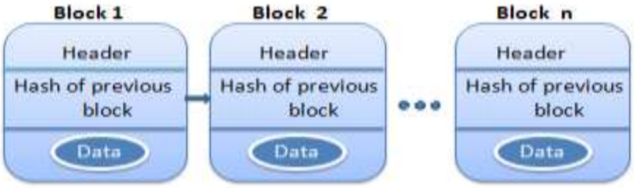


Fig.1 Structure of blockchain

2.3.1 Basic principles in Blockchain

- Network participants must have control of their functions.
- The network must be extensible with membership flexibility.
- The network must be permissioned , but with competitive data protected.
- The network must be scalable for data transfer processing and data encryption processing.

III. PROPOSED METHODOLOGY

We represent a system consisting of three main components namely the network of robots (robot nodes and sensor nodes) control system and blockchain network, where the control system is employed for the collection and distribution of data. Accordingly the storage of the collected data takes place within the coded blocks in the blockchain network hence, a decentralized blockchain network is employed for data validation and for enabling resilience [8].

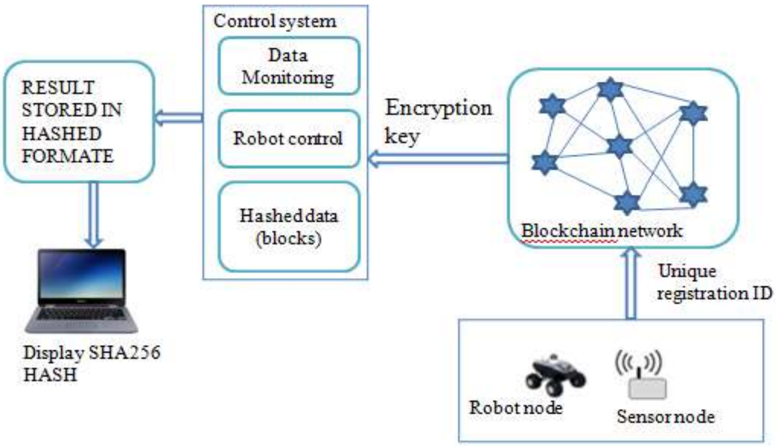


Fig.2 Proposed model

3.1 Description of proposed model

3.1.1 Robot and Sensor network

Sensor network: It comprises of sensor nodes, which are considered as data sources for presenting the sensor value and this values are collected and each of these values are stored in individual block. When this value is transmitted to the other sensor in the network, the value automatically changes to the hash value, it also assures that the value has reached the intended sensor in the network and hence the desired hash value is thus displayed on the serial monitor window.

Robotic network: The network of robots, along with robot registration is used to intensively transmit the message string. Often Hashing and digital signature including public/private key-pair are used in providing authentication to the intended robotic node, in turn providing integrity and authentication in the network.

3.1.2 Control system

Control system is mainly responsible for controlling the action of robotic nodes on receiving the intended data from source node/handheld device, with the help of wireless communication layer, i.e, wireless fidelity. The WI-FI enabled communication mechanism provides way to exchange information or to control the flow of information within the intended network.

3.1.3 Blockchain network

The blockchain network is employed for three purposes:

- To store the data collected or the messages within the blocks.
- To carryout data validation thereby generating the blockchain receipt for the intended message transfer.
- To enable secure communication among the nodes with unique feature such as improved reliable, better fault-tolerance capacity.

3.2 Key Establishment

3.2.1 Robot Registration key

In network of robots, each individual robots, with unique registration key are registered in the network Every time a new node is added or removed depending on the requirements of the robotic network, the registration key can either be added or removed depending on addition/deletion activities.

3.2.2 Data encryption key

The encryption key is generated once the robotic node has registered in the network. When the data/message is entered, the blocks, coded within the blockchain encrypt the entered message, thereby creating the encrypted key. Each time the message is provided, the corresponding hash message will be recorded on the blockchain.

3.2.3 Data access public/private key value pair

For reliable and integrated data communication a public/private key pairs are generated, which is part of digital signature. Private Key is used to generate a fingerprint/digital signature from the sender to indicate or represent data origin, while the public key is used by others to verify whether the intended receiver is receiving the data from the authentication source.

3.3 System Implementation Processes

The system comprises of three main processes namely node registration, data/message transmission and blockchain receipt generation.

3.3.1 Node registration

In our system the nodes which are employed has to enroll, to carry on data transfer and after registration, a unique identification will be assigned to each nodes. Every data record will then get associated with unique ID. The data types thus represent the data that could be a single character, numeric value or a message string.

3.3.2 Data/Message transfer

Once the data/message is sent, the copy of the same is then forwarded to blockchain network. At the same time the corresponding blocks within the network will send back some commands based on data and task with the help of a tuple containing the unique ID, time and commands in hashed format.

3.3.3 Blockchain receipt generation

Once the data is obtained it has to be uploaded to the blockchain network. With the help of a controller, the event will be captured as a blockchain transaction, thus the data gets hashed and eventually gets transformed into a Merkle tree node. This Merkle tree node offers the scalability to satisfy the throughput when large number of nodes is employed within the network. A set of data records/transaction are grouped in the blockchain and each of the blocks are validated using blockchain receipt which contains information of the blockchain message transfer. Whenever a new list of transaction arrives they are grouped together and a new block is validated and it is then added to the existing blockchain.

IV. RESULT ANALYSIS

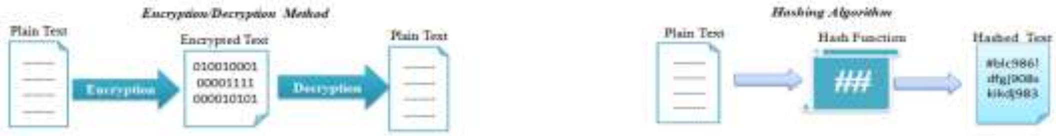
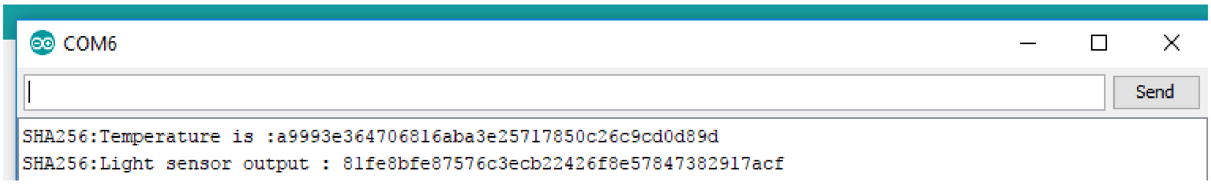


Fig.3 Difference between encryption/decryption method and hashing technique.

The figures.3 provides the comparison between the methods of encryption, with the hashing technique that is implemented in our project. The hashing thus implemented, unlike the method of encryption is irreversible and the nodes registered in the network will be able to understand and respond to data obtained from the sensor nodes.



```
SHA256:Temperature is :a9993e364706816aba3e25717850c26c9cd0d89d
SHA256:Light sensor output : 81fe8bfe87576c3ecb22426f8e57847382917acf
```

Fig.4 Output in the form of hashes

The corresponding hash values for the value obtained from each sensor node is as shown in figure 4.

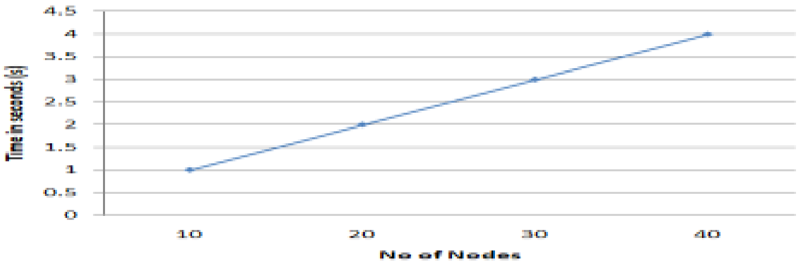


Fig.5 Response time versus varying number of nodes

In Figure 5, the graphical representation states that as the number of nodes increases, the display of hashes for each and every sensor value, takes more time than expected.

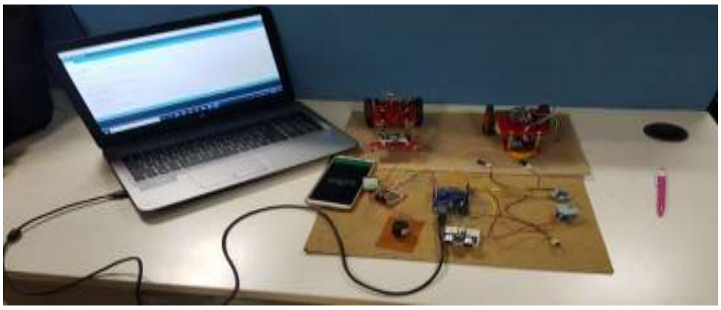


Fig.6 proposed model

Figure 6 represents the proposed working model, with robotic and sensor nodes interfaced.

V. SCOPE FOR FUTURE WORK

Emergence of drones in future IoT applications within the limited locations do include the process of collection of variety of data as well as controlling of IoT devices/nodes using Blockchain would find a trusted path by reducing threats, potential attacks and data losses. The major issue of concern is that, connected devices may sometime avoid the confidentiality of data, leading to unauthorized data transfer. Recent studies on security and privacy control could demonstrate the fundamental aspects of solving the security issues in smart IoT devices.

VI.CONCLUSION

In this paper, we proposed a model comprising of robotic and sensor nodes, with each node entitled with a unique registration ID. The key aspects do involve the mechanism of enabling secure communication on Blockchain platform with hashing and digital signature as the fundamental techniques. Furthermore, creation of block with authentication of each nodes, provide way to enhance the level of security thereby increasing the level of security thereby increasing the level of confidential data flow.

REFERENCES

[1] RichaPurohit (Arya), Upendra Mishra, AbhayBansal, *Design and Analysis of a New Hash Algorithm with Key Integration, International Journal of Computer Applications (0975 – 8887) Volume 81 – No1, November 2013.*

[2] PriyankaVadhera, BhumikaLall, *Review Paper on Secure Hashing Algorithm and Its Variants, International Journal of Science and Research (IJSR), Volume 3 Issue 6, June 2014 629-632.*

[3] Damgard I, *A Design Principle for Hash Functions. Crypto'89, LNCS Springer Verlag 1989; 435: 416-427.*

[4] Berson, Thomas A, *Differential Cryptanalysis Mod 232 with Applications to MD5, EUROCRYPT. pp. 71–80. ISBN 3-540-564136 , 1992.*

[5] Rajeev Sobti, G.Geetha, *Cryptographic Hash Functions: A Review, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012, 461-479.*

[6] Du Mingxiao, MaXiaofeng, ZhangZhe, WangXiangwei, ChenQijun, *A Review on Consensus Algorithm of Blockchain,2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017.*

[7] Moon yong Jung, JuWookJang, *Data Management and Searching System and Method to provide Increased Security for IoT Platform, ICTC 2017, 873-878.*

[8]XuepingLiang, JuanZhao, SachinShetty DanyiL, *Towards Data Assurance and Resilience in IoT using Blockchain , Military Communications Conference (MILCOM), MILCOM 2017 - 2017 IEEE, 11 December 2017,261-266.*

[9] Nikola Boziac, GuyPujolle, StefanoSecci, *A Tutorial on Blockchain and Applications to Secure Network Control Planes, Smart Cloud Networks & Systems (SCNS), 19-21 Dec 2016.*

[10] SupornPongnumkul,ChaiyaphumSiripanpornchana,SuttipongThajchayapong, *Performance Analysis of Private Blockchain Platforms in Varying Workloads, Computer Communication and Networks (ICCCN), 2017 26th International Conference , 31 July-3 Aug. 2017.*