International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Self-Redactable Block chain to Attain Intelligent Trust-Layer for IOT

Anju R G[1], Dr. S Vadhana Kumari[2], Dr. A J Deepa[2]

[1]PG Student , Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

[2]Professor, Department of Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu, India

ABSTRACT

The advance of Artificial Intelligence (AI) propels big data processing and transmission for Internet of Things (IoT), by capturing and structuring big data produced by heterogeneous devices. While applying blockchain to manage IoT devices and associated big data, the blockchain itself suffers from abuse of decentralization from anonymous users. Specifically, it has been utilized to facilitate black market trades and illegal activities. The Chameleon Hash (CH) to derive Redact able Blockchain (RB), which works by embedding a trapdoor in the basic hash function so that block content can be rewritten without causing major hard forks. In short, the redacted block hash remains unchanged. However, there is lacking intelligent design where any mistakes observed in the chain can be corrected universally and automatically. This creates disincentives to use Redact able Blockchain for managing big data or any data-driven business mainly due to ineffective chain redaction. To solve this problem, in this project, propose the notion of the Self-Redact able Blockchain (SRB) to support intelligent execution of chain redaction. Specifically, propose the first Revocable Chameleon Hash (RCH) to power RB. It enables an ephemeral trapdoor for finding collision without any co- operation. Periodical expiration is applied to committed hash and an ephemeral trapdoor to prevent any abuses of redaction power. Here, instantiate how to use proposed RCH to build SRB as an intelligent trust-layer for IoT. Here also give a rigorous analysis as well as comprehensive experiments to validate the proposals. The evidence showed that our proposal is secure and acceptably efficient for IoT devices.

Index Terms- IoT; Intelligence; Blockchain; Automatic Redaction;

I. INTRODUCTION

The advance of Internet-of-Things (IoT) connects and interacts more and more heterogeneous devices (such as mobile devices, sensing devices, etc.) to facilitate people's daily life. Big data serves as an indispensable propellant for the realization of IoT as massive values are hidden behind and waiting for extraction. Meanwhile, Artificial Intelligence (AI) revolutionizes these infrastructures by enabling automation and smart thinking for devices. Although the above concepts partially overlap with each other, they are

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

all under a universal concern over associated privacy and trust. Blockchain serves as a convenient and effective trust layer for the above concepts. It can be used to manage either geographically-located IoT devices or heterogeneous big data at low cost. For example, by recording the corresponding metadata on the chain, it can manage big massive data stored on the distributed cloud server.

When applying blockchain as a trust-layer for IoT or big data, security and privacy rules are applied. However, as recently reported by Ali et al, the newly launched blockchain suffered from powerful attacks such as 51% attack due to small computing pool. Malicious users can easily manipulate the blockchain with considerable but not unimaginably-large computing resources. As a fact, manipulation over 60% of the network power has been witnessed, which is a severe threat against the blockchain. As witnessed by the catastrophic loss caused by the ”DAO” incident to one of the dominant crypto-currencies induced by hackers, it is necessary to grant newly started blockchain with the power of redaction to be immunized against such attack. Redactable Blockchain (RB) mainly relies on the trapdoor one-way hash function (which is also known as chameleon hash function, where finding collision is hard without the trapdoor key. The current design of RB mainly focuses on how to split and distribute the trapdoor key of chameleon hash. It is seemingly impossible under an entirely anonymous and decentralized setting (e.g., bitcoin network) as it requires help or even co- operation of trapdoor key holders. As IoT devices are distributed heterogeneously, it quests for an automatic solution by which redaction can proceed without any helps.

The main objectives of this project is

- The idea is to propose Self-Redactable Blockchain (SRB) to support intelligent execution of chain redaction.
- It can be used to build an intelligent trust- layer for data stored in IoT devices.

IoT is a network system in both wired and wireless connection that consists of many software and hardware entities such as manufacturing management, energy management, agriculture irrigation, electronic commerce, logistic management, medical and healthcare system, aerospace survey, building and home automation, infrastructure management, large scale deployments and transportation

The purpose of IoT is to turn traditional products into connected products by taking advantage of exchanging data and communicating with each other in order to monitor and control the objectives.. The advantage of the IoT is obvious it is efficient data collection and exchange. In addition, IoT provides cost- effective ways for saving energy and contributing to environment protection. In other words, IoT enables advanced security by interconnecting physical and virtual devices based on existing and evolving interoperable information and communication technologies. It involves a variety of protocols, domains and application

A. BLOCKCHAIN TECHNOLOGY

Blockchain provides decentralized data storage service with a tamperresistant ledger consisting of blocks chained in serial in distributed networks. It can record and secure transactions or transactional events using cryptography. Blockchain records data in a secure and distributed manner. The basic unit of records in Blockchain is the transaction. Each time a new transaction is generated, it is broadcast to the entire Blockchain network. Nodes receiving the transaction can verify the transaction by validating the signature attached to the transaction, and mine verified transactions into cryptographically secured blocks. Such nodes are known as block miners (or miners for short). To allow a miner to create a block, a consensus problem needs to be solved in a distributed manner. The miners that manage to solve the consensus problem broadcast their new blocks throughout the network. Upon the receipt of a new block, the miners yet to be able to solve the consensus problem append the block to their own chains of blocks locally maintained at the miners, after all the transactions enclosed in the block are verified and the block is also proven to provide the correct answer to the consensus problem. The new block contains a link to the previous block in the chains, by exploiting cryptographic means. All miners can synchronize their chains on a regular basis, and specific terms are defined to ensure the consistent ledger shared across the distributed network, e.g., Bitcoin. Blockchain only keeps the longest chain, in the case where there is discrepancy among the chains.

B. SECURITY ANALYSIS ON BLOCKCHAIN

Blockchain attracts attentions for its highly anti-tampering property in decentralized networks. Specifically, Blockchain does not require peers to trust each other. However, Blockchain still exhibits vulnerabilities. Typical security threats to Blockchain are as follows,

- **Double spending:** adversaries attempt to mislead the transaction receivers with conflicting transactions, e.g., spending the same coin in Bitcoin. Possible attack methods include sending conflicting transactions and pre-mining one or more blocks to get conflicting transactions accepted by the Blockchain
- **Attacks on consensus protocols:** attackers could break the security assumption of consensus protocols by possessing a considerably large chunk partition of the computing power of the entire network. Such attackers can control and reconstruct the chain. An example is the 51% attack in PoW Blockchains, e.g., Bitcoin. The attackers, owning more than a half of the hash power can make Blockchain accept illegitimate blocks, by solving the consensus problem (e.g., POW in Bitcoin) faster than the rest of peers. Currently, it has proved that 33% hash power is sufficient to overpower POW.
- **Eclipse attacks:** Eclipse attacks refer to the attacks in P2P networks where adversaries monopolize all connections to the legitimate nodes and prevent the legitimate nodes from connecting to any honest peers.
- **Vulnerability of smart contracts:** smart contracts are susceptible due to the openness and the irreversibility of Blockchain. Bugs and frauds are transparent to the public including adversaries. Also, it is challenging to make up bugs in the deployed smart contracts due to the irreversibility of Blockchain. An outstanding example is the attack to the Decentralised Autonomous Organisation (DAO) in 2016, known as the DAO attack, which resulted in a forked Ethereum Blockchain.
- **Programming fraud:** the attackers can exploit frauds in programming codes to extract properties of Blockchain, such as the piracy attack reported in 2018
- **DDoS:** the adversaries exhaust the Blockchain resources (such as exhausting the whole network processing capability) by launching a collaborative attack. The huge number of accounts with low balance produced by adversaries led to a DDoS attack.
- **Leakage of private key:** the attackers can steal the private key of an account to take over the account. This can be achieved via traditional network attacks or capturing physical nodes so that the hackers can easily find key value.

II. LITERATURE SURVEY

Eyal.I et. al [1] proposed that the Cryptographic forms of money, in light of and driven by Bitcoin, have appeared as foundation for pseudonymous online installments, shabby settlement, trustless computerized resource trade, and brilliant contracts. In any case, Bitcoin-determined blockchain conventions have intrinsic versatility constrains that exchange off among throughput and dormancy, which retain the acknowledgment of this potential. The Bitcoin-NG (Next Generation), another blockchain convention intended to scale. Bitcoin-NG is a Byzantine blame tolerant blockchain convention that is vigorous to outrageous agitates and offers a similar trust display as Bitcoin. Notwithstanding Bitcoin-NG, A few novel measurements of enthusiasm for evaluating the security and effectiveness of Bitcoin-like blockchain conventions are presented. Actualize theBitcoin-NG and perform extensive scale tests at 15% the measure of the operational Bitcoin framework, utilizing unaltered customers of the two conventions. These trials show that Bitcoin-NG scales ideally, with data transmission restricted just by the limit of the individual hubs and inertness constrained just by the spread time of the system. It improves latency and throughput to the maximum allowed by network conditions and node processing limits, while avoiding the fairness of the network.

Atzori et. al [2] proposed that the Internet of Things is the fundamental empowering element of this promising worldview is the coordination of a few advances and correspondences arrangements. Distinguishing proof and following innovations, wired and remote sensor and actuator systems, upgraded correspondence conventions (imparted to the Next Generation Internet), and appropriated knowledge for shrewd articles are only the most important. As one can without much of a stretch envision, any genuine commitment to the development of the Internet of Things should fundamentally be the aftereffect of synergetic exercises directed in various fields of learning, for example, broadcast communications, informatics, gadgets and sociology. In such a mind- boggling situation, this review is coordinated to the individuals who need to approach this perplexing control and add to its improvement. Distinctive dreams of this Internet of Things worldview are accounted for and empowering innovations explored. The most important among them are tended to in subtleties. It offers particular value for businesses and transaction depending on various sectors of bank that the data can lead to larger productivity, higher profitability.

Gavin Wood [3] proposed that the blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not least Bitcoin. Each such project can be seen as a simple application on a decentralized, but singleton, compute resource. So it can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalized manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message- passing framework with others. The design and implementation issue that provides the opportunities for the future hurdles we envisage. With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology rooted movements like Bitcoin have demonstrated, through the power of the default, consensus mechanisms and voluntary respect of the social contract that it is possible to use the internet to make a decentralized value-transfer system, shared across the world and virtually free to use. This system can be said to be a specialized version of a cryptographically secure, transaction based state machine.

Lue et. al [4] proposed that the Cryptocurrencies, such as Bitcoin embody at their core a blockchain protocol a mechanism for a distributed at their core a blockchain protocol a mechanism for a distributed network of computational nodes to periodically agree on a set of new transactions. Designing a secure blockchain protocol relies on an open challenge in security that of designing a highly scalable agreement protocol opens to manipulation by byzantine or arbitrarily malicious nodes. Bitcoin blockchain agreement protocol exhibits security, but does not scale it processes 3–7 transactions per second at present, irrespective of the available computation capacity at hand. In this paper, the new distributed agreement protocol for permission-less blockchains called elestico. Elestico scales transaction rates almost linearly with available computation for mining the more the computation power in the network, the higher the number of transaction blocks selected per unit time. Elastico is efficient in its network messages and tolerates byzantine adversaries of up to one-fourth of the total computational power. Technically, elastico uniformly partitions or parallelizes the mining network into smaller committees, each of which processes a disjoint set of transactions. While sharing is common in nonbyzantine settings, a secure sharing protocol.

Christidis et. al [5] proposed that the The recent increase in reported incidents of surveillance and security breaches compromising the user's privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. The decentralized personal data management system that ensures users own and control their data. Unlike Bitcoin, transactions in our system are not strictly financial - they are used to carry instructions, such as storing, querying and sharing data. Finally, the possible future extensions to blockchains that could harness them into a well-rounded solution for trusted computing problems in society. In such a mind- boggling situation, this review is coordinated to the individuals who need to approach this perplexing control and add to its improvement while transmitting the as a block using hash values which create a block in the network.

Paterson et. al [6] proposed that to makes concrete the idea of Certificateless Open Key Cryptography (CL-PKC), a model for the utilization of open key cryptography which stays away from the intrinsic escrow of character based cryptography but then which does not expect endorsements to ensure the validness of open keys. The absence of authentications and the nearness of a foe that approaches an ace key require the watchful improvement of another security demonstrate. It includes center around Certificateless Open Key Encryption (CL-PKE), demonstrating that a solid matching-based CL-PKE plot is secure given that a hidden issue firmly identified with the Bilinear Diffie- Hellman Problem is hard.

Perezs la et. al [7] proposed that the Bitcoin has emerged as the most successful cryptocurrency since its appearance back in 2009. However, its main drawback to become a truly global payment system is its low capacity in transaction throughput. At present time, some ideas have been proposed to increase the transaction throughput, with different impact on the scalability of the system. Some of these ideas propose to decouple standard transactions from the blockchain core and to manage them through a parallel payment network, relegating the usage of the bitcoinblockchain only to transactions which consolidate multiple of those off-chain movements. Such mechanisms generate new actors in the bitcoin payment scenario, the payment service providers (PSP) and new privacy issues arise regarding bitcoin users. The comprehensive description of the most relevant scalability solutions proposed for the bitcoin network and outlines its impact on users privacy based on the early stage proposals published so far.

Buchman [8] proposed that the Tendermint is another convention for requesting occasions in an appropriated system under ill-disposed conditions. All the more regularly known as agreement or nuclear communicate, the issue has pulled in huge consideration as of late because of the across the board achievement of computerized monetary forms, for example, Bitcoin and Ethereum, which effectively tackle the issue out in the open settings without a focal specialist. Tendermint modernizes great scholastic work regarding the matter to furnish a protected accord convention with responsibility ensures, just as an interface for building discretionary applications over the agreement. Tendermint is elite, accomplishing a huge number of exchanges every second on many hubs circulated the world over, with latencies of around one moment, and execution debasing reasonably notwithstanding ill-disposed assaults.

Vukolic [9] proposed that the Bitcoin cryptocurrency demonstrated the utility of global consensus across thousands of nodes, changing the world of digital transactions forever. In the early days of Bitcoin, the performance of its probabilistic Proof- Of-Work (POW) based consensus fabric, also known as block chain. Bitcoin became a success story, despite its consensus latencies on the order of an hour and the theoretical peak throughput of only up to 7 transactions per second. The situation today is radically different and the poor performance scalability of early blockchains no longer makes sense

Zhang et. al [10] proposed that the The multiple computer science and electronic cash innovations it brought, there has been great interest in the potential of decentralized crypto currencies. At the same time, implementation changes to the critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation. A new technology, pegged side chains, which enables bitcoins and other ledger assets to be transferred between multiple block chains. This gives users access to new and innovative crypto currency systems using the assets they already own Since side chains are separate systems, technical and economic innovation is not hindered. a cryptographic break (or malicious design) in a side chain, the damage is entirely confined to the side chain itself. This lays out pegged side chains, their implementation and the work needed to fully benefit from the future of interconnected block chains.

III. EXISTING SYSTEM

A Chameleon-Hash (CH) is a hash function, where hashing is parameterized by a public key pk. It behaves like a collision resistant hash function as long as the trapdoor (the secret key sk corresponding to pk) is not known. Conversely, if the trapdoor sk is known, arbitrary collisions can be found. Using such hash functions as a replacement for collision-resistant ones in blockchains allows introducing some entity that possesses the trapdoor. By computing collisions in the hash function, this entity can efficiently edit the blockchain Firstly, it considers rewriting of a blockchain on the block level, i.e., to replace the hash of an entire block, which seems to be far too coarsegrained and powerful and rewriting on a transaction level seems more reasonable. Furthermore, the party who computes the hash is totally oblivious about who is later able to compute collisions in the chameleon-hash however, when an object should be included into the blockchain, the party performing this operation should be able to specify who is able to perform editing on this object in a fine-grained way. Blockchain serves as a convenient and effective trust layer for the above concepts.

It can be used to manage either geographically-located IoT devices or heterogeneous big data at low cost. For example, by recording the corresponding metadata on the chain, it can manage big massive data stored on the distributed cloud server. When applying blockchain as a trust-layer for IoT or big data, security and privacy rules are applied. However the newly launched blockchain suffered from powerful attacks due to small computing pool. Malicious users can easily manipulate the blockchain with considerable but not unimaginably-large computing resources. As a fact, manipulation over 60% of the network power has been witnessed, which is a severe threat against the blockchain. The Redactable Blockchain to efficiently remove illegal and malicious contents from the blockchain without causing inconsistency of the block hash. As witnessed by the catastrophic loss caused by the ”DAO” incident to one of the dominant crypto- currencies induced by hackers, it is necessary to grant newly started blockchain with the power of redaction to be immunized against such attack. Redactable Blockchain (RB) mainly relies on the trapdoor one-way hash function which is also known as chameleon hash function, where finding collision is hard without the trapdoor key. The current design of RB mainly focuses on how to split and distribute the trapdoor key of CH. It is seemingly impossible under an entirely anonymous and decentralized setting (e.g., bitcoin network) as it requires help or even co-operation of trapdoor key holders. As IoT devices are distributed heterogeneously, it quests for an automatic solution by which redaction can proceed without any helps. As influenced by AI programming is supposed to be dominated by automatic and intelligent execution. We, therefore, request an intelligent design of RB, which is assumingly available to redact itself once an error has been discovered.

3.1 SYSTEM MODEL

The first Revocable Chameleon Hash (RCH) to drive a Self-Redactable Blockchain (SRB). The redaction is launched by any reasonable causes and can be executed automatically at each node’s side without any cooperation. As driven by the theory of economy, each node is enforced to follow redaction (otherwise, corresponding mining is denoted as unorthodox and will not be accepted by the rest of nodes). We summaries the contributions as follows: The first RCH with ephemeral trapdoor, it allows collision to be found via ephemeral trapdoor previously generated. Most importantly, these ephemeral trapdoors, as well as committed hashes, are suffered from periodical expirations so that abuse of trapdoor and forgery are prevented. Besides, revoked hashes can be activated (un-revoked) if fresh trapdoors are given. We instantiate the RCH to build a SRB. The chain is supposed to be self-redacted without the help of other entities. It can be used to build an intelligent trust-layer for IoT. Security analysis is given to validate the RCH and SRB. It also provides a comprehensive analysis of the performance of SRB.

The evidence showed that the data stored are secure and acceptably efficient. Specifically, although the additional computations for redaction, these actions can be executed automatically by using an offline method. The SRB we instantiated inherits merits of the original design of bitcoin so that fast verification and storage saving are supported. It enables an ephemeral trapdoor for finding collision without any Cooperation. Periodical expiration is applied to committed hash and an ephemeral trapdoor to prevent any abuses of redaction power. The rigorous analysis as well as comprehensive experiments to validate RCH. The evidence showed that our proposal is secure and acceptably efficient for IoT devices. The first RCH with ephemeral trapdoor; it allows collision to be found via ephemeral trapdoor previously generated. Most importantly, these ephemeral trapdoors, as well as committed hashes, are suffered from periodical expirations so that abuse of trapdoor and forgery are prevented. RCH functions with ephemeral trapdoor is a nutshell, this primitive requires that a collision in the hash function can be computed only when two secrets are known, i.e., the main trapdoor, and an ephemeral one. The main trapdoor is the secret key corresponding to the chameleon-hash function public key, while the second, ephemeral, trapdoor is generated by the party computing the hash value. The latter party can then decide whether the holder of the long-term secret key shall be able to equivocate the hash by providing or withholding the second trapdoor information the formal security model for this new primitive. Furthermore, the RCH functions not considered before, including the new notion of uniqueness, and show how to construct SRB functions being secure in this stronger model. When applying blockchain as a trust-layer for IoT or big data, security and privacy rules are applied. However the newly launched blockchain suffered from powerful attacks due to small computing pool .The reason that more metadata is to enable redaction, and such metadata include chameleon hash, randomness and ephemeral trapdoor. It enables an ephemeral trapdoor for finding collision without any cooperation. Periodical expiration is applied to committed hash and an ephemeral trapdoor to prevent any abuses of redaction power.

IV. PROPOSED SYSTEM

The framework of our SRB is driven by RCH scheme. As coincided by, there are three major entities, including the user, the miner and the blockchain. A simple workflow is depicted by user A publishes the signed transaction together with its ephemeral trapdoor by running algorithms RCH.Hash and RCH.Etd-Gen, the miner then verifies (by RCH.Verify) and records them in SRB the way as we later instantiated. Thus, user B is allowed to perform redaction (by RCH.Forge) on SRB without any helps or breaking the consistency of hash in the blockchain.

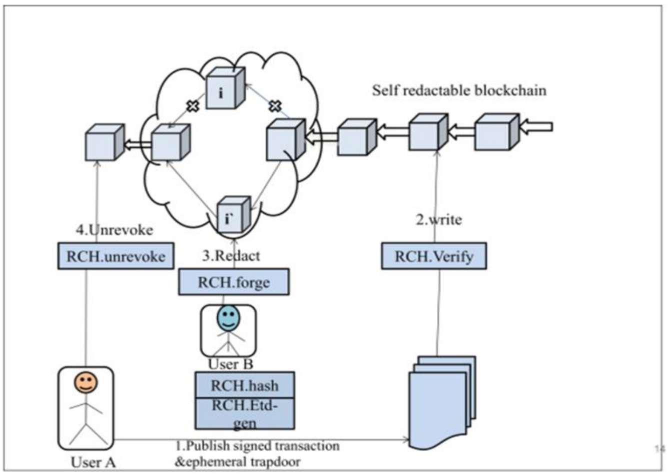


Figure.4.1 The framework of SRB

The framework of SRB is driven by RCH scheme. There are three major entities, including the user, the miner and the SRB. The user will register by giving all the details about the particular person including name, email address, phone number, address etc. The miners are used to verify the computed hash value is same as the original hash value. The SRB is used to delete the unwanted blocks without losing the data from each block. Specifically the user as one who signs and publishes transactions to the network for confirmation, denote the miner as an entity with potentially-large computing power to compete in a Proof-Of-Work (POW) consensus mechanism to reach a global agreement, and denote the SRB as a redactable public ledger maintained by miner and accessible for all users.

A simple workflow is depicted by user, A publishes the signed transaction together with its ephemeral trapdoor by running algorithms RCH: Hash and RCH: Etd-Gen, the miner then verifies (by RCH Verify) and records them in SRB Thus, user B is allowed to perform redaction (by RCH Forge) on SRB without any helps or breaking the consistency of hash in the blockchain. To reverse hash revocation, user A can run RCH Un-Revoke to activate expired hash with fresh trapdoor.The RCH is used for building SRB. Before instantiating the details, the first describe how to derive a RCS based on RCH. CH function trivially derives a Chameleon Signature (CS) since digital signature basically follows hash-and-sign paradigm.

A. Setup Phase

- On input a security parameter is chosen to two groups G and GT with prime order p and generator g.
- Set bilinear map and Pick a cycle time to expire chameleon hash and ephemeral trapdoor periodically.
- Set hash functions and prepare output as system parameters.

B. Key Generation Phase

- On input system parameters, pick a random number as trapdoor key, and compute as hash key.
- The key is generated based on the message and the computed hash value given by the user.

C. RCH hashing phase

- Pick a random number and then compute randomness value and hash value as output.
- The hash value is stored in the form of blocks. The hash value consists of mixed number and alphabets.

D. RCH Verification phase

- On input system parameters, a tuple which includes customized identity CID, hash value, randomness, message and a current time.
- First compute hash value using customized identity and current time
- Check whether True. If yes, proceed; else, output 0.
- Next, check the RCH hash, If yes, output 1; else output 0

E. RCH Ephemeral trapdoor Generation

- On input system parameters, a trapdoor key x, a customized identity CID and a given time tc.
- First compute hash value using customized identity and given time
- Then, compute ephemeral trapdoor using trapdoor key.

F. RCH Ephemeral trapdoor Verification

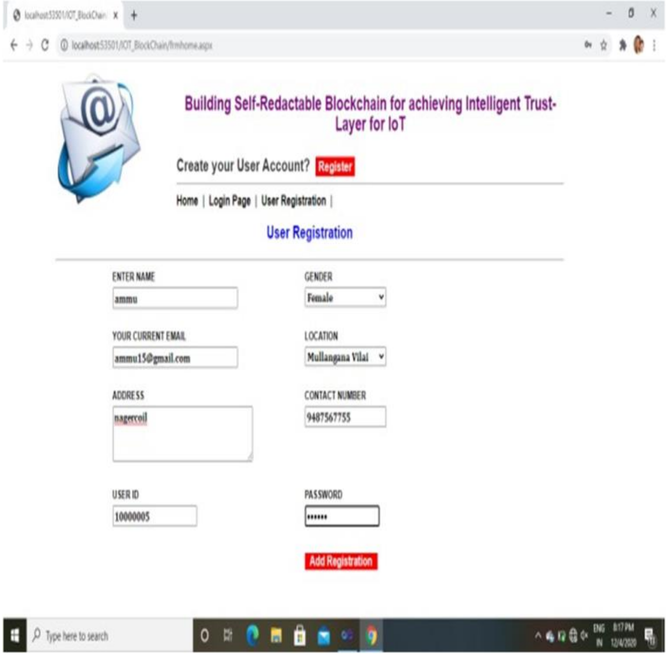
- On input system parameters, an ephemeral trapdoor, a customized identity, a current time and hash key are generated.
- Compute hash value using customized identity and given time.

G. RCH Forge phase

- On input system parameters, a tuple which includes customized identity CID, hash value, randomness and committed message, an ephemeral trapdoor, a new message, are converted into hash value.
- Compute hash value using customized identity and given time and then new randomness.

V. RESULTS AND DISCUSSION

In this work, the first RCH is to derive a SRB. The redaction is supposed to be executed intelligently without anyone's help. Here, instantiated how to use RCH to build SRB as an intelligent trust-layer for IoT. The security and experimental evidence showed that our proposals are secure and acceptability efficient to be implemented in IoT devices. Although introduced additional costs and metadata to obtain redaction, it can be compensated.


localhost53501/IOT_BlockChain/frmhome.aspx
Create your User Account? Register
Home | Login Page | User Registration |
Add Registration
Type here to search
ENG IN 8:17 PM 12/4/2020

Building Self-Redactable Blockchain for achieving Intelligent Trust-Layer for IoT

User Registration

ENTER NAME: ammu

GENDER: Female

YOUR CURRENT EMAIL: ammu15@gmail.com

LOCATION: Mullangana Vilai

ADDRESS: nagercoil

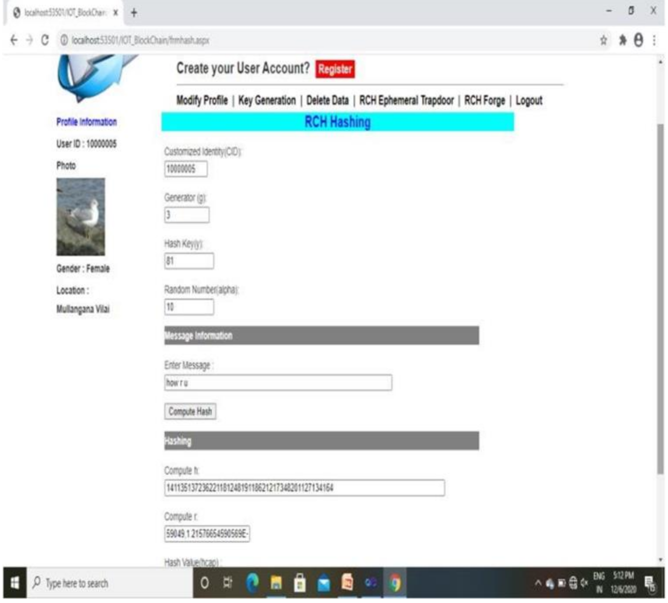
CONTACT NUMBER: 9487567755

USER ID: 10000005

PASSWORD: ••••••

Figure 5.1 User Registration

In user registration here we can able to generate user id. We have to enter the name, email address; address, gender, location, contact number, password and then click add registration.


localhost:53501/IOT_BlockChain/frmhash.aspx
Create your User Account? Register
Modify Profile | Key Generation | Delete Data | RCH Ephemeral Trapdoor | RCH Forge | Logout
RCH Hashing
Profile Information
Message Information
Compute Hash
Hashing
Type here to search

User ID : 10000005

Photo

Gender : Female

Location : Mullangana Vilai

Customized Identity(CID): 10000005

Generator (g): 3

Hash Key(y): 81

Random Number(alpha): 10

Enter Message : how r u

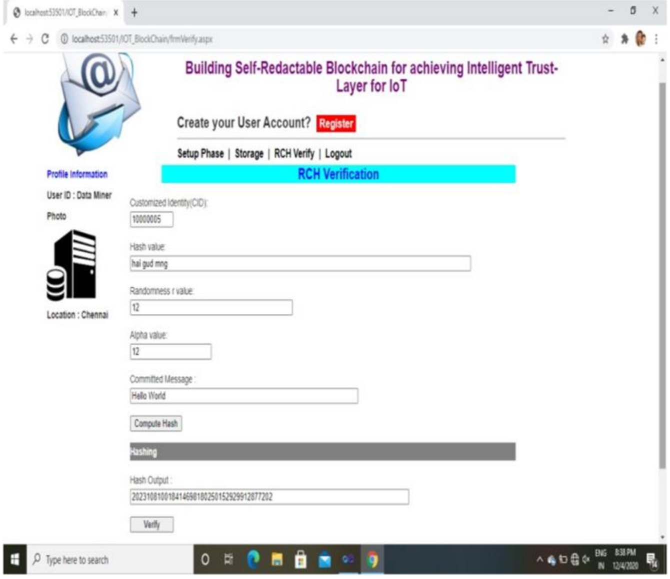
Compute h: 14113513723622118124819118621217348201127134164

Compute r: 59049,1.21576654590569E-

Hash Value(hcap) :

Figure 5.2 RCH Hashing

The orginal message is converted into hash value and the particular hash value is stored as a block.


localhost:53501/IOT_BlockChain/frmVerify.aspx
Building Self-Redactable Blockchain for achieving Intelligent Trust-Layer for IoT
Create your User Account? Register
Setup Phase | Storage | RCH Verify | Logout
RCH Verification
Profile Information
Compute Hash
Hashing
Verify
Type here to search

User ID : Data Miner

Photo

Location : Chennai

Customized Identity(CID): 10000005

Hash value: hai gud mng

Randomness r value: 12

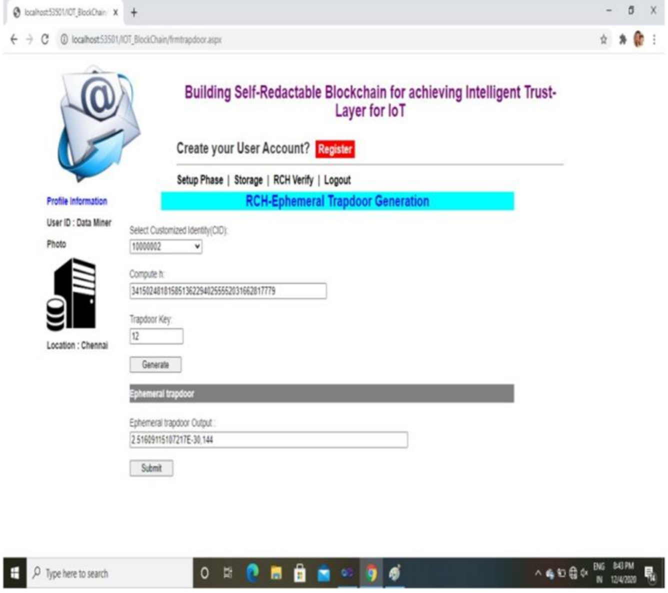
Alpha value: 12

Commited Message : Hello World

Hash Output : 202310810018414698180250152929912877202

Figure 5.3 RCH Verification

RCH Verification verifies if the hash value and the committed message are same if it is same the output is 1 otherwise 0.


localhost:53501/IOT_BlockChain/frmtrapdoor.aspx
Building Self-Redactable Blockchain for achieving Intelligent Trust-Layer for IoT
Create your User Account? Register
Setup Phase | Storage | RCH Verify | Logout
RCH-Ephemeral Trapdoor Generation
Profile Information
Generate
Ephemeral trapdoor
Submit
Type here to search

User ID : Data Miner

Photo

Location : Chennai

Select Customized Identity(CID): 10000002

Compute h: 3415024818158513622940255552031662817779

Trapdoor Key: 12

Ephemeral trapdoor Output : 2.51609115107217E-30,144

Figure 5.4 RCH Trapdoor Generation

In Trapdoor Generation we have to select the customized id and the computed hash value it will generate a trapdoor key.

VI. PERFORMANCE ANALYSIS

To simulate the performance we compare both the existing system and the proposed system.

Since IoT devices are generally equipped with limited resources (power, processing and storage capacity), it is vital to investigate the energy cost and the performance.

6.1 PERFORMANCE OF BLOCK REDUCTION

The experiments to test performance of proposed SRB. Each block in a chain consists of multiple transactions; first evaluate the cost of redaction on a single transaction. As instantiated, the rationale is replacing ordinary signature with RCS as instantiated. For ease of analysis, suppose the transaction generation is dominated by RCS generation, and only test the computational cost. Here incrementally set the number of transactions from 10 to 100, and test corresponding cost at each stage. This is because the more is redacted; the more is needed to be confirmed.

The gap between redaction and verification cost widens with a number of processed blocks and the time taken to process each block. In existing system the block reduction time increases compare with the system.

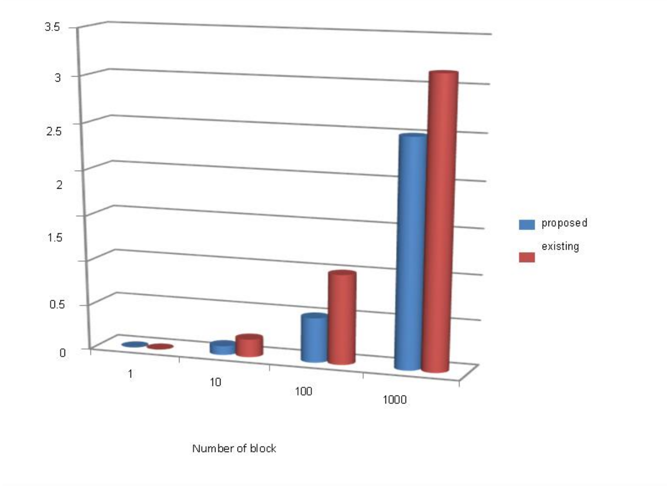


Figure 6.1 Performance of Block Reduction

VII. CONCLUSION

In this article, we propose the first RCH is to derive a SRB. The redaction is supposed to be executed intelligently without anyone's help. Here, instantiated how to use RCH to build SRB as an intelligent trust- layer for IoT. The security and experimental evidence showed that our proposals are secure and acceptability efficient to be implemented in IoT devices. Although introduced additional costs and metadata to obtain redaction, it can be compensated without any help by the user.

FUTURE WORK

Threshold Chameleon Hash (TCH) and Accountable and Sanitizable Chameleon Signature (ASCS) schemes are used. Based on them, a Redactable Consortium Blockchain (RCB) which is efficient for IoT devices to operate. It allows a group of authorized sensors to write and rewrite blockchain without causing any hard forks. Basically, TCH is the first TCH and ASCS is a public-key signature supporting file-level and block-level modifications of signatures without impairing authentications. Additionally, ASCS achieves accountability to avoid abuse of redaction.

VIII. REFERENCES

[1]. I.Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A Scalable Blockchain protocol." in NSDI, 2016, pp. 45–59.

[2]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey, Computer networks, vol. 54, no. 15, pp. 2787–2805, 2017.

[3]. Dr. Gavin Wood, "Ethereum: A secure decentralized generalized transaction Ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[4]. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 Conference on Computer and Communications Security. ACM, 2016, pp. 17–30.

[5]. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for The Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[6]. Paterson , Sahai. A and Waters. B, "Ciphertext-policy attributebased encryption," in 2007 IEEE Symposium on Security and Privacy. IEEE Computer Society Press, May 2007, pp. 321–334.

[7]. Perezs la and Rogaway .P, "Random oracles are practical: A paradigm for designing efficient protocols," in ACM CCS 93, As by .A, Ed. ACM Press, Nov. 1993, pp. 62–73.

[8]. E. Buchman, "Tendermint: Byzantine fault tolerance in the age of Blockchains" Ph.D. dissertation, University of Guelph, 2016.

[9]. M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-workVs. BftReplication," in International Workshop on Open Problems in Network Security. Springer, 2015, pp. 112–125.

[10]. Zhang J, Russell and Peter Norvig. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited, 2016.

[11]. Ateniese.G, Magri.B, Venturi.D, and Andrade E.T, “Redactable blockchain - or - rewriting history in bitcoin and friends,” in 2017 IEEE European Symposium on Security and Privacy, EuroS&P 2017, 2017.

[12]. Badertscher. C, Matt. C, and Maurer. U, “Strengthening access control encryption,” in ASIACRYPT 2017, Part I, ser. LNCS, Takagi.T and Peyrin .T, Eds., vol. 10624. Springer, Heidelberg, Dec. 2017, pp. 502–532.

[13]. Bellare .A, Namprempre .C, Poi ntcheval .D, and Semanko.M, “The one-more-RSA-inversion problems and the security of Chaum’s blind signature scheme,” Journal of Cryptology, vol. 16, no. 3, pp. 185–215, Jun. 2003.

[14]. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A survey. Computer networks, 54(15):2787–2805, 2010.

[15]. J. Herrera-Joancomart and C. Perez-Sola, “Privacy in bitcoin transactions: New challenges from blockchain scalability solutions,” in Modeling Decisions for Artificial Intelligence. Springer, 2016, pp. 26–44.