Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 1, pp. 11–15, DOI 10.12694:/scpe.v21i1.1602

AN ENSEMBLE INTEGRATED SECURITY SYSTEM WITH CROSS BREED ALGORITHM

SURESH MUNDRU[*] AND K. MEENA[†]

Abstract. Blockchain and IoT are two technologies are most widely popular in present scenario, but technologies are more complicated. The blockchain used to transforms storage and data analysis. In recent years, the blockchain is at the heart of computer technologies. It is a cryptographically secure distributed database technology for storing and transmitting information. Various attacks are done in many networks. Many research articles discussed about the security issues over the IoT based secure using block chain technology. In this paper, an Ensemble Integrated Security System (EISS) is introduced to improve the security for the heterogeneous network which consists of normal and abnormal nodes which is processed with the block chain, IoT. Results show the performance of the OUATH-2 and EISS algorithm.

Key words: Blockchain, Internet of things, Networks.

AMS subject classifications. 68M11, 68M10

1. Introduction. Security is most widely used in many applications. In routing protocols it is very important to secure the routing. If the WSN is integrated with IoT and blockchain it becomes more compatible for security. IoT is the fast-growing technology in the present world [1]. In 2015, i.e., around 20 years after the term was authored, the IEEE IoT Initiative discharged a report whose principle objective was to set up a benchmark meaning of the IoT, with regards to applications extending from little, confined frameworks obliged to a particular area, to enormous worldwide frameworks made out of complex sub-frameworks that are geologically circulated [2]. In this archive, we can discover an outline of the IoT's design necessities, its empowering advancements, just as a brief meaning of the IoT as an ”application space that incorporates distinctive innovative and social fields”. At its center, the IoT comprises of arranged items that sense and assemble information from their environment, which is then used to perform robotized capacities to help human clients. The IoT is still relentlessly developing around the world, on account of extending Internet and remote access, the presentation of wearable gadgets, the falling costs of installed PCs, the advancement of capacity innovation and distributed computing [3]. Today, the IoT pulls in a large number of research and modern interests. As time passes, littler and more intelligent gadgets are being executed in numerous IoT areas, including lodging, exactness agribusiness, foundation observing, individual medicinal services, and independent vehicles just to give some examples.

Blockchain is the technology which is used to improve the performance in terms of security. Users can use various private and public keys to solve the security issues to transfer the data. The most serious issue with IoT security is that ”there is no most concerning issue [4] [5] [6].” IoT has more mind-boggling details than conventional data innovation (IT) framework. It is significantly more liable to comprise of different equipment and programming items. As indicated by Forrester senior investigator Merit Maxim, the three primary regions of IoT security are a gadget, arrange, and back-end, which can all be objective and we ought to be cautious about.

Providing security for the IoT and nodes in the Network. In this paper, an ensemble integrated security system (EISS) is introduced to provide security between the nodes. To improve the performance of the security

[*] Research Scholar, Vel Tech Rangarajan, Dr. Sagunthala R&D Institute of Science and Technology,Chennai-600062, India. & Assistant Professor, CSE Department, KKR&KSR Institute of Technology and Sciences, Andhra Pradesh, India.

[†] Professor, CSE Department, Vel Tech Rangarajan, Dr.Sagunthala R & D Institute of Science and Technology, Chennai-600062, India.

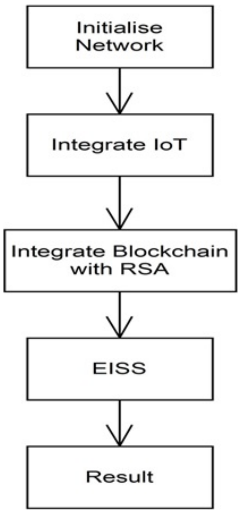

Fig. 1.1. *Architecture Diagram for EISS*

within the nodes which are integrated with IoT and blockchain. All the domains are integrated and called as EISS.

2. Problem Statement. The present problem is addressed in IOT devices is security. Many routing protocols have the problem with security and certainty. Many researches have been done on providing security and predictable issues with IOT and routing protocols. Blockchain is updated technology to improve the security in IOT and routing protocols.

3. Releated Work. A basic security challenge of the IoT originates from its consistently extending edge. In an IoT arrange, hubs at the edge are potential purposes of disappointment where assaults, for example, Distributed Denial-of-Service (DDoS) can be propelled [7]. Inside the IoT edge, a lot of adulterated hubs and gadgets can act together to fall the IoT administration arrangement, as observed as of late in botnet attacks [8].

A main issue of disappointment not exclusively is a danger to accessibility, yet additionally to classification and approval [9]. A concentrated IoT does not give worked in ensures that the specialist co-op won't abuse or alter clients IoT information. Besides, classification assaults emerge from personality parodying and dissecting directing and traffic data. In an information driven economy, ensures are important to anticipate misappropriation of IoT information.

IoT faces classification assaults that emerge from character parodying and examining steering and traffic data, just as uprightness assaults, for example, change assaults and Byzantine directing data assaults [10]. Information honesty in the incorporated IoT arrangement is tested by infusion assaults in applications where basic leadership depends on approaching information streams. IoT information modification, information burglary and personal time can bring about shifting degrees of misfortune. Guaranteeing security is vital in a framework where keen gadgets are required to connect self-ruling and take part in financial exchanges. Current security arrangements in the IoT are incorporated, including outsider security administrations. Utilizing blockchains for security strategy implementation and keeping up openly auditable record of IoT connections, without relying upon an outsider, can demonstrate to be profoundly beneficial to the IoT.

IoT frameworks produce huge volumes of information that require arrange network and power, preparing and capacity assets to change this information into significant data or administrations. Close to dependable availability and system versatility, digital security and information protection of are significant significance in utilizing IoT systems. Right now, unified engineering models broadly used to validate, approve and interface various hubs in an IoT organize. With the developing number of gadgets to many billions, incorporated frameworks will separate and bomb when they brought together server winds up inaccessible. Decentralized IoT design was proposed to understand this issue, wherein it moves away a portion of the system handling assignments to the edge [11]. For example, in haze registering models, a portion of the basic activities that used to be handled by cloud servers are currently relegated to be performed by IoT centers or haze [12]. Distributed (P2P) engineering gives another arrangement, where neighbouring gadgets legitimately connect with one another in lattices to distinguish, verify and trade data without utilizing any incorporated hub or operator between them [13].

4. Block Chain. The blockchain, consists of a chain of blocks. In every block, the data structure is allowed to blockchain to save the transactions done on every block which is linked to the chain by cryptography. In blockchain there are basic fundamental attributes such as Saved, transparent, and decentralized [14]. Every transaction in blockchain is safely and communicate with each other based on the trust-less method, i,e there is no need to believe another device and third parties. Especially in this paper, the blockchain technology is used to save every data into the each block and uses the encryption and decryption with the key. It is very powerful to use the algorithm for security.

5. An Ensemble Integrated Security System (EISS). This section explains about the functionality of the Encryption and decryption algorithm and how the IoT and blockchain are integrated in this. RSA is a very efficient and fast encryption algorithm that is used for securing data with the public-key. In this scenario, RSA is used to provide security at every node which is integrated with blockchain and generates a key for every block. Maintaining the secret keys at the block level is very difficult. The key generation is also very fast for every block and this also maintains the large data at every block. At the network setup, the integration of RSA and blockchain is implemented with the efficient network setup and security. The total no of nodes within the network is based on the data allowed at every node. The integrated system is implemented at network.

The integration of RSA and Block chain at every network is formalized by:

KeyGen:$(E, q, a, b, G, n, h; d, Q)$

where
E is variable with elliptic curve

$$y^2 = x^3 + ax + \frac{b}{Fq} \tag{5.1}$$

q is prime

$$2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \tag{5.2}$$

while $a, b : a = 0, b = 7$
G, n : consider random base point in E with prime order n.
h: hash, instantiated with SHAI
Signing key: $d = [1, n-1]$
Verification key: $Q = dG \in E$
Sign$(d : m)$:

$$(r, s) \in F^2 \tag{5.3}$$

where:
r is the non-zero x-coordinator of point kG for some k←[1,n-1]
s :

$$s = k^{-1}(hm + d \cdot r) \mod n \tag{5.4}$$

Verify $(Q; r, s) : (s, s \in [1, n-1])$ and $(v = r)$, where v=the x-coordinator of point
The hash function used is defined with parameters x, y and z.
The equation is to find the $2y$ numbers a_1,a_2,....,a_{2^y} satisfying the below equations

$$a_j < 2^{(\frac{n}{(y+1)})+1}, j = 1, ., 2^y \tag{5.5}$$

$$h(a_1) \oplus h(a_2) \oplus \ldots \oplus h(a_{2^y}) = 0 \tag{5.6}$$

where h is the Blake2b hash function.

Table 6.1
The performance of the ouath2 with various data sizes (kb)

File size (Kb)	Key Type	Encryption Time (MSec)	Decryption Time (MSec)
10	64Bit	0.987	0.9878
20	64Bit	1.343	1.234
30	64Bit	3.432	2.542
40	64Bit	4.321	3.766

Table 6.2
The performance of the EISS with various data sizes (kb)

File size(Kb)	Key Type	Encryption Time (MSec)	Decryption Time (MSec)
10	256Bit	0.789	0.678
20	256Bit	0.897	0.789
30	256Bit	1.231	0.987
40	256Bit	1.341	1.987

Table 6.3
Overall performance in terms of security and accuracy

Parameters	OAUTH2	EISS
Encryption Time (MS)	2.231	1.098
Decryption Time (MS)	2.432	1.567
Accuracy	78%	97%

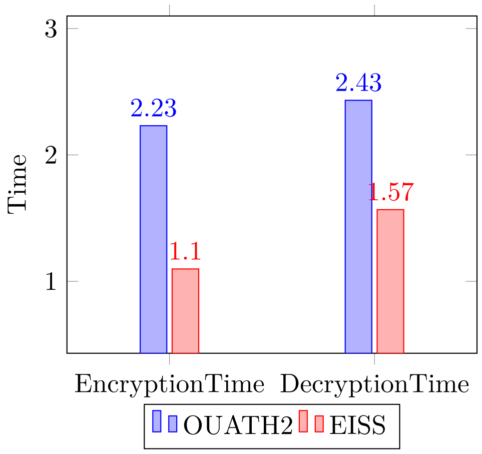

Fig. 6.1. *Variatios in the system*

6. Evolution Results. The experiments are done in UBUNTU operating system, NS3 is used to develop the proposed EISS. To maintain the system speed and performance the compatibility if the implementation is needed. The Processor is I3 or I5. The simulation parameters are such as encryption time, decryption time and accuracy.

Table 6.1–6.3 show the overall performance in terms of security and accuracy. Based on the system performance the result may get variations (Figure 6.1).

7. Conclusion. This paper, mainly focus on providing the security for the routing protocol and data transfer nodes within the network with the integration of blockchain technology to the nodes present in the network and IoT is used to monitor the data transmission between the nodes. With the integration of blockchain and IoT the security is provided very highly to transfer the data within the nodes. To access the data between the nodes the private and public keys are generated with RSA algorithm. According to the EISS the three parameters are calculated to improve the performance of the security and accuracy.

REFERENCES

[1] K. Ashton, *That 'Internet of Things' in RFID J., Jun. 2009.*

[2] R. Minerva, A. Biru,and D. Rotondi, *Towards a definition of the Internet of Things (IoT),* IEEE Internet Initiative, vol. 1, pp. 1-86, 2015.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, *Internet of Things: A survey on enabling technologies protocols and applications*, IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015.

[4] Savelyev, LU-*A. Copyright in the Blockchain era: Promises and challenges*, Comput. Law Secur. Rev. 2018, 34, 550–561.

[5] Kshetri, N, *Blockchain's roles in strengthening cybersecurity and protecting privacy,*Telecommun. Policy 2017, 41, 1027–1038.

[6] Kim, S.-K.; Huh, J.-H, *A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. Energies 2018, 11, 1.*

[7] H. Suo, J. Wan, C. Zou, J. Liu, *Security in the Internet of Things: A review*, Proc. Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE), vol. 3, pp. 648-651, 2012.

[8] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, *DDoS in the IoT: Mirai and other Botnets*, Computer, vol. 50, no. 7, pp. 80-84, 2017.

[9] S. Sicari, A. Rizzardi, C. Cappiello, D. Miorandi, A. Coen-Porisini, *Toward data governance in the Internet of Things*, in New Advances in the Internet of Things, Cham, Switzerland:Springer, pp. 59-74, 2018.

[10] M. U. Farooq, M. Waseem, A. Khairi, S. Mazhar, *A critical analysis on the security concerns of Internet of Things (IoT)*,Int. J. Comput. Appl., vol. 111, no. 7, pp. 1-6, 2015.

[11] Y. Ai, M. Peng, and K. Zhang, *Edge computing technologies for internet of things: a primer*, Digital Communications and Networks, vol. 4, no. 2, pp. 77–86, 2018.

[12] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, Fog computing for the internet of things: Security and privacy issues: IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[13] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and paradigms*, Elsevier, 2016.

[14] Hopali, Egemen and Vayvay, Ozalp(2018). , *Internet of Things (IoT) and its Challenges for Usability in Developing Countries*, IJIESR.1. 6-9

Edited by: Swaminathan JN
Received: Sep 7, 2019
Accepted: Dec 9, 2019