The Blockchain Random Neural Network in Cybersecurity and the Internet of Things

Will Serrano

The Blockchain Random Neural Network in Cybersecurity and the Internet of Things

Will Serrano

Intelligent Systems and Networks Group
Electrical and Electronic Engineering
Imperial College London

g.serrano11@imperial.ac.uk

Abstract. The Internet of Things (IoT) enables increased connectivity between devices; however, this benefit also intrinsically increases cybersecurity risks as cyber attackers are provided with expanded network access and additional digital targets. To address this issue, this paper presents a holistic digital and physical cybersecurity user authentication method based on the Blockchain Random Neural Network. The Blockchain Neural Network connects increasing neurons in a chain configuration providing an additional layer of resilience against Cybersecurity attacks in the IoT. The proposed user access authentication covers holistically its digital access through the seven OSI layers and its physical user identity such as passport before the user is accepted in the IoT network. The user's identity is kept secret codified in the neural weights, although in case of cybersecurity breach, its physical identity can be mined, and the attacker identified, therefore enabling a safe decentralized confidentiality. The validation results show that the addition of the Blockchain Neural Network provides a user access control algorithm with increased cybersecurity resilience and decentralized user access and connectivity.

Keywords: Neural Network, Internet of Things, Blockchain, Cybersecurity, User Management, Access Credentials

1 Introduction

In the Internet of Things (IoT), things are objects of the physical world (physical things) that can be sensed, or objects of the information world (virtual things) that can be digitalized; both are capable of being identified and integrated into information and transmitted via sensor and wired or wireless communication networks [1]. The IoT enables comprehensive connectivity between devices; however, this benefit also intrinsically increases cybersecurity risks as cyber attackers are provided with expanded network access and additional digital targets [2-4].

Blockchain enables the digitalization of contracts as it provides authentication between parties and information encryption of data that gradually increments while it is processed in a decentralized network such as the IoT [5]. Due to these features,

Blockchain has been already applied in Cryptocurrency [6], Smart Contracts [7], Intelligent Transport Systems [8] and Smart Cities [9].

1.1 Research Motivation

To address the increased cybersecurity risk of the IoT, this paper proposes a holistic digital and physical cybersecurity user authentication method based on the Blockchain Random Neural Network [10]. The Blockchain Neural Network connects neurons in a chain configuration providing an additional layer of resilience against Cybersecurity attacks in the IoT. The Cybersecurity and IoT application presented on this paper can be generalized to emulate an Authentication, Authorization and Accounting (AAA) server where user access information is encrypted in the neural weights and stored decentralized servers.

The Blockchain Neural Network solution is equivalent to the Blockchain with the same properties: user authentication, data encryption and decentralization where user access credentials are gradually incremented and learned while travelling or roaming. The Neural Network configuration have analogue biological properties as the Blockchain where neurons are gradually incremented and chained through synapses as variable user access credentials increase; information is stored and codified in decentralized neural networks weights. The main advantage of this research proposal is the biological simplicity of the solution however it suffers high computational cost when the neurons increase.

1.2 Research Proposal

Internet of Things and the Blockchain related work is described in Section 2. The proposed user access authentication described in Section 3 covers holistically its digital access through the seven OSI layers and its physical user identity such as passport ID before the user is allowed to use IoT network resources. The method forces the user to be physically authenticated before establishing the connection that allows access to the IoT network, therefore cybersecurity is increased by reducing the likelihood of criminal network access. The user's digital OSI layer identification such as MAC and IP address and physical identification such as biometrics generates the Private Key whereas there is no need for a Public Key, therefore this paper defines a truly decentralized solution with the same Blockchain validation process: mining the input neurons until the neural network solution is found as presented in Section 4.

Experimental results in Section 5 show that the additional Blockchain neural network provides increased cybersecurity resilience and decentralized confidentiality to user access and connectivity. The main conclusion presented in Section 6 proves that the user physical identity is kept secret codified in the neural weights although in case of cybersecurity breach the identity can be mined and the attacker identified by its passport ID or biometrics.

2 Related work

2.1 Internet of Things

The IoT has provided new services and applications with additional Cybersecurity issues. G. Lee et al [11] present the evolution of the IoT technology started from Machine to Machine to connect machines and devices, Interconnections of Things that connect any physical or virtual object and finally Web of Things that enables the collaboration between people and objects. The IoT is formed of three layers, as proposed by Q. Jing et al [12]: sensor, transportation and application that similar as traditional networks, also have security issues and integration challenges. R. Roman et al [13] state that because physical, virtual and user private information is captured, transmitted and shared by the IoT sensors, Cybersecurity aspects on data confidentiality and authentication, access control within the IoT network, identity management, privacy and trust among users and things; the enforcement of security and privacy policies shall be also considered and implemented. S. Sicari et al [14] declare that the dynamic IoT is formed by heterogeneous technologies to provide innovative services in various application domains which shall meet flexible security and privacy requirements where traditional security countermeasures cannot be directly applied due the different standards, communication protocols and scalability issues because of the high number of interconnected devices. An important challenge for supporting diverse multimedia applications in the IoT is the security heterogeneity of wired and wireless sensor and transmission networks that requires a balance between flexibility and efficiency, as presented by L. Zhou et al [15]. Secure and Safe Internet of Things (SerIoT) was proposed by E. Gelenbe et al [16] to improve the information and physical security of different operational IoT applications platforms in a holistic and cross-layered manner. SerIoT covers areas such as mobile telephony, networked health systems, the Internet of Things, Smart Cities, Smart Transportation Systems, Supply Chains and Industrial Informatics [17]

2.2 Neural Networks in Cryptography

Neural Networks have been already applied to Cryptography; D. Pointcheval [18] presents a linear scheme based on the Perceptron problem or N-P problem suited for smart cards applications. W. Kinzel et al [19] train two multilayer neural networks on their mutual output bits with discrete weights to achieve a synchronization that can be applied to secret key exchange over a public channel. A. Klimov et al [20] propose three cryptanalytic attacks (genetic, geometric and probabilistic) to the above neural network. E. Volna et al [21] apply feed forward neural networks as an encryption and decryption algorithm with a permanently changing key. A. Yayık et al [22] present a two-stage cryptography multilayered neural network where the first stage generates neural network-based pseudo random numbers and the second stage, a neural network encrypts information based on the non-linearity of the model. T. Schmidt [23] et al present a review of the use of artificial neural networks in cryptography.

2.3 Blockchain in Security

Currently; there is a great research effort in Blockchain Algorithms applied to security applications. D. Xu et al [24] propose a punishment scheme based on the action record on the blockchain to suppress the attack motivation of the edge servers and the mobile devices in the edge network. S.-C. Cha et al [25] utilize a blockchain network as the underlying communication architecture to construct an ISO/IEC 15408-2 compliant security auditing system. K. Gai et al [26] propose a conceptual model for fusing blockchains and cloud computing over three deployment modes: Cloud over Blockchain, Blockchain over Cloud and Mixed Blockchain-Cloud. Y. Gupta et al [27] propose a Blockchain consensus model for implementing IoT security. R. Agrawal et al [28] present a Blockchain mechanism that evaluates legitimate presence of user in valid IoT-Zone continuously without user intervention.

3 Blockchain Neural Network in the Internet of Things

Blockchain [6] is based on cryptographic concepts which can be applied similarly by the use of Neural Networks. Information in the Blockchain is contained in blocks that also include a timestamp, the number of attempts to mine the block and the previous block hash. Decentralized miners then calculate the hash of the current block to validate it. Information contained in the Blockchain consists of transactions which are authenticated by a signature that uses the user private key, transaction origin, destination and value (Figure 1).

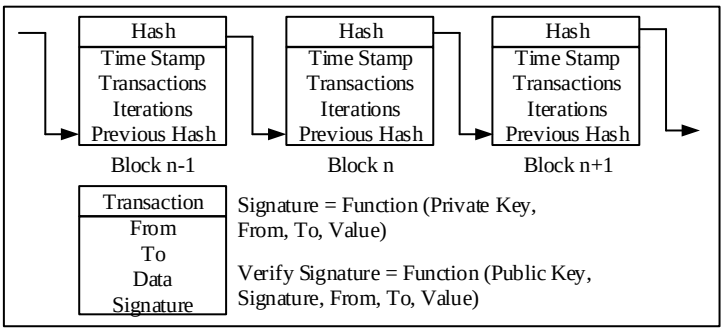


Fig. 1. Blockchain Model

3.1 The Random Neural Network

The proposed Blockchain configuration is based on the Random Neural Network (RNN) [29-31] which is a spiking neuronal model that represents the signals transmitted in biological neural networks, where they travel as spikes or impulses, rather than as analogue signal levels. The RNN is a spiking recurrent stochastic model for neural networks where its main analytical properties are the "product form" and the existence of the unique network steady state solution.

3.2 The Random Neural Network with Blockchain configuration

The Random Neural Network with Blockchain configuration consists of L Input Neurons, M hidden neurons and N output neurons Network (Figure 2). Information in this model is contained networks weights $w^+(j,i)$ and $w^-(j,i)$ rather than neurons x_L, z_M, y_N.

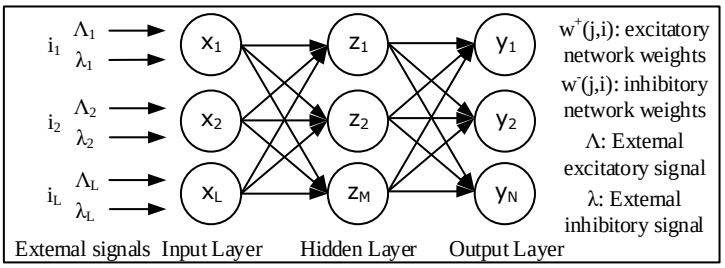


Fig. 2. The Random Neural Network structure

- $I = (\Lambda_L, \lambda_L)$, a variable L-dimensional input vector $I \in [-1,1]^L$ represents the pair of excitatory and inhibitory signals entering each input neuron respectively; where scalar L values range $1<L<\infty$;
- $X = (x_1, x_2, \dots, x_L)$, a variable L-dimensional vector $X \in [0,1]^L$ represents the input state q_L for the neuron L; where scalar L values range $1<L<\infty$;
- $Z = (z_1, z_2, \dots, z_M)$, a M-dimensional vector $Z \in [0,1]^M$ that represents the hidden neuron state q_M for the neuron M; where scalar M values range $1<M<\infty$;
- $Y = (y_1, y_2, \dots, y_N)$, a N-dimensional vector $Y \in [0,1]^N$ that represents the neuron output state q_N for the neuron N; where scalar N values range $1<N<\infty$;
- $w^+(j,i)$ is the (L+M+N) x (L+M+N) matrix of weights that represents from the excitatory spike emission from neuron i to neuron j; where $i \in [x_L, z_M, y_N]$ and $j \in [x_L, z_M, y_N]$;
- $w^-(j,i)$ is the (L+M+N) x (L+M+N) matrix of weights that represents from the inhibitory spike emission from neuron i to neuron j; where $i \in [x_L, z_M, y_N]$ and $j \in [x_L, z_M, y_N]$.

The main concept of the Random Neural Network Blockchain configuration is that the neuron vector sizes, L, M and N are variable instead of fixed. Neurons or blocks are iteratively added where the value of the additional neurons consists on both the value of the additional information and the value of previous neurons therefore forming a neural chain. Information in this model is transmitted in the matrixes of network weighs, $w^+(j,i)$ and $w^-(j,i)$ rather than in the neurons. The input layer X represents the user's incremental verification data; the hidden layer Z represents the values of the chain and the output layer Y represents the user Private Key.

4 Cybersecurity and the Internet of Things Blockchain Model

Cybersecurity and the Internet of Things in the Neural Network Blockchain model described in this section is based on the main concepts shown on Figure 3:

- Private key, y_N;
- Roaming, R(t) and Verification, V;
- Neural Chain network and Mining;
- Decentralized information, $w^+(j,i)$ and $w^-(j,i)$.

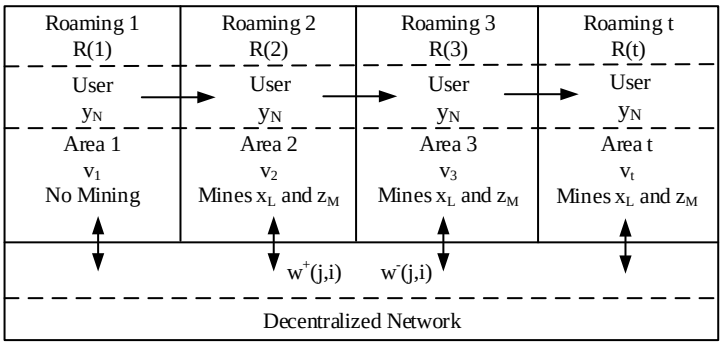


Fig. 3. Cybersecurity and the Internet of Things in the neural Blockchain Model

4.1 Private key

The private key $Y = (y_1, y_2, \dots, y_N)$ consists on the user digital AAA authentication credentials that covers the seven layers of the OSI model and physical information such as a passport, biometrics or both. The private key is presented by the user every time its credentials require verification from the accepting roaming node (Table 1).

Table 1. Private Key

Private Key	Bits	Reference	Type	Interface
y_8	72	User	Physical	Passport - Biometrics
y_7	16	Web	Digital	OSI Layer 7
y_6	16	Middleware		OSI Layer 6
y_5	16	Socket		OSI Layer 5
y_4	16	Port		OSI Layer 4
y_3	32	IP		OSI Layer 3
y_2	48	MAC		OSI Layer 2
y_1	16	Bit		OSI Layer 1

4.2 Roaming and Verification

Let's define Roaming and Verification as:

- Roaming, R(t) = {R(1), R(2), … R(t)} as a variable vector where t is the roaming number;
- Verification, V = {v_1, v_2, … v_t} as a set of t I-vectors where v_o = (e_{o1}, e_{o2}, … e_{oI}) and e_o are the I different dimensions for o=1,2, ... t.

The first Roaming R(1) has associated an input state X = x_I which corresponds to v_1 and represents the user verification data. The output state Y = y_N corresponds to the user Private Key and the hidden layer Z = z_M corresponds to the value of the neural chain that will be inserted in the input layer for the next roaming.

The second Roaming R(2) has associated an input state X = x_I which corresponds to the user verification data v_1 for the first Roaming R(1), the chain (or the value of the hidden layer z_M) and the additional user data v_2. The output state Y = y_N still corresponds the user Private Key and the hidden layer Z = z_M corresponds to the value of the neural chain for the next transaction. This process iterates as more user verification data is inserted. The neural chain can be formed of the values of the entire hidden layer neurons, a selection of neurons, or any other combination to avoid the reverse engineering of the user identity from the stored neural weights.

4.3 Neural Chain Network and Mining

The first Roaming R(1) calculates the Random Neural Network neural weights with an E_k < Y for the input data I = (Λ_L, λ_L) and the user private key Y = y_N. The calculated network weights $w^+(j,i)$ and $w^-(j,i)$ are stored in the decentralized network and are retrieved in the mining process. After the first Roaming; the user requires to be validated at each additional Roaming with its private key where its verification data is validated and verification data v_t from Roaming R(t) are added to the user.

Verification data is validated or mined by calculating the outputs of the Random Neural Network using the transmitted network weighs, $w^+(j,i)$ and $w^-(j,i)$ at variable random inputs i, or following any other method. The solution is found or mined when quadratic error function E_k is lesser than determined minimum error or threshold T:

$$E_k=\frac{1}{2}\sum_{n=1}^{N}\left(y'_n-y_n\right)^2<T \tag{1}$$

where E_k is the minimum error or threshold, y'_n is the output of the Random Neural Network with mining or random input I and y_n is the user Private Key. The mining complexity can be tuned by adjusting E_k. The Random Neural Network with Blockchain configuration is mined when an Input I is found that delivers an output Y with an error E_k lesser than a threshold T for the retrieved user network weights $w^+(j,i)$ and $w^-(j,i)$.

When the solution is found, or mined, the user data can be processed; the potential value of the neural hidden layer $Z = z_M$ is added to form the Neural Chain as the input of the next transaction where more user data is added. Then, the system calculates the Random Neural Network with gradient descent learning algorithm for the new pair (I, Y) where the new generated network weights $w^+(j,i)$ and $w^-(j,i)$ are stored in the decentralized network. The more roaming and verification data; the validation or mining process increases on complexity.

4.4 Decentralized Information

The user network weights $w^+(j,i)$ and $w^-(j,i)$ are stored in the decentralized network rather than its data I directly where I is calculated with the mining process. The network weights expand as more verification data is inserted creating an adaptable method. In addition; only the user Data can be extracted when the user presents its biometric key therefore making secure to store information in a decentralized system.

5 Neural Blockchain in Cybersecurity and IoT Validation

This section proposes a practical validation of the Neural Blockchain model in the Internet of Things and Cybersecurity using the network simulator Omnet ++ with Java for a network of ten nodes. The three independent experiments will emulate a Bluetooth network with roaming validation of MAC addresses, WLAN network with roaming validation of MAC and IP addresses and LTE Mobile network with a roaming validation of MAC and IP and user Passport (Table 2).

Table 2. Neural Blockchain in IoT and Cybersecurity Validation – Node values

Type	Use	Coverage	Layer	Node Vt	User y_N
Bluetooth Master	Room Floor	10m $3140m^2$	MAC	48 bits 01-23-45-67-89-XX	48 bits 01-23-45-67-89-AB
Wireless LAN Access Point	Building Campus	100m $0.314km^2$	MAC-IP	48+32 bits 192.168.11.XX	48+32 bits 192.168.11.11
Mobile LTE Base Station	City Country	1km $31.4km^2$	MAC-IP PASSPORT	48+32 bits N/A	48+32+72 bits VGD12345F

The user is assigned a private key y_N that requires validation before is allowed to transmit. When the user travels through the space, the credential private key is validated by the roaming node; the decentralized system retrieves the neural weights associated to the private key; mines the block, adds the node code and stores back the network weights in the decentralized system. This validation considers mining as the selection of random neuron values until $E_k < T$. When the user roams, the private key is presented and the information of the node (MAC and IP address) v_t is added to the neural chain once it is mined. Each bit is codified as a neuron however rather than the binary 0-1, neuron potential is codified as 0.25 – 0.75 (Figure 4); this approach removes overfitting in the learning algorithm as neurons only represent binary values.

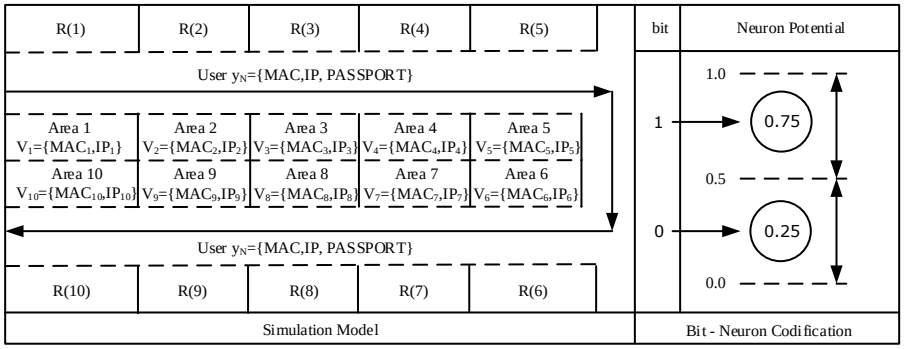


Fig. 4. Neural Blockchain in Cybersecurity validation

The simulations are run 100 times for a Bluetooth MAC Network (Table 3). The information shown is the number of iterations the Random Neuron Network with Blockchain configuration requires to achieve an E_k < 1.0E-10; the error E_k, the number of iterations to mine the Blockchain and the number of neurons for each layer; input x_L, hidden z_M and output y_N.

Table 3. Bluetooth MAC Simulation – Learning and Mining

Roaming	Learning Iteration	Learning Error	Mining Iteration	Mining Threshold	Mining Error E_k	Number of Neurons (x_L, z_M, y_N)
1	233.00	9.96E-11	36.22	1.00E-05	2.48E-06	48-4-48
2	190.52	9.46E-11	24.88	1.00E-05	3.30E-06	100-4-48
3	171.42	9.40E-11	56.32	1.00E-05	3.01E-06	152-4-48
4	160.90	9.18E-11	758.37	1.00E-05	3.97E-06	204-4-48
5	150.67	9.12E-11	109.10	1.00E-05	3.64E-06	256-4-48
6	144.31	9.43E-11	116.59	1.00E-05	3.13E-06	308-4-48
7	140.00	9.47E-11	354.38	1.00E-05	3.09E-06	360-4-48
8	137.00	9.06E-11	2134.31	1.00E-05	3.70E-06	412-4-48
9	132.99	8.75E-11	12.13	1.00E-05	3.56E-06	464-4-48
10	131.00	9.30E-11	141.99	1.00E-05	3.26E-06	516-4-48

With four neurons in the hidden layer, the number of learning iterations gradually decreases while the number of input neurons increases due the additional information added when roaming between nodes. The results for the mining iteration are not as linear as expected because mining is performed using random values (Figure 5). Surprisingly; mining is easier in some Roaming stages when it would have been expected harder as the number of neurons increases.

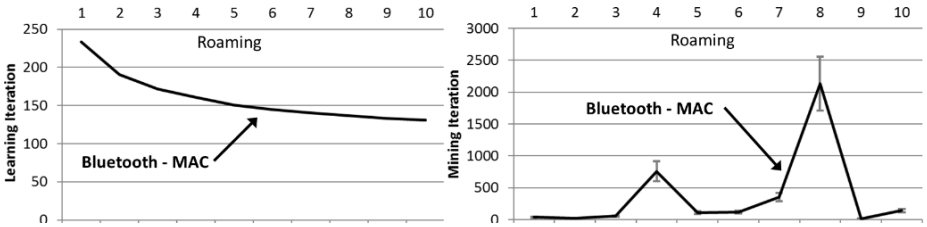


Fig. 5. Bluetooth MAC Simulation – Learning and Mining

The Blockchain Random Neural Network algorithm shall detect tampering to be effective (Table 4) where Δ represents the number of tampered bits.

Table 4. Bluetooth and WLAN Simulation – Tampering Error

Roaming	Bluetooth - MAC			WLAN - IP		
	Error Δ=0.0	Error Δ=1.0	Neurons (X_L, Z_M, Y_N)	Error Δ=0.0	Error Δ=1.0	Neurons (X_L, Z_M, Y_N)
1	9.96E-11	1.31E-03	48-4-48	9.28E-11	1.18E-03	80-4-80
2	9.49E-11	1.50E-04	100-4-48	9.57E-11	1.63E-04	164-4-80
3	9.18E-11	4.32E-05	152-4-48	9.36E-11	5.21E-05	248-4-80
4	9.38E-11	1.95E-05	204-4-48	9.50E-11	2.23E-05	332-4-80
5	9.01E-11	8.54E-06	256-4-48	9.21E-11	1.02E-05	416-4-80
6	9.07E-11	4.28E-06	308-4-48	9.36E-11	5.22E-06	500-4-80
7	9.49E-11	2.56E-06	360-4-48	9.12E-11	3.07E-06	584-4-80
8	9.33E-11	1.71E-06	412-4-48	9.28E-11	2.10E-06	668-4-80
9	8.93E-11	9.00E-07	464-4-48	9.25E-11	1.15E-06	752-4-80
10	9.59E-11	7.22E-07	516-4-48	9.55E-11	7.81E-07	836-4-80

The effects of tampering the Neural Block Chain (Figure 6) is detected by the learning algorithm even when the tampered values only differ in a bit, Δ=1.0, although this error reduces with an incrementing roaming as the number of neurons increases. Both Bluetooth and WLAN Networks perform similarly.

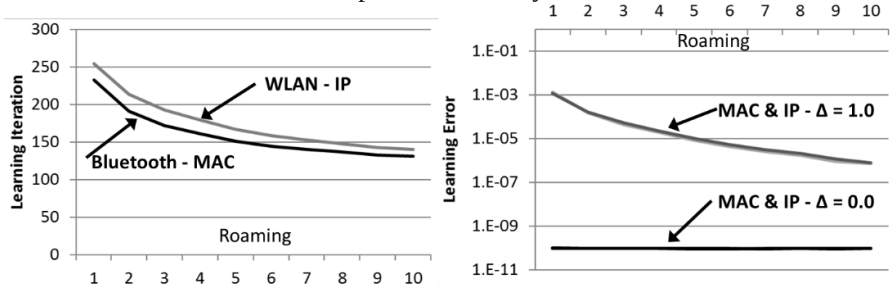


Fig. 6. Bluetooth and WLAN Simulation – Tampering Error

6 Conclusions

This paper has presented the application of the Blockchain Random Neural Network in Cybersecurity and the IoT where neurons are gradually incremented as user validation data increases through travelling and roaming, although this research can be generalized to any AAA server or Access Control solution. This configuration provides the proposed algorithm the same properties as the Blockchain: security and decentralization with the same validation process: mining the input neurons until the neural network solution is found.

The Random Neural Network in Blockchain configuration has been applied to an IoT AAA server that covers the digital seven layers of the OSI Model and the physical user credentials such as Passport or biometrics. Experimental results show that Blockchain applications can be successfully implemented using neural networks with a gradually increased mining effort, user authentication and data encryption in a decentralized network therefore removing centralized validation mechanisms.

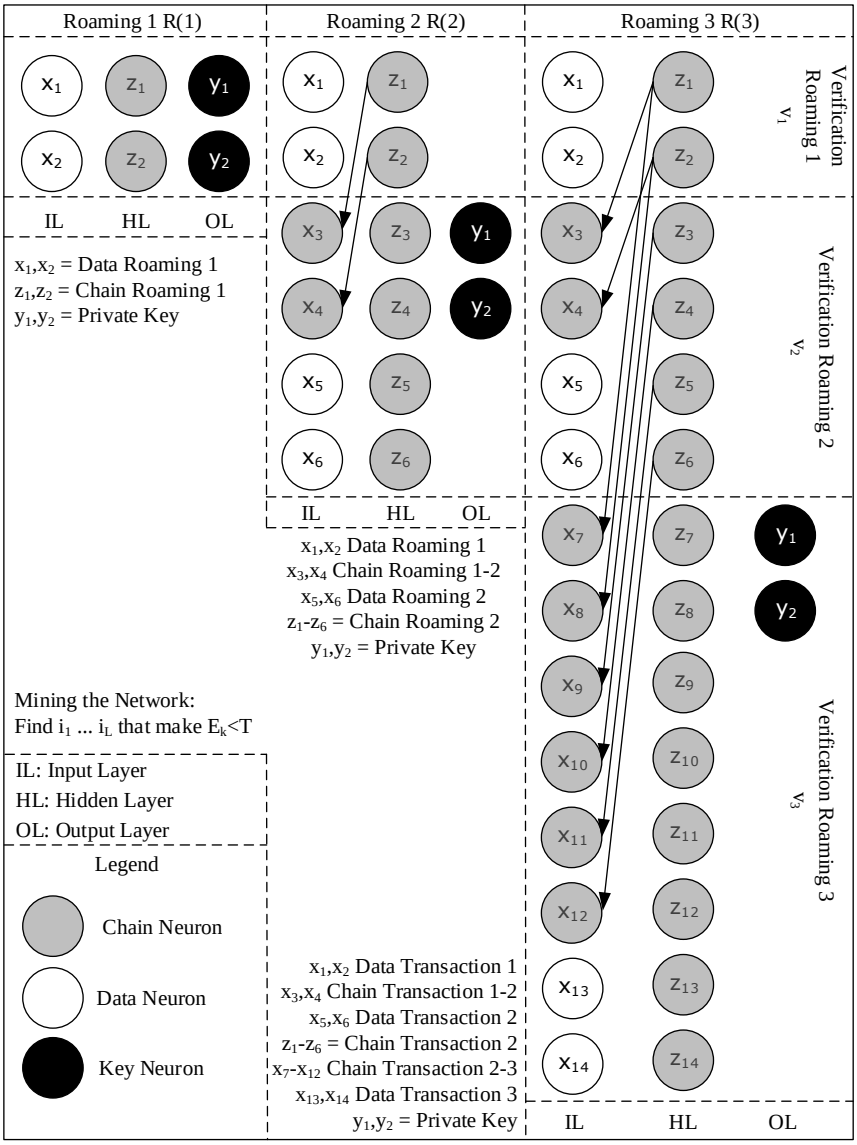
This paper has provided a holistic physical and digital Cybersecurity application in the IoT where access to the network in an area requires prior user physical verification between decentralized parties. User data is encrypted, information is decentralized where attackers can be identified if a criminal attack is delivered.

References

1. International Telecommunication Union. Overview of the Internet of Things. Y.2060. (2012), 1-22.
2. I. Andrea, C. Chrysostomou, G. Hadjichristofi. Internet of Things: Security Vulnerabilities and Challenges. IEEE Symposium on Computers and Communication. (2015), 180-187.
3. J. Deogirikar, A. Vidhate. Security attacks in IoT: A survey. IEEE International Conference on IoT in Social, Mobile, Analytics and Cloud. (2017), 32-37.
4. J. Granjal, E. Monteiro, J. Sá Silva. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials 17, 3. (2015), 1294-1312.
5. S. Huh, S. Cho and S. Kim. Managing IoT devices using Blockchain platform. International Conference on Advanced Communication Technology. (2017), 464-467.
6. S Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org. (2008), 1-9.
7. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami. Blockchain contract: Securing a blockchain applied to smart contracts. International Conference on Consumer Electronics. (2016), 467-468.
8. Y. Yuan and F.-Y. Wang. Towards blockchain-based intelligent transportation systems. International Conference on Intelligent Transportation Systems. (2016), 2663-2668.
9. K. Biswas and V. Muthukkumarasamy. Securing Smart Cities Using Blockchain Technology. International Conference High Performance Computing and Communications / Smart City / Data Science and Systems. (2016), 1392-1393.
10. W Serrano. The Random Neural Network with a Blockchain Configuration in Digital Documentation. International Symposium on Computer and Information Sciences. (2018), 196-210.

11. G. Lee, N. Crespi, J. Choi, M. Boussard. Internet of Things. Telecommunication Services Evolution. LNCS 7768. (2013), 257-282.
12. Q. Jing, A. Vasilakos, J. Wan, J. Lu, D. Qiu. Security of the Internet of Things: perspectives and challenges. Wireless Netw 20. (2014), 2481-2501.
13. R. Roman, P. Najera, J. Lopez. Securing the Internet of Things. IEEE Computer Society 0018-9162. (2011), 51-58.
14. S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks 76. (2015), 146-164.
15. L. Zhou, H. Chao. Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network, 0890-8044. (2011), 35-40.
16. E. Gelenbe, J. Domanska, T. Czàchorski, A. Drosou, D. Tzovaras. Security for Internet of Things: The SerIoT Project. IEEE International Symposium on Networks, Computers and Communications. (2018), 1-5.
17. J. Domańska, M. Nowak, S. Nowak, T. Czachórski. European Cybersecurity Research and the SerIoT Project. International Symposium on Computer and Information Sciences. (2018), 66-173
18. D. Pointcheval. Neural Networks and their Cryptographic Applications. Livre des resumes Eurocode Institute for Research in Computer Science and Automation. (1994), 1-7.
19. W. Kinzel and I. Kanter. Interacting Neural Networks and Cryptography Secure exchange of information by synchronization of neural networks. Advances in Solid State Physic, 42. (2002), 383-391.
20. A. Klimov, A. Mityagin and A. Shamir. Analysis of Neural Cryptography. International Conference on the Theory and Application of Cryptology and Information Security, 2501. (2002), 288-298.
21. E. Volna, M. Kotyrba, V. Kocian and M. Janosek. Cryptography based on the Neural Network. European Conference on Modelling and Simulation. (2012), 1-6.
22. A. Yayık and Y. Kutlu. Neural Network based cryptography. International Journal on Neural and Mass - Parallel Computing and Information Systems, 24, 2. (2014), 177-192.
23. T. Schmidt, H. Rahnama and A. Sadeghian. A review of applications of artificial neural networks in cryptosystems. World Automation Congress. (2008), 1-6.
24. D. Xu, L. Xiao, L. Sun, M. Lei. Game theoretic study on blockchain based secure edge networks. IEEE International Conference on Communications in China. (2017), 1 – 5.
25. S.-C. Cha, K.-H. Yeh. An ISO/IEC 15408-2 Compliant Security Auditing System with Blockchain Technology. IEEE Conference on Communications and Network Security. (2018), 1-2.
26. K. Gai, K.-K. Raymond, L. Zhu. Blockchain-Enabled Reengineering of Cloud Datacenters. IEEE Cloud Computing, 5, 6. (2018), 21-25.
27. Y. Gupta, R. Shorey, D. Kulkarni, J. Tew. The applicability of blockchain in the Internet of Things. IEEE International Conference on Communication Systems & Networks. (2018), 561 – 564.
28. R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. Anirudh, S. Shekhar. Continuous Security in IoT Using Blockchain. IEEE International Conference on Acoustics, Speech and Signal Processing. (2018), 6423 – 6427.
29. E. Gelenbe. Random Neural Networks with Negative and Positive Signals and Product Form Solution. Neural Computation. 1, (1989), 502-510.
30. E. Gelenbe. Learning in the Recurrent Random Neural Network. Neural Computation. 5, (1993), 154-164.
31. E. Gelenbe. G-Networks with Triggered Customer Movement. Journal of Applied Probability. 30, (1993), 742-748.

Appendix


Roaming 1 R(1)
Roaming 2 R(2)
Roaming 3 R(3)
Verification Roaming 1
Verification Roaming 2
Verification Roaming 3
IL HL OL
x1,x2 = Data Roaming 1
z1,z2 = Chain Roaming 1
y1,y2 = Private Key
x1,x2 Data Roaming 1
x3,x4 Chain Roaming 1-2
x5,x6 Data Roaming 2
z1-z6 = Chain Roaming 2
y1,y2 = Private Key
Mining the Network:
Find i1 ... iL that make Ek<T
IL: Input Layer
HL: Hidden Layer
OL: Output Layer
Legend
Chain Neuron
Data Neuron
Key Neuron
x1,x2 Data Transaction 1
x3,x4 Chain Transaction 1-2
x5,x6 Data Transaction 2
z1-z6 = Chain Transaction 2
x7-x12 Chain Transaction 2-3
x13,x14 Data Transaction 3
y1,y2 = Private Key