International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

EMPIRICAL ANALYSIS AND SURVEY FOR AUTHENTICATION SCHEME USING BY CRYPTOSYSTEM

S.Sengamala barani[1], Dr. R. Durga[2]

[1]Research Scholar,Department of Computer Science,VISTAS,Chennai,India

[2]Associate Professor,Department of Computer Science,VISTAS,Chennai,India

Email:priya.barani08@gmail.com[1],drrdurgaresearch@gmail.com[2]

ABSTRACT

In recent years, establishment of secure communication channel over a public network has been considered as one of the most significant challenge in network applications. Conventionally, asymmetric cryptography is commonly utilized technique to produce a key between two users and to transfer it by means of an unsafemedium. Nonetheless, approaches utilized this mechanism, such as Rivest–Shamir–Adleman (RSA) technique and Diffie-Hellmankey exchange (DH) algorithm have faced lot of issues and there is a necessity to develop efficient approach to generate key that can provide high security. DH is a basic key exchange technique that employs asymmetric keys to exchange the secret key distributed by only two parties over unencrypted networks. However, limitations faced by DH algorithm can be solved by introducing Neural Key Exchange (NKE) technique, which is purely dependent upon neural network and it is somewhat same as that of DH algorithm. The only difference is that it is solely dependent on mutual learning or mutual synchronization in the artificial neural network (ANN)rather than discrete logarithmic constraints. In this article, 25 papers are taken into an accountwith respect todiverse secure authentication mechanism with neural key based on blockchain techniques, which are effectively used for effective secure authentication over networks. The categorization methods are divided into five methods, such as deep-learning-based method, optimization, chaos, mutual learning, and cryptography-based methods and constraints and challenges faced by classical approaches are revealed in this survey. In addition, the evaluation is performed depending upon research using classification techniques, tool used, publication year, and evaluation metrics.

KEYWORDS: *Authentication; Blockchain; Key exchange protocol; Neural Key Exchange (NKE), Neural Networks (NNs)*

International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

INTRODUCTION

Developing a safe communication over public network is the significant problems in network applications. The classical private key modelis employed to compressdata utilizing confidential keys that are distributed among particular parties for safe communication. Generally, key exchange protocol dependent on public key model by means of an unsafemediumis developed to distributeconfidential keys among parties without the interpretation of third party. However, DH is a basic key exchange technique that employs asymmetric keys that grants permission to process more than two users to create secret keys distributed by two individuals over unencrypted networks. The privacy of DH is solely dependent upon discrete logarithmic issue. However, the DH algorithm will no longer be secure at any cost [1]. In order to address the limitations faced by DH algorithm, NKE is introduced and the structure of NKE is somewhat identical to that of DH algorithm but, the only difference is that it is based on mutual learning in the ANN rather than discrete logarithmic issue. In neural synchronization, two usersmatch their weights in the neural network (NN) by means of an unsafe channel. In fact, they choose the identical NNarchitecture and input vectors are considered as shared factors and unevenly choose corresponding weights present inside the structure.

Generally, NKE is another latest method for refining a symmetrical key by employing neural networks [3]. When speaking about shared environment, safe interaction in unsafe networks is highly significantproblem that must be resolved immediately. Therefore, user authentication and secret key revealing become the significant services for communication networks. A general characteristic of traditional password authentication method is that they utilize a verification list. An example for remote user authentication technique is the password-based user authentication method, which is the highly utilized and less cost mechanism. It is a fundamental feature to authorize confidential files, photos, bank accounts, and many other private files. However, this category of authentication model is time consuming process [8]. Blockchain technology is considered as an intelligent technology that has been used in many research areas and industrial arenas. In blockchain structure, each block is comprised with two parts, such as block head and block. On the other hand, block header consists of two groups of metadata, one is associated with mining, whereas other is related to the block itself [10].

The ultimate intention of this survey is to evaluate the diverse secure authentication mechanism with neural key based on blockchain techniques for effective authentication over networks. A NKE mechanism runs based on neural synchronization of the NN that exchanges the secret key. However, research gaps existed in the existing techniques of NKE mechanism based on blockchain is analyzed in this survey. Here, 25 research papers are considered for analyzing various secure authentication mechanism with neural key based on blockchain techniques and they are differ from each other based on some characteristics. The adopted methods are analyzed through tool set, techniques used, evaluation parameter utilized and publication year. The drawbacks pointed on the survey papers are elaborated in research gaps and limitations section. Therefore, the research gaps section drives the motivation for future development of secure authentication mechanism with neural key techniques.

The article is arranged as beneath: Section 1 delineates introduction of secure authentication mechanism with neural key based on blockchain techniques. Section 2 deliberates motivation of this analysis and corresponding works associated with the classification of neural key exchange techniques are discussed in 3rdsection. Moreover, section 4 describes the research gaps and constraints and the analysis are explained in 5thsection. Finally, last section concludes the work.

MOTIVATION

A NKE is a secret key exchange approach dependent on neural synchronization of NN. As the neural key exchange is dependent on weights inside NN architecture, algorithm's privacy does not rely on intruder's computational abilities. Nevertheless, because of the repetition of neural key exchange's mutual learning mechanism, utilizing explicit user authentication techniques like public key certificate is ineffective because of maximum communication overhead. Hence, this survey analyzes various techniques corresponding to secure authentication mechanism with neural key based on blockchain techniques, which motivates the researchers to analyze various techniques and to make a better decisions based on the analysis.

LITERATURE SURVEY

This section deliberates various secure authentication mechanism with neural key based on blockchain techniques from various research papers. Such technique can be widely categorized into five types, namely deep learning-based method, optimization-based method, chaos-based method, cryptography-based method, and mutual learning-based method. The categorization of

International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

secure authentication mechanism with neural key based on blockchain techniques is depicted in Figure 1.

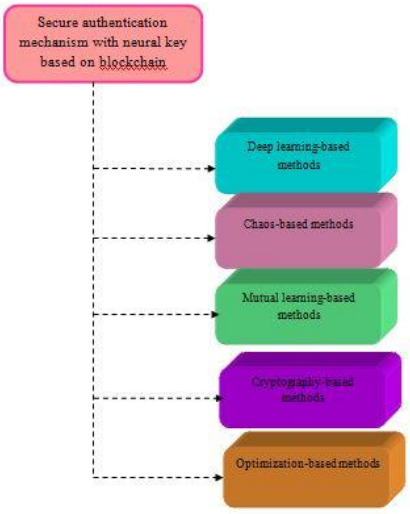


FIGURE 1. CLASSIFICATION OF SECURE AUTHENTICATION MECHANISM WITH NEURAL KEY BASED ON BLOCKCHAIN TECHNIQUES

A.Deep learning-based methods

The research papers with deep learning-based methods are described as follows: Arindam Sarkar, et al. [2] devised artificial neural group synchronization for secured NKE over public channels. In order to distribute the key via public channel, two Artificial Neural Networks (ANNs) were combined together using mutual learning. The main problem existed in neural coordination was evaluation of synchronization of two users ANN's without the presence of weights. However, classical approaches faced serious problems in coordination measurement that results in low confidentiality of neural coordination. This limitation can be addressed using a mutual learning methodologyfor quick and efficient synchronization of a cluster of ANN's. If a specific threshold was attained, the hash function was utilized to ensure whether all networks were correctly coordinated. This approach utilized the weight vectors values to attain complete coordination among two communication devices. The developed approach had some benefits, such as that it generated a session key through entire binary tree-based group mutual neural synchronization and recommended approach allowed two communication devices among two communication devices to determine full coordination in a quick way.

Arindam Sarkar, [7] developed an efficient model named Double Hidden Layer Neural Networks synchronization mechanism using Generative Adversarial Network (GAN) and mutual learning for cryptographic key exchange protocol. The developed GAN easily detected the intruders that cause serious threatsto the significant data by spoofing, sniffing, and phishing. In order to improve the privacy of synchronization mechanism, GAN created the optimal random sequence of input vector. At the end of synchronization technique, synchronized weight act as a session key. The suggested approach processed the authentication steps in a parallel manner.

Daniel Lee and Ivan Stanimirovic, [15] developed a method that described the working process of general neural networks, how RSA encryption worked out, and deliberated the process of exchanging the secret keys using neural key. The method delivered successful results in exchanging the keys using mathematic form to generate the neural network. The method effectively shared the secret keys among two communication devices without letting in any other un-trusted parties.

Qutaiba I. Ali, and Shefs A. Dawwd, [17] introduced a new light weight highly secured ciphering methodology called on Demand Ciphering Engine (ODCE). The main characteristics included in this methodology was ciphering engine and secret key, which were stored as a secret one and produced either by the user or model administrator. Once the transmission was initialized, the included sides exchanged the secret keys. The main building component considered in this system was Artificial Neural Network (ANN). This approach effectively minimized the quantity of data to be transmitted among the involved parties.

J.K. Mandal, et al. [18] modeled a key generation mechanism dependent on Hopfield Neural Network. At the terminals of Hopfield Neural network, equivalent input and weight vector was produced and this results to generate identical output vector. This output vector was employed for producing secret key for encryption and decryption mechanisms. Here, encryption was carried out using exclusive-OR function among plain-text and secret key, whereas decryption was done at the receiver end using exclusive-OR function among cipher text and generated sameunknown key. The chance of attack for this method was very low. In this technique, there was no possibility to regenerate the message.

B.Chaos-based methods

This section deliberates the chaos-based methods gathered from various existing research works are given as follows: Arindam Sarkar, [5] modeled a chaos-based triple-layer tree parity machine (TLTPM)-guided neural synchronization for establishment of public key exchange protocol. The neural

synchronization was accomplished through a peculiar network structure named tree parity machine (TPM). In some procedures, it caused whole synchronization and weights of two TPMs are equivalent. Such equivalent weights played the role of a secret key. In order to deliver faster synchronization, this research developed a TLTPM structurethat employs logistic chaos-generated random general input vector. The developed model achieved better performance and obtained significant results when compared to other TPM models.

N.N Mosola, et al. [9] developed a client-end encryption and key management model that tackled the attacks affecting the integrity of cloud-hosted data. This developed scheme utilized a chaotic atmospheric calamity to create a fitness parameter and this created random numbers generated the encryption keys. However, strength of encryption key was obtained from chaotic pattern of environmentcalamity. In order to overcome the inherent key management technique, the approach employed a NN to understand the patterns of an encryption key. At the end of the process, key was eliminated to beat possible key attacks.

Arindam Sarkar, et al. [10] designed a chaos-guided artificial neural learning-based session key coordination for industrial internet-of-things (IIoT) to improve privacy of CEI. The classical method did not properly address the problems faced by IIoT networks. In order to solve this problem, a chaos-based triple layer vector-valued neural network (TLVVNN) was developed. In addition, a chaos-based transmission was employed to generate the similar input vector at both source end and destination end. Besides, ANN coordination was adopted for exchange of neural keys among IIoT devices. The findings based on experimentation provided superior performance when compared to other classical techniques.

Arindam Sarkar, [23] developed a chaos-based neural synchronization for establishment of public-key exchange protocol. Here, a peculiar NN structure named TPM was utilized for neural synchronization. Moreover, two TPMs utilized in this method considered the general input and various weights vector and updated the weights by exchanging their result using neural learning rule. In some cases, it produced entire synchronization and the biases of two TPMs become equivalent. In addition, logistic Chaos model based TPM(CTPM) was introduced for quick synchronization. The developed model was robust and shown promising results.

C.Mutual learning-based approaches

The article that utilize the mutual learning-based techniques related to secure authentication mechanism with neural key based on blockchainmethodologies are elaboratelyshown in this part. Ahmed M. Allam, et al. [13] introduced pre-shared secrets to maximize the security level of neural cryptography by verifying the communication. Here, mutual learning was altered so that the reflecting regionsamong

hidden and legalized by two partners. Here, the boundaries were located at two locations, such as straight line path, and circular path. The developed algorithm named Neural Cryptography with Secret Boundaries (NCSB) shown promising results, such that the confidential files can be transferred over the public medium in a safe manner.

Xinyu Lei, et al. [14] developed a two-layer tree-connected feed-forward neural network (TTFNN) system for a neural protocol. The TTFNN inspected two parties, whether they were capable to transfer the multiple bits at each time step. The TTFNN protocol satisfied the conditions properly depending upon the two analytically offered heuristic rules. However, selection of best neural networks was still considered as a major problem.

V. Naveena, and Dr. S. Satyanarayana, [21] introduced neural networks that had the capability to identify well-known cryptographically insecure communication. Here, parity machine (PM) was a NN considered in cryptography to create a key. It was employed mainly for key exchange. In general, TPM structure comprised with input neurons built in the McCulloh-Pitts system. While considering the second layer, network had neurons with particular activation parameters. Here, each PM was defined by three functions, such as hidden neurons, input neurons, and output neurons. The advantage of mutual learning was effective synchronization of networks among two parties without transferring inputs over a public channel.

Ahmed M. Allam, and Hazem M. Abbas, [22] suggested a recursive algorithm that extends the mutual learning mechanism to accomplish the group secure communication. By adopting this algorithm, a cluster of users was capable to distribute a general key. In order to attain this aim, two binary tree models were designed. The developed algorithm had so many benefits, like video and voice conferences.

Arindam Sarkar, [24] modeled a mutual learning-based effective synchronization of neural network for exchanging of neural key. In order to evaluate the entire coordination, a significant approach for evaluating coordination was presented. The networks having the similar output were considered to evaluate the degree of synchronization. The hash was utilized to find if both the networks were entirely synchronized when a limit was crossed. By utilizing the weight vectors, the improved approach provided absolute coordination among two communication parties. This improved method reduced the efficient geometric likelihood. The safety measures were increased for neural key exchange. The method failed to decrease the delay measure.

International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

D.Cryptography-based methods

Some of the secure authentication mechanism with neural key based on blockchain techniques based on cryptography-based methods is briefly elaborated as follows:SayanticaPattanayak, and Simone A. Ludwig, [8] introduced a remote password based authentication system depending upon ANNs. This approach mainly comprisedwith two phases. In the first phase, users communicated with various users in a secure manner. At the second phase, 540 passwords were experimented using diverse classifiers. In addition, the developed approach was highly efficient and accurate authentication method was delivered through this novel technique.

Mayank Gupta, et al. [19] developed a Shamir's scheme for secure sharing of secret keys between two parties with the assistance of neural cryptography. The major contribution of this mechanism was to exchange the secret keys over public channel safely and with minimum computational power. In neural cryptography scenario, the output bits were trained dependent upon the generated output and identical input bits. The dynamics of two structures and their weight vectors was determined to perform a synchronization level along with similarbiases. Moreover, this similar key served the role of common key used for sharing the information between two parties. The developed technique was robust and did not disclose the secret information.

E. Optimization-based methods

Various techniques of secure authentication mechanism with neural key based on optimization-based methods are described as follows: Arindam Sarkar, et al. [4] developed a novel approach to improve the security of Critical Energy Infrastructure (CEI) using Harris' Hawks weight optimization. The security and privacy issues were easily solved using TLVVNN. This suggested approach quickly optimized the weight of neural networks in a quick way for faster coordination. The internal structure of TLVNN comprised with three hidden layers and this made the coordinated weight became session key. The advantage of this approach was creation of session key through mutual neural synchronization.

Arindam Sarkar, et al. [6] developed a Gravitational Search-guided ANN key for secure authentication over public networks. The ANN synchronization was utilized to generate a neural key exchange protocol among two communication entities over a medium for cryptographic services. The developed method offered an optimized model that assists the development of neural key among two devices. Moreover, artificial neural synchronization delivered the benefits of sharing the private key over public medium. The optimal design of neural key reduced the polynomial time. However, the method failed to include any optimization-based algorithms for quicker synchronization.

Daxing Wang, [11] developed an algorithm named genetic algorithm for secure key establishment using neural synchronization. Here, neural cryptography was used, which was generally utilized to share a secret key. However, key production in TPM NN was performed using mutual learning. A quicker synchronization of neural network was achieved from a genetic mechanism by creating the best weights. However, this optimal weight factor was determined using developed genetic algorithm. Meanwhile, the achievement of genetic algorithm was evaluated by changing amouny of hidden and input neurons.

Mohd. Sadim, et al. [12] modeled a hybrid Blowfish (BF) for preventing the data from third parties attacks. Here, secret key was generated as input of NN over a public channel. Using this generated secret key, the confidential files sent over a public medium can be either encrypted or decrypted. For this, initially mutual output bits were generated based on the identical input bits. Moreover, similar time independent vectors were determined to synchronize such interaction networks up to a level. Finally, the general secret key was transferred over public channels. The developed model provided more security when compared to other existing approaches.

Arindam Sarkar, et al. [16] developed a peculiar neural network named DLTPM for efficient neural synchronization mechanism. Here, two DLTPMs acquired general input and various weight vectors and updated their individual weights by exchanging their outcomes using neural learning rules. In certain cases, it resulted in entire synchronization and weight of two DCTMs become same and such similar weights served as a secret key. In order to optimize the weight vector, Whale Optimization Algorithm (WOA) was employed. The developed model provided quick response and achieved high security.

F. Other methods

This section describes the secure authentication mechanism with neural key based on blockchain techniques of various methods.Siwan Noh, and Kyung-Hyune Rhee [1] developed an implicit authentication-based mechanism for effective exchange of keys over network for secure communication. Here, the authors presented a method to distribute the secret keys for implicit authentication dependent onuneven manner of blockchain. This method considerably minimized the communication overhead and it effectively distributed secret information for authentication purposes amonglegitimate users. Moreover, this approach concealed the shared secret key from the third parties because of transparency of blockchain. This method ensured the transparent uneven manner in the trustless structure without the assistance of a trusted third party.

Arindam Sarkar, [3] presented a neural synchronization of optimal structure-based group of NNs. The major intention of this model was to produce a secret key over untrustworthy channel. This research

examined the optimal NN structure for production and definition of a secret key among two authorized entities. Moreover, a TLTPM was introduced to establish the public key exchange protocol. This key exchange protocol can also be employed in wireless medium.

Lela Mirtskhulava, et al. [20] designed a neural key exchange protocol. Encryption was a major requirement for preserving IoT by means of a secure communication. Gnerally, key exchange played a vital role in preserving the significant information through IoT network. Here, the synchronization process was accomplished using hebbian learning rule by balancing weights. The major benefit of this approach was that an attacker took long time to identify the generated key. The main limitation was limited number of samples.

Hailong Yao, et al. [25] designed a homomorphic hash and blockchain based authenticated key exchange protocol. The developed model proved its effectiveness in terms of hash one-way, discrete logarithm and blockchain transaction-level privacyconsideration. The developed model resisted against various attacks and the protocol was more secure and more flexible in all applications.

RESEARCH GAPS AND ISSUES

This section delineates the barriers confronted by diverse secure authentication mechanism with neural key based on blockchain techniques. The method in [1] failed to strengthen the security of neural cryptography and as an outcome it caused communication overhead among the networks and a strong PRNG with sufficient features for input production was not included in [2], as it improves the security of neural coordinating mechanism.In [3], the method did not consider the optimization for optimizing the weight of NN for quick synchronization and the method failed to reduce the network latency in [4]. Moreover, it had enough potential to boost the privacy of neural coordination mechanism.Although the method had huge success rate over all attacks, it failed to resist against geometric attacks [5].The elevation in the bias of NN increased the complexity of an efficient intruder eventually, but it reduced polynomial time of a neural key [6].The method presented in [8] failed to focus on decentralized model and it only used users and servers without any trusted authority.In [9], the approach failed to conduct experimentation on encrypting multi-media digital information and failed to implement crypto system to possess number of rounds for encryption.The method had the inability to reduce the neural coordination latency and also it failed to carry out neural coordination instead of a longer one [10].The developed NCSB algorithm failed to derive the suitable length for the derived secret key [13].However, selection of

International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

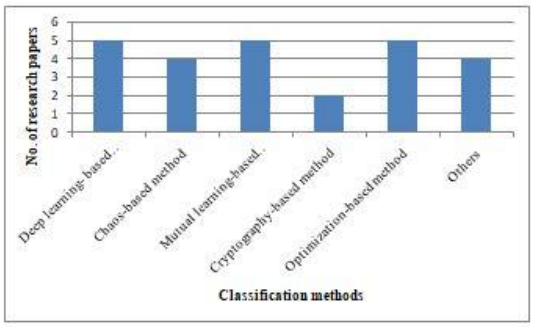
best neural networks was still considered as a major problem in [14]. The method DLTPM-based WOA was incapable to achieve the optimal weights [16]. In [17], the OCDE method failed to block the attackers task due to the production of new cipher engines every time. The only drawback of method developed in [19], is that it failed to use multiple secret images. Moreover, this method had enough potential to preserve the electronic health records. However, the algorithm employed in [22] failed to implement key sharing approach using neural cryptography. The limitation of the technique developed in [24] did not consider any strong PRNG with better statistical characteristics.

ANALYSIS AND DISCUSSION

This part describes the discussion of different secure authentication mechanism with neural key based on blockchain and its classification techniques, evaluation measures, tool used, and publication year are explained in this section.

A. **Analysis using classification models**

This fragmente laborates about the categorization methodologies employed in different secure authentication mechanism with neural key based on blockchain techniques. The classification methods analyzed here are deep learning-based methods, optimization-based models, chaos-based methods, mutual learning-based techniques, and cryptography-based methods. Most of the approaches utilized deep learning-based approaches, optimization-based methods, and mutual learning-based methods, which is used in five research papers. However, four and two research papers utilized chaos-based and cryptography-based techniques. Besides, other than the aforementioned classification methods are employed in four research papers. The evaluation depend upon categorization schemes is illustrated in figure 2.



International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

FIGURE 2. ANALYSIS USING CLASSIFICATION METHODS

B. **Evaluaion based on evaluation metrics**

This fragmented lineates the assessment of secure authentication mechanism with neural key based on blockchain techniques in terms of evaluation metrics and it is shown in figure 3. From the evaluation, it is clear that the highly utilized evaluation metric is communication cost that is employed in seven research papers. The memory usage and computation time metric are used by three research papers, whereas five research papers utilized synchronization time as evaluation metrics. Moreover, computation cost is employed in only two research articles and the metrics other than above said metrics are used in four research papers for evaluation purpose.

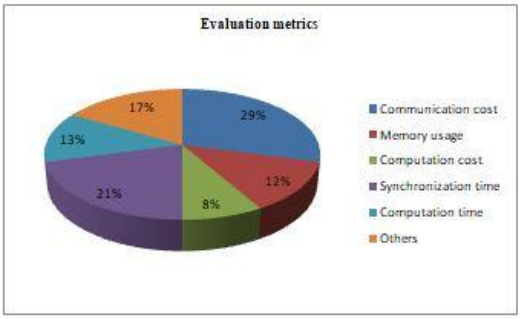


FIGURE 3. ANALYSIS USING EVALUATION MEASURES

C. **Analysis using tool**

The assessment depending upon tool utilized by various secure authentication mechanism with neural key based on blockchain techniques is illustrated in figure 4. The most commonly utilized tool is PYTHON tool, which is employed in 11 research papers while the least utilized tool is MATLAB, which is merely wielded in only three research articles.

International Journal of Multidisciplinary Research in Arts, Science & Commerce (IJMRASC) ISSN Online: 2583-018X

Vol. 4(1), March 2024, pp. 68-82

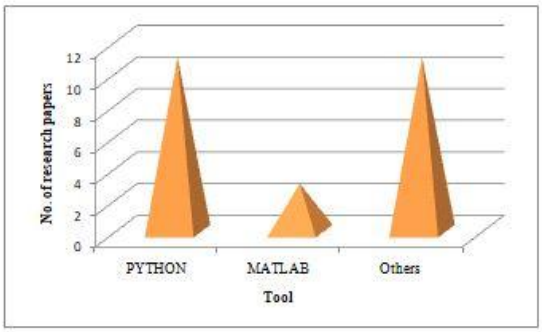


FIGURE 4. ANALYSIS USING TOOL

D. **Analysis using publication year**

This fragment illustrates the evaluation using publication year using various research papers referred for survey is portrayed in figure 5. The years of 2017, 2018, 2019, 2020, and 2021 are reviewed and based on that, two papers are considered from the year 2017 and 2020, while three research papers are acquired from the year 2018. However, 11 research articles are surveyed depending on the year 2021.

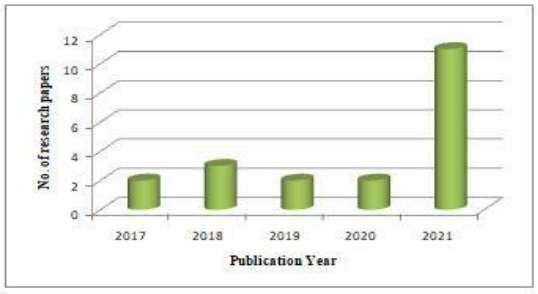


FIGURE 5. ANALYSIS BASED ON PUBLICATION YEAR

CONCLUSION

Establishing a secure communication channel over public networks using secret key is always remains as a huge hurdle and it has been considered as a hot research topics among researchers for the past few years. This survey analyzes the various techniques related to NKE mechanism,

which is a secret key exchange approach dependent upon synchronization of NN. Therefore, this survey analyzed the issues and problems existed in various secure authentication mechanism with neural key based on blockchainmethodologies. Thissurveyis gathered from 25 research articles and techniques are classified into five types, namely deep learning-based method, optimization-based method, mutual learning-based method, chaos-based method, and cryptography-based method. Nevertheless, benefits and limitations related to individual works are deliberated in this survey. The traditional research articles are collected and reviewed form IEEE, Google scholar and so forth. The evaluation is attainedbycategorizationmethods, evaluation measures, tool utilized, and publication year. From the discussion, it is vivid that deep learning-based method, optimization-based method, mutual learning-based methodareutilized in large-scale for all types of applications. Likewise, PYTHON tool is the most commonly utilized metric in more research articles and evaluation measures, such as communication cost, and synchronization time are widely used metrics.

REFERENCES

1. S. Noh and K. H. Rhee, (Nov 2020)“Implicit Authentication in Neural Key Exchange Based on the Randomization of the Public Blockchain”, In IEEE International Conference on Blockchain (Blockchain), pp. 545-549,
2. A. Sarkar, M. Z. Khan and A. Noorwali,(2021) “Secured communication using efficient artificial neural synchronization”, Engineering Applications of Artificial Intelligence, vol.106, pp.104478.
3. A. Sarkar,(2021). “Neural synchronization of optimal structure-based group of neural networks”, Neuro computing, vol.450, pp.156-167.
4. A. Sarkar, M. Z. Khan, and A. Alahmadi, (2021).“Neural weight coordination-based vector-valued neural network synchronization”, Neuro computing, vol.464, pp.507-521.
5. A. Sarkar, (2021).“Chaos-Based Mutual Synchronization of Three-Layer Tree Parity Machine: A Session Key Exchange ProtocolOver Public Channel”, Arabian Journal for Science and Engineering, pp.1-20.
6. A. Sarkar, M. M. Singh, M. Z. Khan, and O. H. Alhazmi,(2021). “Nature-Inspired Gravitational Search-Guided Artificial Neural Key Exchange for IoT Security Enhancement”, IEEE Access, vol.9, pp.76780-76795.
7. A. Sarkar,(2021). “Deep Learning Guided Double Hidden Layer Neural Synchronization Through Mutual Learning”, Neural Processing Letters, vol.53, no.2, pp.1355-1384.

8. S. Pattanayak and S. A. Ludwig,(2018). “A secure access authentication scheme for multiserver environments using neural cryptography”, Journal of Information Assurance and Security, vol.13, no.1, pp.56-65.
9. N. N. Mosola, T.M.Dlamini, J.M.Blackledge, J.H.P.EloffandH.S.Venter,(2017). "Chaos-based encryption keys and neural key-store for cloud-hosted data confidentiality".
10. A. Sarkar, M.Z. Khan and A. Noorwali,(2021). "Chaos-guided neural key coordination for improving security of critical energy infrastructures", Complex & Intelligent Systems, vol.7, no.6, pp.2907-2922.
11. D.Wang,(2015). "Neural synchronization using genetic algorithm for secure key establishment", Journal of Engineering Science and Technology Review, vol.8, no.2, pp.152-156.
12. M. Sadim, N.Pratap, S.Kumar and A.Latoria,(2021)."Hybrid neural synchronization blowfish algorithm for secret key exchange over public channels", Materials Today: Proceedings,.
13. A.M.Allam, H.M. Abbas and M.W.El-Kharashi,(August2013)."Authenticated key exchange protocol using neural cryptography with secret boundaries", In International Joint Conference on Neural Networks (IJCNN), pp. 1-8..
14. X.Lei, X. Liao, F. Chen and T. Huang,(2013). "Two-layer tree-connected feed-forward neural network model for neural cryptography", Physical Review E, vol.87, no.3, pp.032811.
15. D. Leeand I. Stanimirovic,(2018);"Neural Network Key Exchange Protocol for Encrypted Communication", Analysis of applied mathematics, pp.108.
16. A. Sarkar, M.Z. Khan, M.M. Singh, A.Noorwali, C. Chakraborty and S.K. Pani,(2021)."Artificial neural synchronization using nature inspired whale optimization", IEEE Access, vol.9, pp.16435-16447.
17. Q.I.A.S.A Dawwd,"On Demand Ciphering Engine (ODCE) Using Artificial Neural Network (ANN)".
18. J.K. Mandal, D.Datta and A.Sarkar,(2015) "Hopfield network based neural key generation for wireless communication (HNBNKG)", In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), pp. 217-224, Springer, Cham.
19. M.Gupta, M. Gupta and M. Deshmukh,(2020)."Single secret image sharing scheme using neural cryptography", Multimedia Tools and Applications, pp.1-22..
20. L. Mirtskhulava, N.GuluaandN. Meshveliani,(2019)."IoT security analysis using neural key exchange protocol", Computer Science & Telecommunications, vol.57, no.2..
21. V. NaveenaandS. Satyanrayanan, (2019)."Symmetric Cryptography using Neural Networks".
22. A.M. Allam, and H.M. Abbas,(May 2011); "Group key exchange using neural cryptography with binary trees", In 24th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 000783-000786.
23. A. Sarkar,(2021). "Secure exchange of information using artificial intelligence and chaoticsystem guidedneural synchronization", Multimedia Tools and Applications, vol.80, no.12, pp.18211-18241.

24. A. Sarkar,(2021)."Mutual learning-based efficient synchronization of neural networks to exchange the neural key", Complex & Intelligent Systems, pp.1-15.
25. H.Yao, C. Wang, B. Hai and S. Zhu,(August 2018). "Homomorphic hash and blockchain based authentication key exchange protocol for strangers", In Sixth International Conference on Advanced Cloud and Big Data (CBD), pp. 243-248.