I. J. Computer Network and Information Security, **2023, 6, 30-39**
Published Online on December 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.06.03

An Optimized Authentication Mechanism for Mobile Agents by Using Machine Learning

Pradeep Kumar*
JSS Academy of Technical Education, Noida /Department of Computer Science and Engineering, Uttar Pradesh, 201301, India
Shobhit Institute of Engineering & Technology (Deemed to-be-University), Meerut, 250110, India
E-mail: pradeep8984@jssaten.ac.in
ORCID iD: https://orcid.org/0000-0001-6177-8527

Niraj Singhal
Shobhit Institute of Engineering & Technology (Deemed to-be-University), Meerut, 250110, India
E-mail: drnirajsinghal@gmail.com
ORCID iD: https://orcid.org/0000-0002-2614-4788

Mohammad Asim
MGM College of Engineering and Technology, Noida/ Department of computer Science and Engineering, Uttar Pradesh, 201301, India
E-mail: er.mohdasim@gmail.com
ORCID iD: https://orcid.org/0000-0003-2447-479X

Avimanyou Vatsa
Gildart Haase School of Computer Sciences and Engineering, Fairleigh Dickinson University New Jersey USA
E-mail: avatsa@fdu.edu
ORCID iD: https://orcid.org/0000-0001-6694-7967

Received: 08 April 2022; Revised: 21 June 2022; Accepted: 15 August 2022; Published: 08 December 2023

Abstract: A mobile agent is a small piece of software which works on direction of its source platform on a regular basis. Because mobile agents roam around wide area networks autonomously, the protection of the agents and platforms is a serious worry. The number of mobile agents-based software applications has increased dramatically over the past year. It has also enhanced the security risks associated with such applications. Most of the security mechanisms in the mobile agent architecture focus solely on platform security, leaving mobile agent safety to be a significant challenge. An efficient authentication scheme is proposed in this article to address the situation of protection and authentication of mobile agent at the hour of migration of across multiple platforms in malicious environment. An authentication mechanism for the mobile agent based on the Hopfield neural network proposed. The mobile agent's identity and password are authenticate using the specified mechanism at the moment of execution of assigned operation. An evaluative assessment has been offered, along with their complex character, in comparison to numerous agent authentication approaches. The proposed method has been put into practice, and its different aspects have been put to the test. In contrasted to typical client-server and code-on-demand approaches, the analysis shows that computation here is often more safe and simpler.

Index Terms: Mobile Agents, Degree of Mobility, Hopfield Neural Network, Distributing Computing.

1. Introduction

An architecture based on mobile agents (MA)[1] is a modification for distributed computing. A mobile agent is a hyperthreaded independent software that can be deployed throughout a malicious communication environment to accomplish the assigned task. The mobile agent approach allows for a great deal of computational freedom. Client-server processing (in which a service provider provide the services to users), Code-on-Demand Computation [2] (in which a server sends executable file to a client in response to a client request), and Agent-Based Computer technology [3] are the three primary categories of computing. (A mobile agent's intelligent piece of software and process that assigned operation on the basis of owner and migrates from one host computer to another computer automatically.)

Information moves from one user to another in a client server architecture; however, the throughput consumes additional channel capacity. Rather than moving data, a special procedure available in the Mobile agent methodology that migrate from one executing platform to another one, using less network traffic than the client-server model. Figure 1 depicts the use of mobile agents in computing.

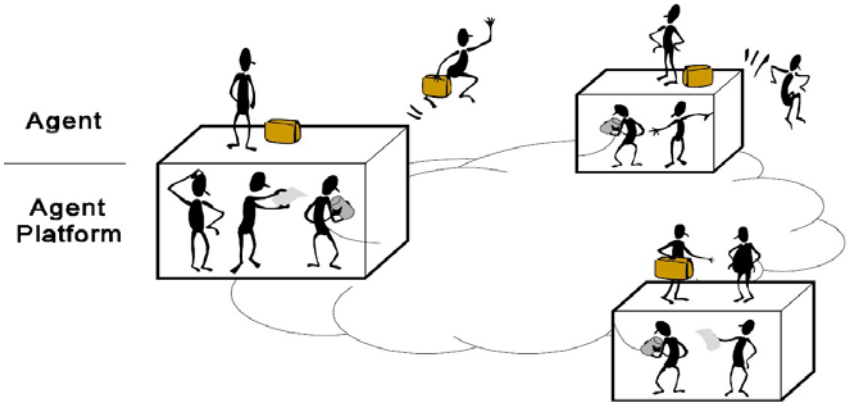

Fig.1. Execution of operation using mobile agent paradigm

Every mobile agent follows a predefined life cycle for the execution of assigned operation by source platform. Mobile agent life cycle[4] shown in Figure 2,when communicating with other agents and platforms.

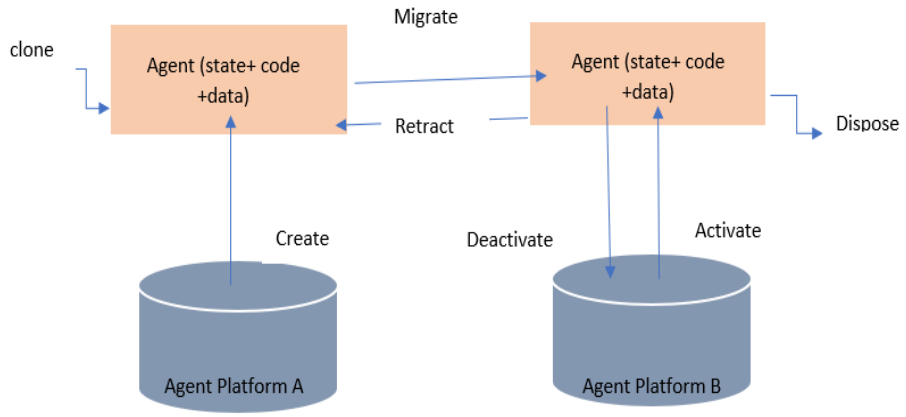

Fig.2. Operation execution life cycle of mobile agent

At the hour of execution of assigned task mobile agent follow a specified life cycle in various stages occur creation of new mobile agent, cloning of mobile agent, dispatch of mobile agent, deactivation of mobile agent, activation of mobile agent, interaction of mobile agent, communication of mobile agent and platform and finally disposal of mobile agent. So, the security [5]of mobile agent in malicious network is prime issue. for the security point of view there are three main parameters play important role Confidentiality (Confidentiality should never be violated throughout interactions by multiple mobile agents or by different executing platforms throughout the life cycle of the agent.), data integrity (Information and data must be in their original state, with no tampering by outsiders. For any safety and health performance of mobile agents, both internal and global systems on which agents migrate for executions, integrity must be maintained). and availability (The term "availability" relates to the accessibility of data and information needed by the system or agents. Both local and remote agents will be able to use the agent platform.)[6].

Besides the aforementioned parameters, users require authentication of the agents' and platform's identities. The protection of mobile agents [7] while propagation on distributed systems is a major challenge in the development of the mobile agent architecture. In previous agent systems, the focus was primarily on determining how agents should work instead of on protection[8]. The majority of the systems fail to provide adequate protection for mobile agents.

It demonstrates the importance of protecting [9] mobile agents in order to provide compatibility between agent frameworks and paradigmatic protection. Safety of mobile agents has received less attention in studies than centralized monolithic computers. As a result, a technique that can operate in a completely secure system [10] is required.

Using a Hopfield neural network, a safe access control strategy for mobile agents in an agent-based framework is proposed in this research. The following is the whole structure of the article. Sections 2 and 3 focused mostly on agent-based frameworks and issue formulation. Sect. 4 gives the proposed approach as well as preliminary information. Sect. 5 discusses the approach's performance review as well as its implementation. Sect. 6 highlights the conclusions as well as future direction to extend that work.

2. Related Works

The major kinds of security risks [11] include information disclosure, denial of service, and information corruption. These types of dangers can be examined in further depth as they relate to the agent paradigm. Mobile agents merely provide more opportunities for exploitation and misuse, dramatically expanding the scope of risks.

Rakesh Kumar proposed a secret share generation mechanism using threshold-based polynomial. When the share is created, the transmission of offers should be possible straightforwardly. In any case, to improve the security and adequacy a two-level encryption has been executed on the share to shield them from any alterations during transmission. During encoding process, contamination is added with each level and hence changes the pixel values with high haphazardness. At the decoding phase, an MLFF backpropagation neural network was used to decode the highly randomized stego share in much less time and with better efficiency. There is no requirement of secure key exchange protocol before transmission of information. The performance of proposed system better as compare to other system.

Hong Zhong [12] proposed a new anonymous secret key sharing mechanism by utilizing Back Propagation Artificial Neural Network (ANN). Propose mechanism can assure that the participants personalities are totally unknown when the private key is revealed. Dissimilar to past scheme, our scheme is an optimum (t, n) edge conspire which threshold value ‘t' doesn't have lower limits and require less extra room. Additionally, stockholders can choose their own shares, and interaction between the dealer and participants does not require a secure connection. Furthermore, members can check the accuracy of their shares as well as the secret key.

Anirban Bhowmik [13]offered a low-computing-overhead robust session key-based secret sharing technique. The proposed approach is built around a new mask creation method as well as CNN and DNA sequence-based key generation. The participants are equal to the order of the unit matrix in the mask method. The transaction and verification keys are created utilizing the CNN and DNA sequence principles. The private data and verification key are distributed among a fixed number of users, and all of these participants can recreate the original message when they work collectively. This is, as far as we understand, the easiest thresholds privacy preserving mechanism. The efficacy and acceptance of our method is demonstrated through a variety of experimental results and analyses.

S. Santhanalakshmi [14]Utilizing neural crypto, developed a fast and safe cooperative key agreement technique. It's helpful, safe, and somewhat effective. Any overlaying architecture is allowed, and intermediary trustworthy nodes are not required. Both methods' efficiency and safety are explored, as well as a technique for improving scalability. The suggested system has an unusual characteristic in that no cryptography is needed for just any key release.

Mohd. Sadim [15]suggested a system for secret key distribution over a malicious network using a hybrid neural synchronizing with blowfish algorithm. Mechanism collaboration with neural network and blowfish symmetric cryptography generate optimal throughput and synchronization as compare to AES and DES.

Supriya Narad [16] discussed One of the most pressing challenges in real life is ensuring the confidentiality of sensitive data that is communicated on a daily basis. he encoding of the actual picture and decoding using produced shares is done using 0.0000 MSE and optimal result in the suggested scheme of (n, n) SSS. The Shamir Secret Sharing Strategy (n, n) is used to establish verification for group-oriented operation. It supports many-to-many verification, allowing for secure group tasks. The Cascade Forward Back-propagation Machine Learning technique is used to encode and decode messages and information, and the correctness is improved in research observations. It ensures that the secret photos and text communications are completely secure. According to the results obtained, there is no loss in the reconstructed images when compared to the initial image. As a result, it demonstrates to be a fully verified system. Decoder with the implemented approach does not involve any sophisticated calculations.

Apdullah Yay_k, [17] proposed a cryptography mechanism based on the neural network. There are two phases to the mechanism. During first phase, neural network-based pseudo-random numbers (NPRNGs) are produced, and the outputs are checked for randomization utilizing randomization standards developed by the National Institute of Standards and Technology (NIST). Throughout the second phase, NPRNGs are utilized to generate a neural network-based cryptographic algorithm. Data that has been encoded using quasi algorithms is subjected to decoding efforts using two equal artificial neural networks in this cryptographic protocol. Quasi encoding is modelled utilizing relationship necessary for the design during first neural network. The second neural net uses judgement capability to retrieve data.

Édgar Salguero Dorokhin [18] This article was written as part of the development of a TPM neural protocol that allows 2 different authorized users to create a 512-bit secret. To accomplish so, experiments have been used to determine the ideal values of K, N, and L, allowing protection against its attacker network to be addressed. This assaulting system attempts to emulate the behavior of the other two systems using a passive assault, obtaining combination with other two model on a single instance. This shows that an encryption key could be transferred with such a frequency of 0.00004 percent with both two authorized parties in a network, allowing an attacker network to replicate the original system behavior. furthermore, a geometrical assault was devised and carried out, with a positive outcome of 0%. Private key of variable size can also be created by changing the values of K, N, and L in a TPM deep net.

Smita Jhajharia [19] proposed method for secret key creation by utilizing Genetic Algorithm with Machine Learning. It was discovered that using GA in PRNGs for initializing input variables in ANN has a viable use, as it solves the problem of recognizing the different value produced by standard PRNGs in ANN, which left it susceptible to hackers once trends in these random values were found. It was discovered that another random variable produced could not be

anticipated based on earlier random value. It's also impossible for all values to have the same number. Repetitions are used to retrieve the keys from the beginning sentence.

J.K. Mandal [20] proposed a secret key generation method based on a Hopfield Neural network using for secure communication in wireless network. At it from both endpoints, Hopfield Neural Networks produce identical input vectors, weight vectors, and output vectors, that are used to create private cryptography and decoding. The cypher text is formed by encrypting plain text with this private key. The plaintext and private are both encrypted using an Exclusive-OR procedure. Exclusive-OR procedure between encrypted output and same private key created has been used to decode at the recipient. The recipient's information is regenerated as an encoded streams by the recipient. The secret key has never been exchanged between the sender and recipient in the HNBNKG method. This method guaranteed that no one could recreate the information while it was being transmitted between sender and receiver because no key was used. This method assured that no one could recover quickly the information while it was being transmitted between sender and recipient because no key was transferred.

After the studying the literature of above researcher in field of mobile agent protection in heterogenous and malicious environment is mainly focused the protection of mobile agent platform at which mobile agent execute the assigned task. Here major prime concern is protection of mobile agent as well as platform during migration.

3. Proposing Modeling

There is a requirement of powerful and effective authentication scheme for mobile agent architecture highly protect. In Conventional security mechanism cryptographic algorithm were used to provide the security of mobile agent paradigm. But in cryptographic mechanism one major challenge is security of private key in malicious environment which is use for encryption as well as authentication. The authentication and security of a mobile agent is totally dependent on the strength of the key created by the agent platform and its safe access control mechanisms. The issue with mobile agent safety starts with the source platform of the agents, which is entirely trustworthy and safe. As during course of its lifetime, this trustworthy atmosphere is hard to migrate to other agent systems. In contrast to the origin hop, an agent's security is weak once it is relocated to some other hop. Depending on several cases, such an agent security method may be acceptable, although it is not ideal in general. A few strategies for identifying unauthorized access to an agent's behavior include execution tracking, incomplete outcome encapsulating, and mutual itinerary tracking. The suggested approach proposes a strategy whereby an agent goes between several platforms to complete a task and preserves itsprivacy utilizing a Hopfield neural network for authentication.

To access the code of mobile agent by any platform or other mobile agents, a non-authenticate platform or attacker require sufficient verification. The proposed approach is based on a Hopfield neural network enabling mobile agent protection. During the life cycle of the mobile agent, an identification key was created and used at the mobile host for execution and verification. Every mobile agent has a private key that is used for verification.

Preliminaries

The basic preliminaries used here such as, Artificial Neural network and Hopfield Neural Network (HNN)

3.1. Artificial Neural Network

Artificial neural networks (ANNs)[21] are software programs influenced by biology that imitate the fact that the human brain functions. ANNs adapt (or are taught) by finding patterns and correlations in data rather than via coding. An ANN [8] is made up of a lot of individual units, also known as artificial neurons or processing elements (PE), which are coupled by coefficients (weights) and structured in layers to form the neural structure. Basic structure of artificial neural network shown on figure 3.

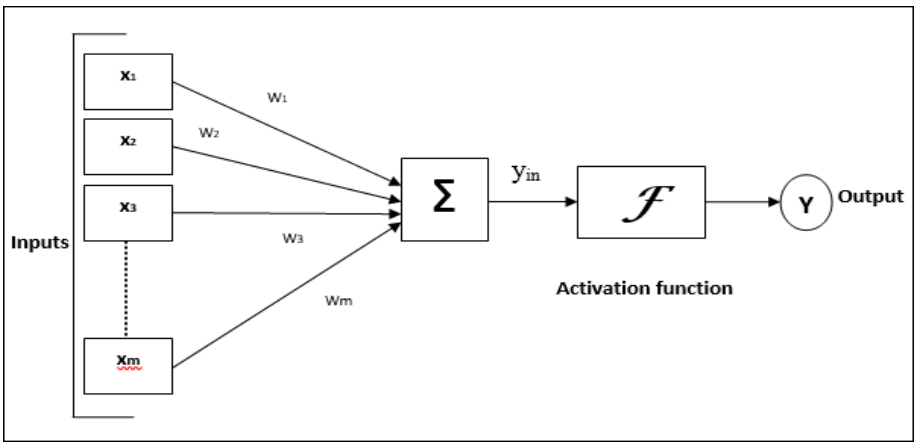

Fig.3. Artificial neural networks

The net input for activation function can be determined using the formula in Eqn-1, for the following architecture of artificial neural network. And generalize formula shown in Eqn-2.

$$y_{in} = w_1x_1 + w_2x_2 + w_3x_3 + w_4x_5 \dots\dots\dots w_nx_n \quad (1)$$

$$\text{i.e., Net input} y_{in} = \sum_{i=1}^{i=n} w_ix_i \quad (2)$$

The activation function can be utilized to the net input to determine the outcome by using Eqn-3.

$$Y_{output} = F(y_{in}) \quad (3)$$

Where *F* is activation function.

Hopfield Neural Network (HNN): In 1982, Dr. John J. Hopfield developed the Hopfield neural network[22]. It is made up with one or even more fully linked recurring neurons in a thin layer. Hopfield neural network is used for many applications like auto association of task and optimization of task in the field of engineering, medical sector, storage of information, supervised learning etc.

3.2. Discrete Hopfield Neural Network

Discrete Hopfield neural networks (DHNN) [23] works on discrete input vector like binary form 0,1 or bipolar +1, -1. DHNN consist of symmetric weight and no self-connectivity i.e., $w_{ij=}w_{ji}$ and $w_{ii} = 0$. Architecture of Hopfield neural networks shown in figure 4. There are some basic terminologies apply in Hopfield neural network as follow

- Hopfield neural network consist neural with one inverting and other noninverted outcome.
- The outcome of each and every neuron is considered input to other but no self-connection.
- Weight of neural network represented using symbol w_{ij}

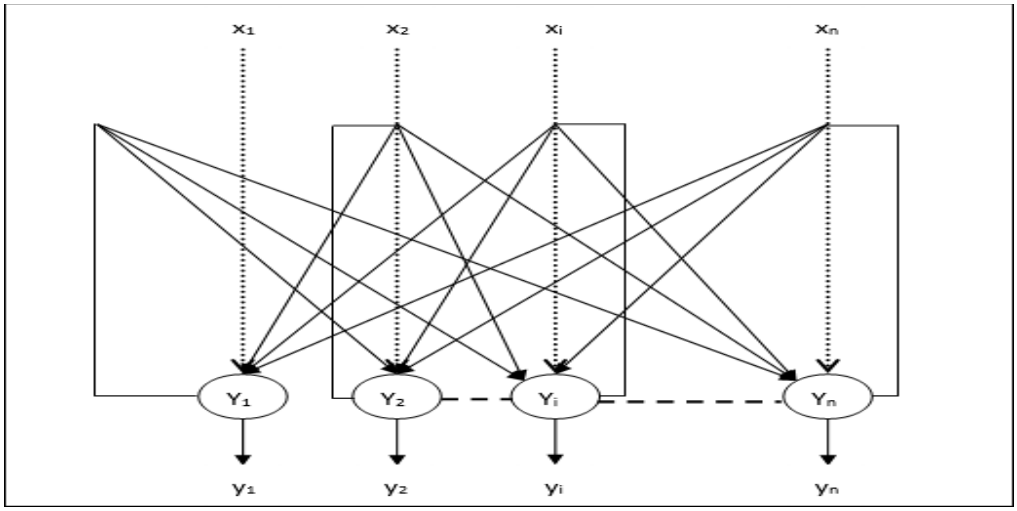

Fig.4. Hopfield neural network

3.3. Hopfield Neural Network Training Methodology

At the time of learning of Hopfield neural network weight will be modified on the basis of apply input like binary input and bipolar input vector. In both cases the weight updating process is different condition '1' and condition '2 'used for binary and bipolar input respectively.

Condition 1–For the Binary input vector the Hopfield neural network, for all the input binary bit patterns p=1 to P

Where p = s_1p, s_2p , s_3p $\dots\dots\dots\dots s_np$

Weight Matrix for the Hopfield neural network generated by given equation

$$w_{ij} = \sum_{p=1}^{P}[2s_i(p) - 1]\,[2s_j(p) - 1] for i \neq j \quad (4)$$

Condition 2– For the Bipolar input vector the Hopfield neural network, for all the input binary bit patterns p=1 to P

Where p= $s_1p,\ s_2p,\ s_3p\ \ldots\ldots\ldots\ldots s_np$

Weight Matrix is given by

$$w_{ij} = \sum_{p=1}^{P}[2s_i(p)]\left[s_j(p)\right] for i \neq j \tag{5}$$

3.4. Hopfield Neural Network Testing Algorithm

- To initialize weights value of Hopfield neural network use Hebb training rule.
- If the network signals are not aggregated, repeat steps 3 to 9.
- Steps 4 to 8 must be completed for every input vector 'X'.
- Set the network's starting activation to the external input vector using Eqn 5.

$$y_i = x_i \ for\ i = 1\ to\ n \tag{6}$$

- For every y_i execute the step 6 to 9.
- Compute the total input of Hopfield neural network as follows

$$y_{total} = x_i + \sum_{j=1}^{n} y_i w_{ji} \tag{7}$$

- Apply the activation function as the given rule

$$y_i = \begin{cases} 1 & if\ y_{total} > \emptyset \\ y_i & if\ f\ y_{total} = \emptyset \\ 0 & if\ y_{total} < \emptyset \end{cases} \tag{8}$$

where ∅ is the threshold value for hopfield neural networks

- Propagate the outcome y_i to all units.
- Test the Hopfield neural network for conjunction.

3.5. Energy Function for Hopfield Neural Networks

The term "energy function" refers to a finite and quasi mechanism of the system's status. Energy function E_f known as Lyapunov Function which compute the consistency of discrete Hopfield neural networks and defines as follow

$$E_f = -\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} y_i y_j w_{ji} - \sum_{i=1}^{n} x_i y_i + \sum_{i=1}^{n} \emptyset_i y_i \tag{9}$$

- Constraints: For a Stable Hopfield neural network theenergy function will decreases when the phase of particular node change. Neuron *'i' state has been changed from* $y_i^{(k)}$ *to* $y_i^{(k+1)}$ *after that the energy function of network changes using formula*

$$\Delta E_f = E_f\left(y_i^{(k+1)}\right) - E_f\left(y_i^{(k)}\right) \tag{10}$$

$$= -\left(\sum_{j=1}^{n}(w_{ij}\, y_i^{(k)} + x_i - \emptyset_i\ )\left(y_i^{(k+1)} - y_i^{(k)}\right)\right. \tag{11}$$

$$= -(net_i \Delta y_i)$$

$$\text{Where} \Delta y_i = y_i^{(k+1)} - y_i^{(k)} \tag{12}$$

The fact that only one unit may update activation at a time causes energy changes.

3.6. Countermeasure of the Protection of Mobile Agent

Security of mobile agent in the malicious environment at the time of transmission and execution of task on untrusted platform is critical issue. To focusing this issue an authentication scheme of mobile agent is proposed. In the proposed mechanism every mobile agent allocates an individual identity and password for execution of task on specific platform. This mechanism works under the collaboration of Hopfield neural network [22] and reed Solomon algorithm. Reed Solomon [24] used to convert of any text and image in to binary and bipolar data. Proposed strategy basically categorized in to two phases. The architecture of proposed approach shown in figure 5.

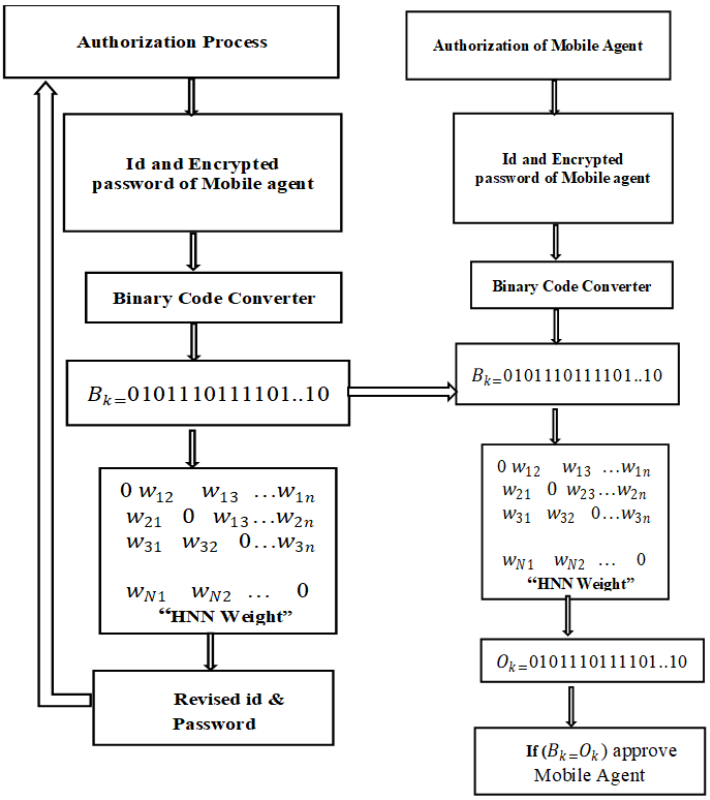

Fig.5. Frame work for mobile agent authentication using hopfield neural network

First phase: At the first phase registration of mobile agents with personal identity and encrypted password is done. Registration of mobile agent discussed in the algorithm 1. In the algorithm 1, each and every mobile registered with their personal id and encrypted password will register. The combination of identity of mobile agent and password converted in to binary (B_k) data using reed Solomon algorithm. Each and every binary digit if used as input for learning of Hopfield neutral network desired outcome. After the proper learning of Hopfield neural network save these programs online for authentication purpose of mobile agents. Another advantage of registration phase mobile agent can change their password and again trained the programmed as per the training algorithm.

Algorithm 1: Registration of mobile agents

$for\ i = 1\ to\ n$
{
Assign each mobile agent ID_i *and* Pw_i /*each mobile agent has different user id and password*/

$$E(Pw_i)\ encrpt\ every\ password\ using\ encryption\ algorithm$$

Apply reed Solomon algorithm to covert combination of ID_i and encrypted password $E(Pw_i)$ in binary value.
Output B_k is used to trained the 'n' Hopfield neural network training algorithm.
Trained Hopfield neural network util all user name and password remember by network.
}

Second phase: During the second phase mobile agent want to access permission to execute their assigned task. first apply their user id and password as an input to machine. The combination of mobile agent id and encrypted password converted in to binary code B_k. Download the trained program and apply the B_k and obtained output O_k. If meet the desired condition then authentication is successful otherwise failed the authentication. Algorithm 2 discuss about the authorization of mobile agent.

Algorithm 2: Authorization of mobile agents

Mobile agent provides user id (ID_r) and password (PW_r) at the time of authorization.
Platform compute encrypted password $E(PW_r)$ by using same algorithm uses at the time of registration.
The combination of (ID_r) and $E(PW_r)$ convert in to binary code.
Download the trained program apply input to Hopfield neural network.

If output ($O_r = B_r$)
{
authentication successful.
}
Else
{
Authentication failed.
}

4. Results and Discussions

Hopfield neural network [23] based proposed mechanism for the authentication of mobile agent is self-contained. At the of registration of mobile agents will never make mistake for matching of correct user id and password. The fusion of Hopfield neural network and reed Solomon algorithm implemented for the authentication of mobile agents on python platform. After the implementation proposed approach compared with layered artificial neural network and three other authentication approach first Chinese remainder theorem-based authentication [25], second Euler theorem-based authentication[26] and third two polynomial based authentication [27] using Lagrange interpolation. Table 1 represent the comparison of Hopfield neural network and layered neural network. After the analysis observer that for 25 ,50 ,100, 10 million mobile agent Hopfield neural network takes computational time '0.000436' sec,'0.000784'sec,' 0.00136'sec and 214 sec respectively and for the same number of mobile agents layered artificial neural network takes 92 sec ,317 sec ,1876 sec and exponential time respectively. It was observed that proposed approach is far better than layered neural network.Here another examination of proposed algorithm done by comparing with authentication using none artificial neural network approach such as Chinese remainder theorem-based authentication, second Euler theorem-based authentication and third two polynomial based authentication using Lagrange interpolation on same parameter. Table 2 represent the Comparison of computing performance of Hopfield Neural Network with Other three CRT, EULER and Polynomial based authentication layered Neural network. After the observation of outcome of experiment Hopfield neural network if better in term of computation time of authentication. Figure 6 discussed computation time for the performance of Hopfield Neural Network with Other three CRT, EULER and Polynomial based authentication layered Neural network.

Table 1. Comparison of computing performance of hopfield neural network with layered neural network

No of mobile agent	Hopfield Neural Networks	Layered Neural Network
25	0.000436 Sec	92 sec
50	0.000784 Sec	317 sec
100	0.00136 Sec	1876 sec
10 million	214 sec	Exponential time

Table 2. Comparison of computing performance of hopfield neural network with other three crt, euler and polynomial based authentication

	No of Mobile Agent									
	5	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
HNN	87 µsec	175 µsec	260 µsec	347 µsec	436 µsec	506 µsec	578 µsec	650 µsec	722 µsec	794 µsec
CRT	3.3 msec	4.2 msec	5.2 msec	6.8 msec	6.1 msec	7.4 msec	8.7 msec	10 msec	11.3msec	12.6msec
EULER	3 msec	3.7 msec	0.0035	5.3 msec	5.3 msec	6.1 msec	6.9 msec	7.7 msec	8.5 msec	9.3 msec
Polynomial	4.2 msec	4.4 msec	4.5 msec	5.0 msec	5.2 msec	5.3 msec	6.1 msec	6.5 msec	7.1msec	8.2 msec

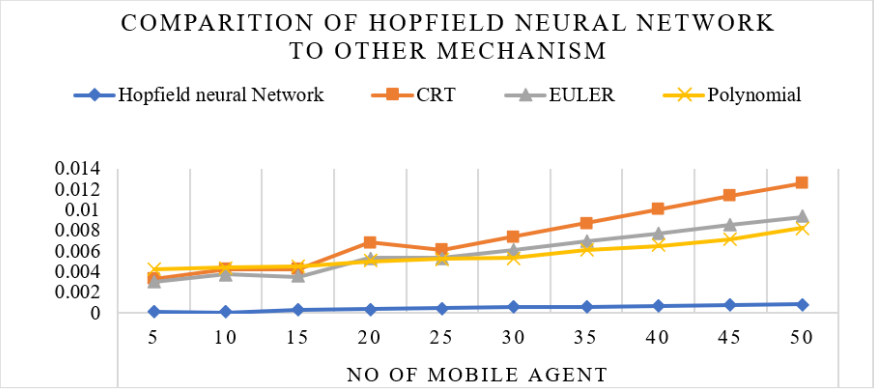

Fig.6. Comparison of computing performance of hopfield neural network with other three crt, euler and polynomial based authentication

5. Conclusion and Future Scope

Mobile agent freely migrating in venerable environment. The security of mobile agent from malicious agent and non-trusted platform is key concern. Protecting the mobile agent throughout cross-platform interaction is indeed a key concern. An adaptation of the Hopfield neural Network and the Reed Solomon algorithm has been proposed in this study to make communication between mobile agents and platform more secure. It provides assurance of mobile agent verification in a malicious and heterogeneous environment. After the analysis of Hopfield neural network-based mechanism computation time for the authentication as compared to other layered neural architecture is 10^5 time better. Also compared with the other three strategies based on CRT, EULER theorem and polynomial based authentication proposed mechanism is 10^3 time optimal in term of time required for authentication. Verification of any agent by other hosts is a major security feature. Hopfield's neural network-based architecture has a lower time complexity than others. It focuses on increasing the security features of agents, which in turn opens up research directions to suit additional security needs. In the future, a more coherent approach might be built to meet the needs of agent protection as well as detecting untrustworthy clients for key applications. This will help to prevent the mobile agent computing model from fraud, and the suggested effort will benefit various new application fields.

References

[1] W. Jansen and A. T. Karygiannis, “Mobile Agent Security.” 1999, Accessed: Jan. 14, 2022. [Online]. Available: https://www.nist.gov/publications/mobile-agent-security.

[2] P. Bagga and R. Hans, “Mobile Agents System Security,” *ACM Comput. Surv.*, vol. 50, no. 5, pp. 1–45, 2017, doi: 10.1145/3095797.

[3] C. Zrari, H. Hachicha, and K. Ghedira, “Agent’s security during communication in mobile agents system,” *Procedia Comput. Sci.*, vol. 60, no. 1, pp. 17–26, 2015, doi: 10.1016/j.procs.2015.08.100.

[4] P. Kumar, N. Singhal, and S. Singh, “Anonymous Scheme for Secure Mobile Agent Migration Using Mignotte’s Sequence and Back Propagation Artificial Neural Networks,” *Int. J. Comput. Inf. Syst. Ind. Manag. Appl.*, vol. 13, no. August, pp. 192–199, 2021.

[5] Monika Arora, Indira Bhardwaj, "Artificial Intelligence in Collaborative Information System", International Journal of Modern Education and Computer Science, Vol.14, No.1, pp. 44-55, 2022.

[6] M. Niemiec, M. Mehic, and M. Voznak, “Security Verification of Artificial Neural Networks Used to Error Correction in Quantum Cryptography,” *2018 26th Telecommun. Forum, TELFOR 2018 - Proc.*, pp. 1–4, 2018, doi: 10.1109/TELFOR.2018.8612006.

[7] W. M. Farmer, J. D. Guttman, and V. Swarup, “Security for Mobile Agents: Issues and Requirements,” *Nist*, pp. 591–597, 1996, [Online]. Available: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper033/SWARUP96.PDF.

[8] Zhengbing Hu, Mykhailo Ivashchenko, Lesya Lyushenko, Dmytro Klyushnyk, " Artificial Neural Network Training Criterion Formulation Using Error Continuous Domain", International Journal of Modern Education and Computer Science, Vol.13, No.3, pp. 13-22, 2021.

[9] Rida Qayyum, Hina Ejaz, " Data Security in Mobile Cloud Computing: A State of the Art Review", International Journal of Modern Education and Computer Science, Vol.12, No.2, pp. 30-35, 2020.

[10] Olawale Surajudeen Adebayo, Shefiu Olusegun Ganiyu, Fransic Bukie Osang, Salawu, Sule Ajiboye, Kasim Mustapha Olamilekan, Lateefah Abdulazeez," Data Privacy System Using Steganography and Cryptography ", International Journal of Mathematical Sciences and Computing, Vol.8, No.2, pp. 37-45, 2022.

[11] A. J. A. Wang, “Information security models and metrics,” *Proc. Annu. Southeast Conf.*, vol. 2, pp. 2178–2184, 2005, doi: 10.1145/1167253.1167295.

[12] H. Zhong, X. Wei, and R. Shi, “A novel anonymous secret sharing scheme based on BP Artificial Neural Network,” *Proc. - Int. Conf. Nat. Comput.*, no. Icnc, pp. 366–370, 2012, doi: 10.1109/ICNC.2012.6234550.

[13] A. Bhowmik and S. Karforma, *An Approach of Secret Sharing Technique Based on Convolution Neural Network and DNA Sequence for Data Security in Wireless Communication*, no. 0123456789. Springer US, 2022.

[14] S. Santhanalakshmi, K. Sangeeta, and G. K. Patra, “Design of group key agreement protocol using neural key synchronization,” *J. Interdiscip. Math.*, vol. 23, no. 2, pp. 435–451, 2020, doi: 10.1080/09720502.2020.1731956.

[15] M. Sadim, N. Pratap, S. Kumar, and A. Latoria, “Hybrid neural synchronization blowfish algorithm for secret key exchange over public channels,” *Mater. Today Proc.*, no. xxxx, 2021, doi: 10.1016/j.matpr.2020.11.363.

[16] M. S. K. Narad, “Group Authentication Using Back-propagation Neural Network,” vol. 6, no. 10, pp. 272–278, 2017, doi: 10.17148/IJARCCE.2017.61048.

[17] A. Yayik and Y. Kutlu, “Neural Network Based Cryptography,” *Neural Netw. World*, vol. 24, no. 2, pp. 177–192, 2014, doi: 10.14311/nnw.2014.24.011.

[18] É. Salguero Dorokhin, W. Fuertes, and E. Lascano, “On the Development of an Optimal Structure of Tree Parity Machine for the Establishment of a Cryptographic Key,” *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/8214681.

[19] S. Jhajharia, S. Mishra, and S. Bali, “Public key cryptography using neural networks and genetic algorithms,” *2013 6th Int. Conf. Contemp. Comput. IC3 2013*, pp. 137–142, 2013, doi: 10.1109/IC3.2013.6612177.

[20] S. C. Satapathy, B. N. Biswal, S. K. Udgata, and J. K. Mandal, “Proceedings of the 3rd international conference on frontiers of intelligent computing: Theory and applications (FICTA) 2014: Volume 2,” *Adv. Intell. Syst. Comput.*, vol. 328, pp. 217–224, 2015, doi: 10.1007/978-3-319-12012-6.

[21] M. Coutinho, R. de O. Albuquerque, F. Borges, L. J. G. Villalba, and T. H. Kim, “Learning perfectly secure cryptography to protect communications with adversarial neural cryptography,” *Sensors (Switzerland)*, vol. 18, no. 5, pp. 1–16, 2018, doi:

10.3390/s18051306.
[22] S. Wang and H. Wang, "Password authentication using Hopfield neural networks," *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.*, vol. 38, no. 2, pp. 265–268, 2008, doi: 10.1109/TSMCC.2007.913901.
[23] A. T. Maolood and A. T. Khudhair, "Towards generating robust key based on neural networks and Chaos theory," *Iraqi J. Sci.*, vol. 59, no. 3, pp. 1518–1530, 2018, doi: 10.24996/IJS.2018.59.3B.18.
[24] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Inf. Sci. (Ny).*, vol. 453, pp. 21–29, 2018, doi: 10.1016/j.ins.2018.04.043.
[25] S. Kandar and B. C. Dhara, "A verifiable secret sharing scheme with combiner verification and cheater identification," *J. Inf. Secur. Appl.*, vol. 51, p. 102430, 2020, doi: 10.1016/j.jisa.2019.102430.
[26] H. Chen and C. C. Chang, "A Novel (t,n) Secret Sharing Scheme Based upon Euler's Theorem," *Secur. Commun. Networks*, vol. 2019, no. c, 2019, doi: 10.1155/2019/2387358.
[27] A. K. Biswas and M. Dasgupta, " Two polynomials based (t, n) threshold secret sharing scheme with cheating detection ," *Cryptologia*, vol. 44, no. 4, pp. 357–370, 2020, doi: 10.1080/01611194.2020.1717676.

Authors' Profiles

Pradeep Kumar is a Ph.D. student of computer engineering and engineering at Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut, 250110. He has obtained his M.Tech. in Computer Science and engineering Department of Computer Engineering Shobhit Institute of Engineering & Technology (Deemed-to-be University), with first class. He obtained his B.Tech in Computer Engineering and engineering degree from college of engineering Roorkee, India in 2006 with first class.

Dr. Niraj Singhal is Ph.D. (Computer Engineering and Information Technology). He is Fellow and member of several International/National bodies and, reviewer and member of the advisory board for several International/National journals. He has many research publications to his credit in National/ International journals/conferences of repute. He has several years of rich experience of administration, coordinating and teaching at various levels. Presently he is working as Professor in the department of Computer Science and Engineering at Shobhit Institute of Engineering & Technology (Deemed-to-be University), Meerut. His area of interest includes system software, web information retrieval and software agents.

Mohammad Asim is a PhD Scholar in Computer Science and Engineering at Sharda University Greater Noida. He has obtained M. Tech in Computer Engineering from Shobhit Institute of Engineering & Technology (Deemed-to-be University) Meerut. He has completed BTech(CSE) from U.P. Technical University, Lucknow. His area of research includes Wireless Technology, Blockchain Technology, Mobile Ad-hoc Network and Cryptography & Network Security.

Dr. Avimanyou Vatsa is working as an assistant professor in the department of computer science, Fairleigh Dickinson University – Metropolitan campus. He also worked as an assistant professor at West Texas A&M University, teaching & research assistant at the University of Missouri, Columbia, and an assistant professor for more than ten years in several engineering colleges and a university in India. He obtained PhD, From University of Missouri, Columbia. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech (I.T.) from V.B.S. Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has supervised more than 25 students M.Tech dissertation. He is on the editorial board of few international journals in network and security area. He has been member of several academic and administrative bodies. During his teaching he has coordinated several Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).

How to cite this paper: Pradeep Kumar, Niraj Singhal, Mohammad Asim, Avimanyou Vatsa, "An Optimized Authentication Mechanism for Mobile Agents by Using Machine Learning", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.6, pp.30-39, 2023. DOI:10.5815/ijcnis.2023.06.03