electronics

MDPI

Article

A Computational Framework for Cyber Threats in Medical IoT Systems

Geetanjali Rathee [1], Hemraj Saini [2], Chaker Abdelaziz Kerrache [3] and Jorge Herrera-Tapia [4,*]

[1] Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi 110078, India; geetanjali.rathee123@gmail.com
[2] School of Computing, DIT University, Uttarakhand 248009, India; hemraj1977@yahoo.co.in
[3] Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat 03000, Algeria; ch.kerrache@lagh-univ.dz or kr.abdelaziz@gmail.com
[4] Faculty of Informatics Sciences, Universidad Laica Eloy Alfaro de Manabí, Manta 130213, Ecuador
* Correspondence: jorge.herrera@uleam.edu.ec

Abstract: Smart social systems are ones where a number of individuals share and interact with each other via various networking devices. There exist a number of benefits to including smart-based systems in networks such as religions, economy, medicine, and other networks. However, the involvement of several cyber threats leads to adverse effects on society in terms of finance, business, liability, economy, psychology etc. The aim of this paper is to present a secure and efficient medical Internet of Things communication mechanism by preventing various cyber threats. The proposed framework uses Artificial Intelligence-based techniques such as Levenberg–Marquardt (LM) and Viterbi algorithms to prevent various social cyber threats during interaction and sharing of messages. The proposed mechanism is simulated and validated with various performance metrics compared with the traditional mechanism.

Keywords: social networks; cyber security; Intrusion detection system; social system threats; artificial model in social systems

Citation: Rathee, G.; Saini, H.; Kerrache, C.A.; Herrera-Tapia, J. A Computational Framework for Cyber Threats in Medical IoT Systems. *Electronics* **2022**, *11*, 1705. https://doi.org/10.3390/electronics11111705

Academic Editors: Wojciech Mazurczyk and Antoni Morell

Received: 3 May 2022
Accepted: 24 May 2022
Published: 27 May 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

The term "social system" can be defined as the combination of two terms, i.e., system and society [1]. A system may be an orderly arrangement of interrelated components where each and every part of the system has a specific responsibility at a fixed place. In the system, all the parts are bounded with some interactions. Likewise, society may be viewed as a collaboration of various interactive parts to achieve a goal [2]. Therefore, a social system can be defined as agroup of interactive units of individuals in society for shared cultural norms and meanings. It includes all the diverse subsystems such as economics, politics, religion, culture, cities, college campuses, nations, etc. At present, most social systems are smart and interaction has become digitized. There are various benefits to smart social systems including resources sharing, reduced cost of operations, flexibility, networking and partnership, faster communication, organic visibility, broader periphery, thought sharing, etc. [3]. On the other side of the coin, there is a big disadvantage in smart social systems as an unwanted unit may be the part of it and can threaten the whole smart social system using cyber threats. Terrorists, Governments, Individual Spies, Crime Groups, Hacktivists, Competitors, Disgruntled Insiders, Hackers, and GAO may be the sources of cyber threats.

A general diagram of cyber security threats in social systems is represented by Figure 1. This figure represents the possible number of cyber threats such as communication threats, computation threats, and control threats.

Cyber threats are of different types and every type may have many variants; therefore, it is really difficult to detect them before they become the cause of a significant loss [4]. A list of types of cyber threats is depicted in Figure 2. Cyber threats are generally categorized

into three different scenarios such as physical, system, and cyber. The physical cyber threat is generally relies on communication and computation, where the number of devices that need various computations while communicating or transmitting the information between each other are affected, leading to drastic damage to the network. The network with various threats increases the network congestion and delays in the network. The phishing attack, man-in-middle attack and cryptographic, denial-of-service threats are various examples of communication and computation attacks. In addition, systems threats consider communication and control behavior where the systems while transmitting the information, suffer from various phishing, request-response, brute force, virus, and trojan horse threats. Finally, the cyber threat is in the computation and control category, where a cryptographic and replay threat may occur while controlling the data flow and traffic management systems among nodes in the network. These cyber attacks significantly affect the social systems in many forms including adverse effects on finance, continuation of business, legal liability, reputation, production, psychology, economy, social values, mentality of youth, etc. as depicted in Figure 3. These types of cyber threats occur among various devices while transferring, data controlling, or moving information from one place to another. Networking, data communication and message encrypting are several areas where certain kind of information can be transmitted among nodes in the network.The wormhole, virus, malware, SQL and cryptographic are various examples of cyber threats that are again divided into various types of threats.

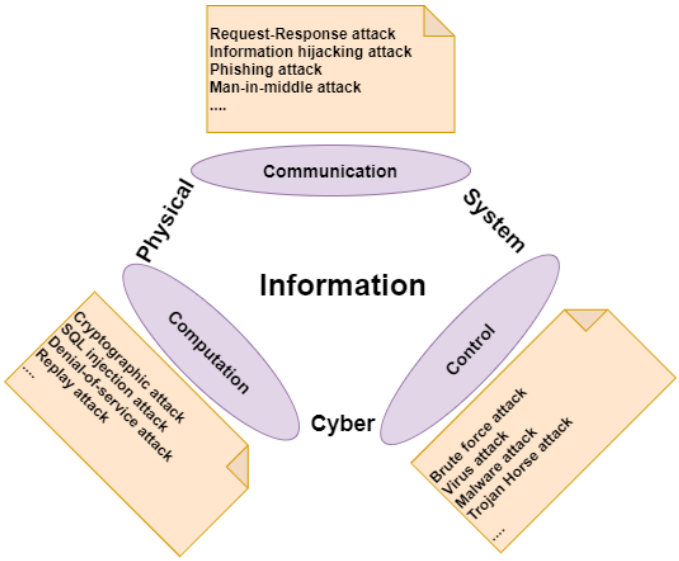

Figure 1. Cyber Threats in Social Systems.

Generally, cyber attacks are difficult to detect and stop but one can be safe by following some required practices, such as by training individuals in how cyber crimes work, updating antivirus and antispyware software, using firewalls with adequate policies, updating operating system patches, backing up information, ensuring physical security, securing WiFi connections, providing separate accounts for all users, limiting access to the information, regular password changing, etc. [5,6]. Following these practices is not the only solution but it can reduce the danger of cyber attacks. Some methodologies such as biometrics, CAPTCHA, password and username, Anti-Malware software, IDS etc. [7] are used to detect and prevent cyber attacks. The Intrusion Detection System (IDS) is the preferred technique to detect cyber attacks and they are of four (04) kinds including the Host-based intrusion detection system (HIDS), Network intrusion detection system (NIDS), VM-based Intrusion Detection System (VMIDS), and Perimeter Intrusion Detection System (PIDS). All these IDSs are based on techniques including the Signature-based, Anomaly-based, and AI-based [8] techniques. The Signature-based technique is a static technique and needs regular updating of the signature database. The Anomaly-based technique monitors system

activity and classifies it as normal or abnormal. Abnormal behavior is detected only after the cyber attack and therefore, loss has already occurred. Therefore, the third one, i.e., the AI-based technique, should better suit the purpose but it needs enhancements in the existing techniques. The societal systems are deployed in the form of web servers, clouds, and distributed information systems. Therefore, the AI-based technique is proposed to predict cyber attacks on the societal systems in the manuscript.

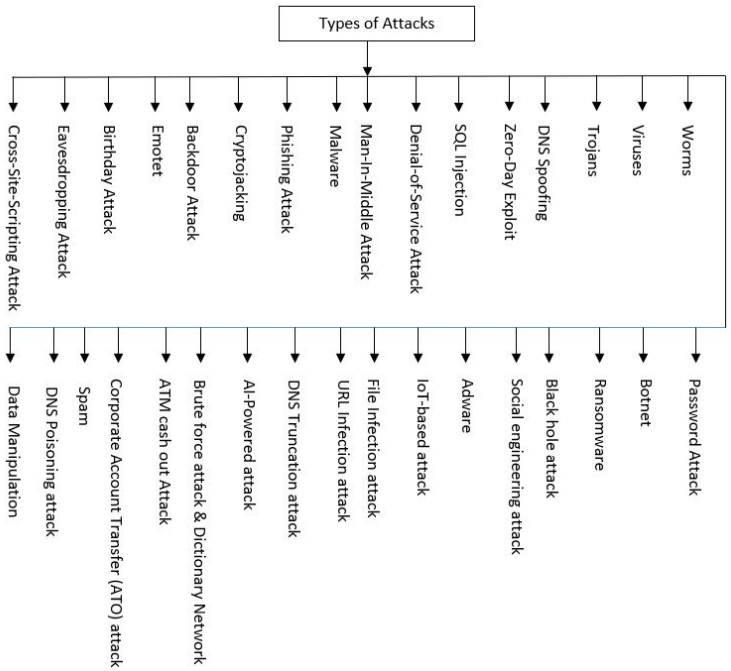

Figure 2. Possible Types of Cyber Threat.

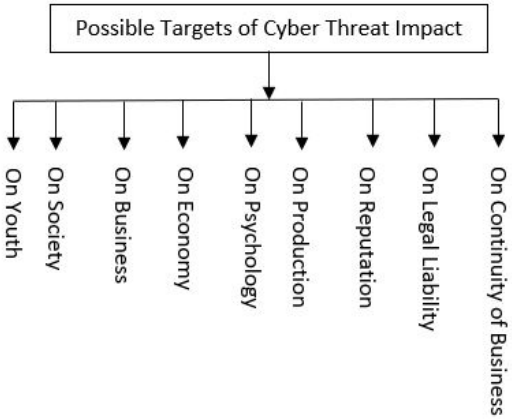

Figure 3. Possible Targets of Cyber Threats Impact.

1.1. Motivation and Objective

The increasing rate of cyber threats is adversely affecting the cyber threats in several IoMT systems. A number of security schemes were proposed by various authors and scientists [9,10], such as that by Saheed et al. [11], who proposed a deep recurrent network for IoMT using supervised machine learning methods. The authors demonstrated KNN, random forest and ridge classifiers for developing an effective and efficient Intrusion Detection System for classifying the cyber threats. Rahman et al. [12] tested several COVID-19 diagnostic schemes relying on DL methods by discussing their adversarial examples. The authors have detailed the examples of adversarial in detail by implementing the perturbations. In addition, Ranganayaki et al. [13] have detailed and worked on introducing the

hospitals security by reducing the cyber threats for ensuring a secure and efficient communication mechanism for smart hospitals. Furthermore, Mushtaq et al. [14] introduced and discussed a number of security threats that can be encountered while ensuring a secure communication process among intelligent devices in smart hospitals. The authors concentrated on various security threats such as Gamut, Emoted, Miari, time-based spoofing, and replay attacks. The intruders may affect the network performance by degrading the system state. The goal of this manuscript is to propose an Artificial Intelligence-based cyber threat detection system. The proposed phenomenon uses Levenberg–Marquardt (LM) [15] and Viterbi algorithms [16] to analyze and compute the malicious behavior of each network. The LM mechanism is used to provide efficiency and higher stability in the network by determining optimization schemes. In addition, the Viterbi algorithm is used to upgrade the transition states by analyzing the behavior of each node as malicious or legitimate in social systems. The proposed mechanism is analyzed against various simulating results over existing mechanisms.

1.2. Contribution

To securely transmit the information in social networks or to enhance the communication process among devices, it is necessary to propose a secure and trusted social system network. It is necessary to propose an intelligent cyber security system to analyze the modeling of human behavior, complex social computing, and computational systems which are involved, while establishing a secure computing network. Malicious behavior in social computing and human behavior recorded by various smart devices can be easily detected using various security protocols. The contribution of this paper is to propose an intelligent analysis and computing algorithms known as LM and Viterbi to provide faster and efficient behavior of social networks. The theoretical contribution of the paper is defined as follows:

- A secure and trusted communication in social networks by analyzing their behavior using the LM mechanism.
- The continuous behavior of involved devices can be easily traced by upgrading their transition nodes using the Viterbi algorithm.
- The performance of proposed scheme is analyzed with various security measures such as response time, system accuracy, number of resources used and request category.

The remainder of the paper is organised as follows. Section 2 presents a literature survey of various security schemes. The LM and Viterbi algorithms to analyze and evaluate legitimate behavior are determined in Section 3. Furthermore, Section 4 analyzes the performance of proposed phenomenon as compared to existing schemes over various metrics. Finally, Section 5 concludes the paper along with future directions.

2. Related Work

This section deliberates the number of schemes and mechanisms proposed by various authors and scientists to ensure a secure and efficient communication mechanism in social systems by identifying various cyber threats. Table 1 shows a number of approaches with their techniques and performance metrics to provide a secure and efficient communication mechanism in social networks. In addition, some recent trends specific to social cyber security threats for analyzing the human behavior, complex social computing and mechanisms are shown in Table 2. A brief introduction on the number of algorithms/techniques/schemes proposed by various researchers/scientists [17–20] specific to social computing networks while analyzing the human and network behaviors can be found in Tables 1 and 2.

Table 1. Related Work Discussion.

Abbreviation	Description
2019	***Tagarev, T., & Sharkov, G.*** [21]
TA	This paper describes high-performance, computer-assisted work related to the development and implementation of cyber security policy.
AP	Specific details were presented in the formulation of cyber security policy and compliance with the ECHO project.
PF	This research looks at using the power of a highly efficient computer, as well as 'supercomputers' for cyber security training, preliminary warning, certification, etc.
2019	***Sánchez, H.S. et al.*** [22]
TA	This review identifies attack modeling, security objectives, and targeted attack planning and threats that present mechanisms for detection and remedial actions.
AP	Open-minded issues and future directions for further research on cyber security.
PF	Provided the guidance for proper organization and reduction of threats.
2020	***Priyadharshini, N. et al.*** [23]
TA	Provides an overview of all the needs of small grids that explain cybersecurity issues.
AP	Effective management and control of Microgrid
PF	Microgrid with Distributed Generations with limited storage and ubiquitous communication networks can be future interest.
2020	***Bejan, A.*** [24]
TA	Physics of evolution causes the origin, evolution and future of the social systems is discussed.
AP	The body movements made by individual producers of ideas and energy are similarly arranged, in stages on the surface of the earth.
PF	In continuation the more effective research has to be carried out.

TA → Technical Aspect; AP → Approach Used; PF → Performance Metrics/Future Aspect.

Table 2. Recent Survey on Social and Medical Systems Cyber Threats.

Abbreviation	Description
2020	***Alturki, A. et al.*** [25]
TA	Identifies factors that contribute to the abuse of social engineering concepts in social gaming systems.
AP	The developed model is based on competitive and health belief ideas.
PF	The presented results predicted the significant factors of risks such as tangible benefits, hard work, cooperative and competitive delays.
2020	***Yaacoub, J.P.A. et al.*** [26]
TA	This paper examines the key features of CPS and related technologies, applications and standards. In addition, CPS security threats and attacks are reviewed by highlighting the challenges and threat key issues.
AP	CPS security solutions categorized as cryptographic and non-encryption solutions with highlighting important lessons learned appropriately throughout.
PF	Deployment of the suggestions and recommendations in CPS as the main component of Industry 4.0.
2020	***Feng, J. et al.*** [27]
TA	A case study and a privacy-preserving tensor computation mechanism is presented for CPSs.
AP	Privacy-preserving tensor computation framework.
PF	The big data analysis is done by proposing the distributed and incremental tensor computations to enhance the performance of privacy-preserving in CPSSs.
2020	***Attatfa, A. et al.*** [28]
TA	A systematic literature survey is conducted to highlight the extent of recent cyber diplomacy research.
AP	Literature gap in cyber diplomacy is covered.
PF	Applied network sociology and Actor-Network Theory (ANT).

TA → Technical Aspect; AP → Approach Used; PF → Performance Metrics/Future Aspect.

Research Statement

Although a number of techniques have been proposed by various researchers/scientists, the existing mechanism includes a number of limitations including storage overhead, communication, and computation overhead. Furthermore, the additional cryptographic and encryption-based schemes include additional costs and delay while ensuring the security in the network. The aim of this paper is to propose an efficient communication model using artificial model. The proposed phenomenon uses LM and Viterbi algorithms to validate and ensure a secure communication and interaction mechanism in social systems.

3. Proposed Approach

Artificial Intelligence can be defined as one of the emergent techniques to ensure a trusted environment in real time scenarios. Artificial networks are considered to be the computational models inspired by biological neural cells where billions of neurons are used to process a particular task. Based on the concept of biological cells, artificial networks are capable of modeling both the operation and architecture as a non-linear approximation function, and clustering and classification techniques. Artificial networks are based on the concept of neurons that are used to produce a reliable and efficient decision making for a particular problem. Cyber security threats such as online frauds, social networking threats such as flooding, synchronization, jamming and others can be easily traced through artificial networks. In this paper, the artificial network model is used to formulate the cyber threats. In addition, the Viterbi algorithm is used for further identification and detection of malicious number of nodes in real time scenarios.

3.1. System Model

Figure 4 depicts the artificial model of proposed scenario having I_n number of input, H_n number of hidden nodes and O_n number of output nodes.

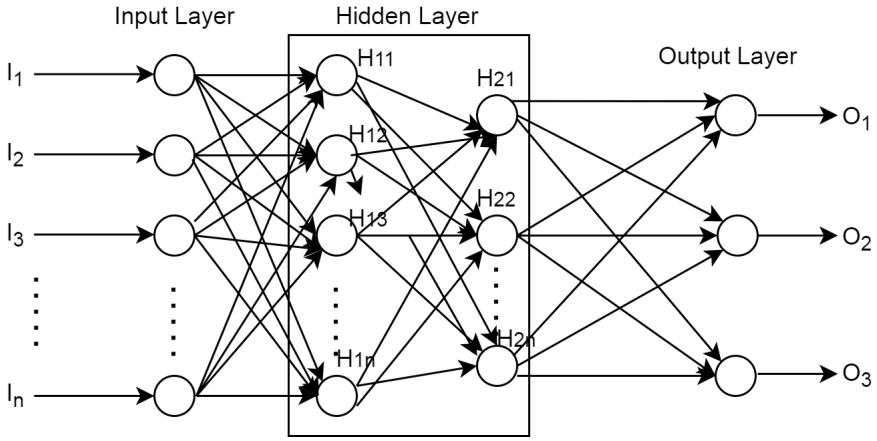

Figure 4. An Artificial Model (combines LM and Viterbi Algorithms to ensure Security).

The number of inputs processed by input layer is passed through various number of hidden layer used to identify the type of threat or its detection by computing its various activities/behaviors. In addition, the information processed by various hidden layer can be passed to the output layer that finally categorize the type of threat in the network. The given architecture used in the artificial network is defined as the Multi-Layer Perception (MLP) model where the activation function with O_n output units, H_n hidden units and I_n input units is expressed in the form of the following equation:

$$W_z(t) = \sum_{x=1}^{H_h} eW_{xz}^2 F(.) \sum_{y=1} I_n eW_{yx}^1 P_y(t)^0 + b_x^1 \quad (1)$$

where eW_{yx}^2 and eW_{xz}^2 illustrates edged weight connection among input and hidden layers and edges weight between hidden and output layers. In addition, b_x^1 and p_y determines the threshold values of hidden and input nodes supplied to the In layer and $F(.)$ defines activation function that is selected as the sigmoid function. From the given Equation (1), the eW_{yx}^2 and eW_{xz}^2 and b_x^1 values are computed using an appropriate algorithm. In this paper, we used the LM and Viterbi algorithms to determine the optimum, reliable decision for identifying the cyber threat in social networks.

3.2. LM Algorithm

The LM algorithm is defined as a gradient deterministic optimization algorithm to provide an efficient and faster convergence rate and stability in the network. Similar to quasi-Newton scheme, LM is used to design second order speed of training to determine the Hessian matrix. Whenever, the function to perform is computed in the form of square sums, the Hessian matrix is determined as:

$$H = M^T M \tag{2}$$

With its computed gradient as:

$$G = M^T \rho \tag{3}$$

where M defines the Jacobian matrix containing the first derivation network error with respect to bias and weights. In addition, e is termed as network error vectors where Jacobian matrix is computed through Hessian matrix. The LM algorithm updates the quasi-Newton in the form of:

$$\delta W = -[M^T M + \mu I_n]^{-1} M^T \rho \tag{4}$$

where μ is controlling parameter and w is the differential weights of the network. In the Newton scheme mu is zero and mu is large in the case of the gradient descent method. To further speed up the computation process and provide a reliable solution, the LM algorithm is merged with the Viterbi method.

3.3. The Viterbi Method

The transition diagram having number of edges are different because of various nodes' behavior. The Viterbi algorithm is used to update the transition graphs according to their various entities. The Viterbi scheme calculates the hidden nodes probability that is based on its various emissions and activities sequences. The depicted Algorithm 1 determines the malicious or cyber threat identification by identifying the malicious activity of each node. Furthermore, the Viterbi algorithm is used to maximize function at each instance of time to choose the best decision or sequence of activities. Let $p_t(n)$ determines the maximum probability of a node in a state i with the sequence length 'l' having 'o' observations in artificial model. The $p_t(n)$ can be defined as the below Equation (3):

$$P_t(i) = maxPr(\mu(1), \mu(2), \ldots \mu(t-1); o(1), o(2), \ldots o(t) | \mu(t) = \mu_i \tag{5}$$

Table 3 represents the abbreviation or notations used to defined Viterbi algorithm.

Table 3. Viterbi Algorithm Notations.

Symbol	Meaning
$P_t(n)$	Prob. of a node from state i to j with input request of length 'l'
α_i	Initial probability of state i
$b_i(\mu(t))$	Probability output of state i.
α_{ij}	Transition state from state i to j

The number of steps required to ensure a secure communication using LM and Viterbi algorithms as shown in Algorithm 1 is computed as follows:

Algorithm 1: Secure Communication Algorithm

Input Value: (1) Number of IoT devices '*d*', (2) 3-believing states (authentic, infected, unidentified)

Input Value: (1) Number of IoT devices '*d*', (2) 3-believing states (authentic, infected, unidentified)

Output: Device is either trusted or in unidentified/infected state

Step 1: Compute the artificial model according to below equation as:

$$W_z(t) = \sum_{x=1}^{H_h} eW_{xz}^2 F(.) \sum_{y=1} I_n eW_{yx}^1 P_y(t)^0 + b_x^1 \tag{6}$$

Step 2: Calculate the LM computation as:

$$H = M^T M \tag{7}$$

With its computed gradient as:

$$G = M^T \rho \tag{8}$$

$$\delta W = -[M^T M + \mu I_n]^{-1} M^T \rho \tag{9}$$

Step 3: The Viterbi algorithm is computed as:

Step 3.1. Variable initialization of matrix and probability as:

$$P_t(n) = \alpha_i b_i(u(t)) \tag{10}$$

$$\alpha_i(i) = 0 \tag{11}$$

Step 3.2. Recursion is done by updating the output α_i as:

$$p_t(j) = max_i[p_{t-1}(i)\alpha_{ij}]b_j(u(t)) \tag{12}$$

Step 3.3. Recursion is terminated as:

$$Q^* = max_i[p_t(i)] \tag{13}$$

$$Q^* = argmax_i[p_t(i)] \tag{14}$$

Step 3.4. The best state is searched for through backtracking as:

$$Q_t^* = \alpha_{t+1}(Q_t^* + 1) \tag{15}$$

The proposed mechanism provided a secure and efficient communication mechanism by integrating two methods such as LM and Viterbi for detecting and categorizing the number of cyber security threats. The LM algorithm is used for ensuring an optimized and fater convergence network by regularly updating their gradient. The continuous surveillance and Hessain matrix method provided sharing and interaction among devices. In addition, the Viterbi scheme is further used to categorize the communicated device depending on their convergence rate and stability into various categories such as legitimate and malicious. The legitimate or ideal devices may further resume their transmissions in the network. However, the malicious devices are blocked and never allowed to perform any type of communication in the network.

In addition, the limitation of proposed mechanism will be a topic of future research as the present approach is not able to successfully recognize the behavior of a communicating device that is mobile in nature. During the handoff process where devices are able to move from one domain to another, it is crucial to identify or recognize their active behavior in the network at the initial stages that may further lead to various drastic changes in the network. Therefore, the dynamic behavior of each altered device can further lead to drastic change in the network performance. The detection and identification of a device's legitimacy during mobility can be considered to be future directions of this research.

4. Performance Analysis

The proposed artificial network using LM and Viterbi algorithm is verified with a synthesized data set with 500 nodes that are categorized as legitimate and malicious. The cyber threat is detected via analyzing the activity and behavior of each node in the network. The numbers of malicious activities of a node increase with the increase rate of nodes count. For example, in a network size of 50 nodes, 5% of nodes are considered to be malicious nodes that may further increase at the rate of 5% on increasing the scalability of the network. In addition, to determine the optimum and reliability of hidden nodes layer, an optimal structured is analyzed. For analyzing or training the artificial model, we used 3100 epochs with 9.723 s, 5.069 s and 4.563 s having time using LM and Viterbi algorithm. Table 4 shows the optimal structure analysis of artificial model using various training schemes.

Table 4. Optimal structure analysis.

Artificial Training Schemes	Number of Hidden Nodes
LM	9
Viterbi	3

A generalized model to analyze the proposed scenario is depicted over Figure 5. Furthermore, Table 5 represents the results analysis of artificial model through various schemes.

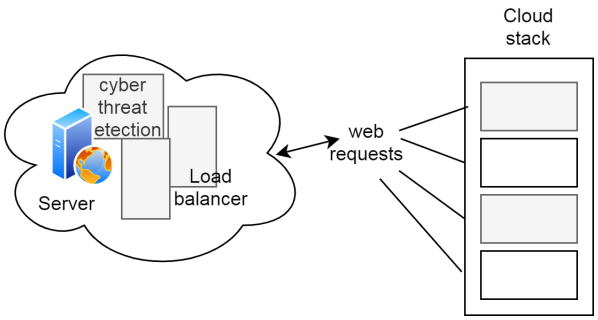

Figure 5. Testbed for cyber security threat simulation.

Table 5. Result analysis.

Artificial Model	Training	Testing	Overall Value
LM	96.98	91.32	92.45
Viterbi	97.42	95.48	94.37

4.1. Baseline Mechanism

The proposed mechanism is simulated with two different traditional approaches to determine the cyber security in social systems. Alturki et al. [18] proposed a competitive and cooperative theory to influence the social engineering victims in gaming networks. The authors simulated the results against various severe threats, benefits and barriers of predicting social victims including significant factors. In addition, Yaacoub et al. [19]

surveyed the cyber physical systems aspects by highlighting the security vulnerabilities, threats, issues, and challenges. The authors determined various security solutions including non-cryptographic and cryptographic schemes. The proposed phenomenon is simulated against these two baseline approaches having cryptographic and game network theory to validate against various metrics.

4.2. System Evaluation

After setup the simulation setup, the overall system evaluation of results is determined in this section. The cyber security model is compared with and without intrusion security abilities. In an intrusion system, the artificial process is done with web requests created by intruders running virtual systems. All the filtered requests of intrusion systems are prevented and blocked by LM scheme. A system without intrusion is aconventional security scheme where web requests are directly going to the server via the virtual machine (VM). Depending on the number of requests generated and devices having malicious activities are used to verify the proposed phenomenon. Furthermore, the number of various input parameters of intruder's sources is presented in Table 6.

Table 6. Result analysis.

Type	% of Attack Request	Level of Severity	Source Name
Legitimate	0	0	30
Malicious	20%	1, 3	15
Hihly sensitive	30%	3, 4, 5	10

Figure 6 deliberates the number of resources efficiently used by VM that hosts the server for processing the attacked web requests. The use of resources will increase on increasing the web requests due to the identification and detection of threats in each request. The proposed phenomenon leads to an 86% improvement due to its proper working using LM scheme.

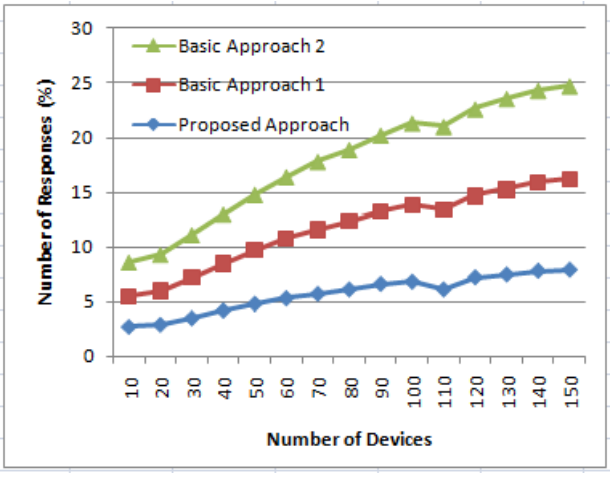

Figure 6. Number of Resources.

In addition, Figure 7 determines the response time in intrusion and without intrusion systems having lesser and higher number of queries based on generated by web requests. The response time of the proposed phenomenon is much better as compared to the traditional scheme due to the involvement of the Viterbi scheme.

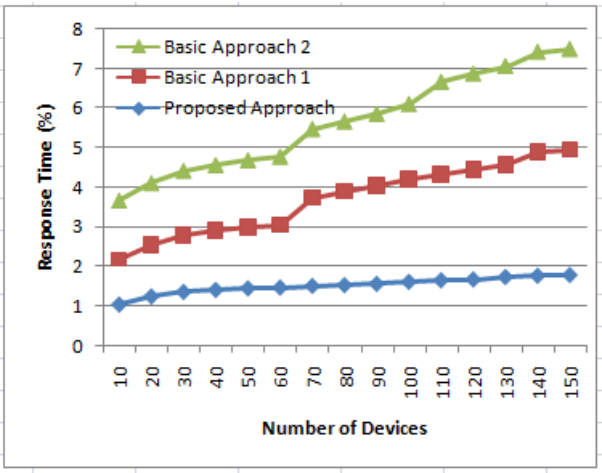

Figure 7. Response Time.

Furthermore, Figures 8 and 9 represent the requests category depending on their behavior and accurate rate with all the attacked sources as compared to traditional mechanism. The proposed phenomenon performs much better as compared to traditional schemes because of their efficient and reliable LM and Viterbi algorithms.

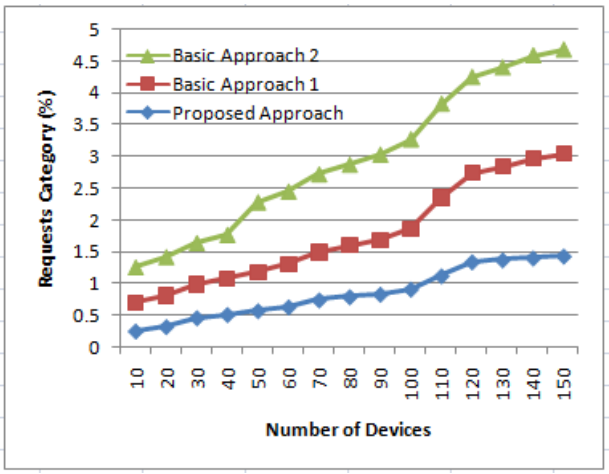

Figure 8. Request Category.

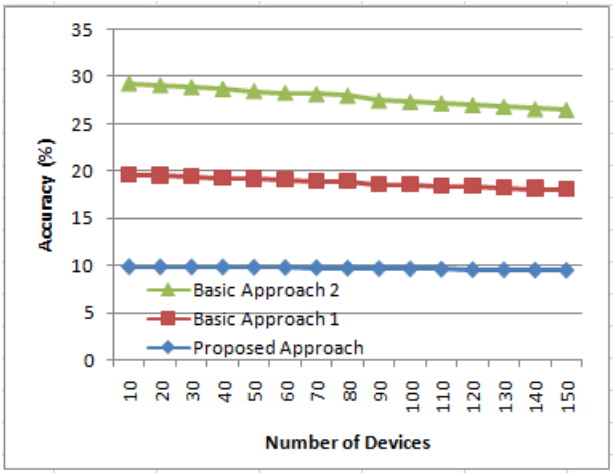

Figure 9. System Accuracy.

4.3. Discussion

The computed results analyzed with various security threats such as number of resources, response time, request category, and system accuracy outperforms existing approaches. The existing mechanisms used various cryptography or gaming schemes for ensuring the security that may further leads to other security and networking concerns such as storage overhead, communication delays, storage issue and so on. The proposed mechanism integrated the LM and Viterbi schemes for providing two-level security by easily categorizing them into legitimate and malicious devices. The identification of malicious behavior of each communicating device does not require extra computation or storage delays as the convergence rate and first order derivatives are computed and change every time. In addition, the categorization of each communicating device is performed on the basis of their behavior. The computed accuracy and response time of each device always leads the existing approaches as proposed the phenomenon does not include any extra storage or computational delays while ensuring the security of a device.

5. Conclusions

This paper proposed a secure and efficient social communication mechanism by detecting and identifying various cyber security threats. The proposed framework used an artificial model for identifying the malicious activities of communicating nodes in the network. The proposed mechanism integrated the Levenberg–Marquardt (LM) and Viterbi algorithms to determine an effective and secure communication mechanism for IoMT. The LM algorithm provides a faster, more efficient and optimized convergence rate while identifying the legitimacy of devices. In addition, the Viterbi algorithm is used to compute the probability of hidden nodes to measure the activities and emissions of malicious nodes. The proposed phenomenon is validated and verified against various performance metrics in terms of response time, resource use, accuracy rate, and requests category. Simulation results depicted the performance of the proposed solution compared with the traditional mechanism. Furthermore, the dynamic behavior of each altered device can further lead to drastic changes in network performance. The detection and identification of a device's legitimacy during mobility can be considered to be a future direction of research.

Author Contributions: G.R., H.S., C.A.K. and J.H.-T. equally contributed to this work in all aspects with more implementation-related efforts from G.R. and H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All implementation details, sources, and data will be delivered upon requesting the corresponding author Jorge Herrera Tapia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dunbar, R.I.M. *Primate Social Systems*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
2. Banathy, B.H. *Designing Social Systems in a Changing World*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
3. Mazman, S.G.; Usluel, Y.K. The usage of social networks in educational context. World Academy of Science. *Eng. Technol.* **2009**, *49*, 338–342.
4. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
5. Parn, E.A.; Edwards, D. Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence. *Eng. Constr. Archit. Manag.* **2019**, *26*, 245–266. [CrossRef]
6. Rathee, G.; Ahmad, F.; Iqbal, R.; Mukherjee, M. Cognitive Automation for Smart Decision-Making in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2152–2159. [CrossRef]
7. Rathee, G.; Jaglan, N.; Garg, S.; Choi, B.J.; Choo, K.K.R. A Secure Spectrum Handoff Mechanism in Cognitive Radio Networks. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 959–969. [CrossRef]
8. Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]

9. Khraisat, A.; Alazab, A. A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity* **2021**, *4*, 18. [CrossRef]
10. Simoglou, G.; Violettas, G.; Petridou, S.; Mamatas, L. Intrusion Detection Systems for RPL Security: A Comparative Analysis. *Comput. Secur.* **2021**, *104*, 102219. [CrossRef]
11. Saheed, Y.K.; Arowolo, M.O. Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. *IEEE Access* **2021**, *9*, 161546–161554. [CrossRef]
12. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Alsolami, F. Adversarial examples—Security threats to COVID-19 deep learning systems in medical IoT devices. *IEEE Internet Things J.* **2020**, *8*, 9603–9610. [CrossRef]
13. Ranganayaki, R.S.; Sreeja, B.; Gandhari, S.; Ranganath, P.T.; Kumar, S. Cyber Security in Smart Hospitals: A Investigational Case Study. In Proceedings of the 2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 10–11 December 2021; pp. 92–98.
14. Mushtaq, M.; Shah, M.A.; Ghafoor, A. The Internet of Medical Things (IOMT): Security Threats and Issues Affecting Digital Economy. In Proceedings of the Competitive Advantage in the Digital Economy (CADE 2021), Online, 2–3 June 2021; pp. 137–142.
15. Lourakis, M.I. A brief description of the Levenberg Marquardt algorithm implemented by levmar. *Found. Res. Technol.* **2005**, *4*, 1–6.
16. Viterbi, A.J. A personal history of the Viterbi algorithm. *IEEE Signal Process. Mag.* **2006**, *23*, 120–142. [CrossRef]
17. Ayub, S.; Shabir, M.; Riaz, M.; Aslam, M.; Chinram, R. Linear Diophantine fuzzy relations and their algebraic properties with decision making. *Symmetry* **2021**, *13*, 945. [CrossRef]
18. Ashraf, S.; Abdullah, S.; Zeng, S.; Jin, H.; Ghani, F. Fuzzy decision support modeling for hydrogen power plant selection based on single valued neutrosophic sine trigonometric aggregation operators. *Symmetry* **2020**, *12*, 298. [CrossRef]
19. Riaz, M.; Hashmi, M.R.; Pamucar, D.; Chu, Y.M. Spherical linear Diophantine fuzzy sets with modeling uncertainties in MCDM. *Comput. Model. Eng. Sci.* **2021**, *126*, 1125–1164. [CrossRef]
20. Li, S.; Zhao, S.; Yuan, Y.; Sun, Q.; Zhang, K. Dynamic security risk evaluation via hybrid Bayesian risk graph in cyber-physical social systems. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 1133–1141. [CrossRef]
21. Tagarev, T.; Sharkov, G. Computationally Intensive Functions in Designing and Operating Distributed Cyber Secure and Resilient Systems. In Proceedings of the 20th International Conference on Computer Systems and Technologies, Ruse, Bulgaria, 21–22 June 2019; pp. 8–18.
22. Sánchez, H.S.; Rotondo, D.; Escobet, T.; Puig, V.; Quevedo, J. Bibliographical review on cyber-attacks from a control-oriented perspective. *Annu. Rev. Control* **2019**, *48*, 103–128. [CrossRef]
23. Priyadharshini, N.; Gomathy, S.; Sabarimuthu, M. A review on microgrid architecture, cyber security threats and standards. *Mater. Today Proc.* **2020**. [CrossRef]
24. Bejan, A. Freedom and evolution in the dynamics of social systems. *Biosystems* **2020**, *195*, 104158. [CrossRef]
25. Alturki, A.; Alshwihi, N.; Algarni, A. Factors influencing players' susceptibility to social engineering in social gaming networks. *IEEE Access* **2020**, *8*, 97383–97391. [CrossRef]
26. Yaacoub, J.P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Microprocess. Microsyst.* **2020**, *77*, 103201. [CrossRef] [PubMed]
27. Feng, J.; Yang, L.T.; Gati, N.J.; Xie, X.; Gavuna, B.S. Privacy-preserving computation in cyber-physical-social systems: A survey of the state-of-the-art and perspectives. *Inf. Sci.* **2020**, *527*, 341–355. [CrossRef]
28. Attatfa, A.; Renaud, K.; De Paoli, S. Cyber diplomacy: A systematic literature review. *Procedia Comput. Sci.* **2020**, *176*, 60–69. [CrossRef] [PubMed]