Exploring Formal Strategy Framework for the Security in IoT in e-health using Computational Intelligence

Youcef Ould Yahia, Soumya Banerjee, Samia Bouzefrane, Hanifa Boucheneb

Exploring Formal Strategy Framework for the Security in IoT in e-health using Computational Intelligence

[1]Youcef Oul Yahia, [2]Soumya Banerjee [3]Samia Bouzefrane,
[4]Hanifa Boucheneb
[1,3] Conservatoire National des Arts et Métiers,
Paris Cédex 03, France
[2]Birla Institute of Technology, Mesra, India
École Polytechnique de Montréal, Canada

July 13, 2016

Abstract

This chapter proposes a novel strategic framework and computationally intelligent model to measure possible vulnerabilities for security context in e-health. The essential input is provided from interconnected wireless sensors under Internet of Health (IoT) paradigm and intelligent social insects that could sense the possibility of threats for a patient moving in different physical locations during his medical diagnosis. Social insect ants can sense and communicate through a chemical, known as pheromone, remotely from their nest towards collection of food. Modeling the pheromone dynamics can be a precise measure to quantify the different e-health security issues like Sinkhole threat or sybil attack under IoT environment. The proposed pheromone alert is presented and compared statistically in terms of precision, recall to identify the classification of possible vulnerability.

1 Introduction

The emphasized growth of computational and web based resources improvise the different contexts of smart environment. Hence, emerging applications of smart and connected devices and *IoT(Internet of Things)* can be made more pervasive with respect to diversified applications. E-health incorporated with IoT is one of the recent vertical applications of smart environment [23] [24]. IoT in e-health can be used to track objects and people (staff and patients), identify and authenticate people, collect and sense data automatically. Conventionally, e-health provides a new method for using health resources - e.g. information, expenses, and medicines. Hence optimized utilization of resources

also becomes important. Although, there is a legitimate concern that security vulnerabilities could pose a significant risk as opposed to the popular usage of Machine to Machine communication (M2M) or IoT towards efficient optimization of resources. M2M describes devices that are connected to the Internet, using a variety of fixed and wireless networks and communicate with each other. There are various active components, data units and sensing elements persist to execute successful deployment of IoT orientation for e-health application. They include sensor devices and actuators, and networking, processing and storage [25] [26].

The overall level of security is upper-bounded by the weakest component in this interactive system. Hence, each component, and the holistic system must be designed with security measures. There are three basic attack vectors, and a corresponding attack surface to each vector. Data is the first attack surface, followed by the communication channels. There could be even malicious attacks to compromise the insulin pump of specific patients. The several aspects solicits to develop an application control comprising of sound alert system with continuous monitoring for all health related IoT devices. The expected behavior to be analyzed from such security framework could be the basis for building a tampering-resistant device in implementations [27]. Considering such manifold parameters of security measures, this paper contributes to a novel architecture to define normal model of security components of e-health in IoT paradigm, primarily utilizing computational intelligence. Broadly, the term of computational intelligence is defined as a set of nature-inspired computational methodologies and approaches to address complex real-world problems to which mathematical or traditional modeling cannot be adequate. The reason to justify computational intelligence could be bi-focal : firstly, the security strategy for IoT in the context of e-health application can be made adaptive to tune with the specific patient and requirement. For example, insulin or monitoring concerned remedies could be different for different patients and a generic framework of medical records cannot be appropriate. Secondly, to interact with data and different medical agents, they can learn from environment. The paper coins an application envisaging bio-inspired algorithms to measure, monitor and update the security alerts in the IoT framework. Bio-inspired elements mimic the natural insects, their dynamic and formal model could assist to develop an application interface for security context in IoT environment. Specifically, the collective behavior and pheromone mapping of social insects can be an interesting proposition to model the ant colony metaphor [28] in the form of mobile and connected devices as IoT. The strategy framework of security measures has been defined as a formal model of dynamic digital pheromone followed by their deposition, evaporation and reinforcement processes. It is significant that whenever IoT environment expands, level of pheromone differs and compared to exact value across the sensors under sensor graph. Certain deliberate tampering of patient on-line data could be vulnerable and can be measured with different suggested classification of output. At present, the model considers only single graph yielded from IoT, later more parallel such graphs could be tested and more secure e-health IoT applications can be invoked.

The major contribution of the paper has been depicted as follows:

- Comprehensive mathematical parameters as objective function is defined to measure the degree of risks or threats for Health IoT.
- Deployment of pheromone mark up as computationally intelligent tool across IoT environment.
- To compare the empirical parameters of standard IoT security benchmark protocol with the proposed model.

The remaining part of the paper has been organized as follows: Section 1.1 describes the basic motivation and need for applying computational intelligence in IoT interaction. Section 2 discusses similar works followed by a formal model, parameters and relevance in section 2.1. Section 3 introduces a generic algorithm of pheromone alert, envisaging computational intelligence. Section 4 discusses the post implementation scenario and data set where the e-health IoT behavior could be tested. Section 5 finally summarizes the results and mentions the relevance of further proposects of such application development. A brief glossary of essential definitions are provided at Appendix for readers.

1.1 Motivation

The e-health system provides new opportunities and improves the quality and efficiency of care while reducing costs. The purpose of the e-health is to make available to health professionals and patients' tools to collect, process, store, return and exchange of health data in automated, convenient, reliable and secure way. To illustrate the contribution of e-health, and we consider the example of patient monitoring. Indeed, traditionally to monitor a patient (heart rate, blood pressure, etc.), hospitalization is mandatory, which is constraining and expensive. However, with the Internet of Things (IoT) this monitoring can be extended easily to the patient's daily environment (home, workplace, etc.).This model allows considering a broad spectrum of application for self-care with medical measurements [1] and the preventive and Low-Cost Diagnostics. In short, we can imagine many applications for the e-health with IoT environment.

Internet of Things (IoT) ideally resembles to the linked and chained data representation among its various components like actuators, sensors and associated hardware.Wither wireless sensor network or any other ad-hoc network is seldom represented by a graph in which vertices correspond to the communication nodes. Directed edge from one vertex to another indicates, that the node corresponding to the former can send data directly to the node corresponding to the latter. It becomes generic to assume that propagation conditions depends on the range of transmission. If all nodes have equal transmission ranges, then the graph becomes undirected. A network is called connected if this associated graph is connected. A graph G is connected if and only if there exists a path between any pair of its vertices [35]. If a network is connected then any pair of nodes can communicate with each other, possibly taking multiple hops through

relay nodes. It is sometimes useful to consider stronger forms of connectivity, such as k-connectivity, in which the network remains connected even if $k - 1$ nodes are removed. If a network is k-connected ($k \geq 2$), it has better fault-tolerance than if it is merely 1-connected. Ensuring k-connectivity extends the network lifetime if nodes fail at random times [25] [26]. The essential parameters of IoT visualization leads to a virtual entity layer, an entity abstraction layer, device can be converged into :

- Capturing invariants & relevant complexity of environments shared by different IoT applications like smart home
- Entity models (nodes of the graph) capture real-time behavior
- Entity to entity and entity to device relationships
- Entity to entity group relationships

Figure 1 could be the visualized form of Graph of Things (GoT) and also ants are placed at random nodes of connectivity of IoT sensors.

These features are responsible for using substantial number of object oriented graph data bases like neo4j. Considering the baseline of IoT orientation, the present model converts the real instant into graph, on which the social insects e.g. ants are placed. The advantage of ants is their flexiblility to navigate and reinforce any path while enhancing the population towards that specific path. Ants use pheromone as their primary communication media and most importantly the dynamics of ant colony is programmable and formal mathematical models are available. Any type of security lapses and vulnerable events can be measured.

The flow of the proposed model can be given as :

- Step 1: Conversion of IoT graph , to be known as Graph of Things (GoT) or G
- Step 2: Positioning the ants on random nodes on the graph
- Step 3: Depending on sensors interaction, physical positions of a patient, the node(s) will be reiterated and a particular threshold values of nodes are predefined. The value is based on time to access the minimum intra communication link, access point and termination criteria (See Figure 3).
- Step 4: Deposition of pheromone across the nodes, where connectivity and interaction are present
- Step 5: If the value of pheromone differs from the threshold value of a particular sensors -connected path, alert message/signal will be initiated anticipating vulnerable points across IoT connection.

Following the above mentioned steps, pheromone alert algorithm and model is presented. Relevant background and scope is also discussed.

Figure 1: **Visualization of GoT & Ants**

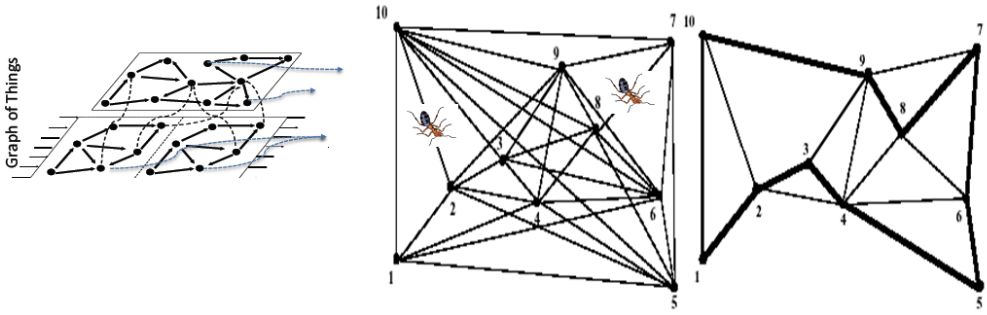
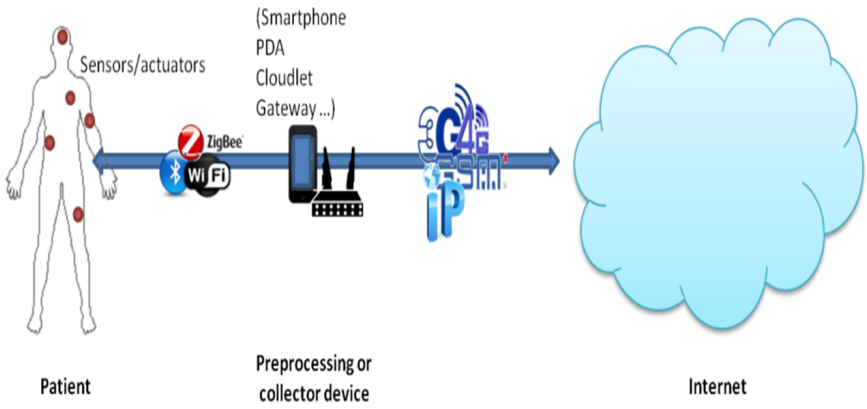


Figure 2: **Conceptual Representation of IoT & e-health**



2 Similar Works

There are significant developments of e-health applications with IoT environment. The authors of [2] demonstrate the implementation ease of such model. In Taiwan, a telemedicine platform is deployed for monitoring elderly [3].

Karunarathne et al.[4] propose a similar application for monitoring people predisposed to cardiovascular accidents with motion and acceleration sensors. Research in the field of public health provides a platform for the acquisition of epidemiological data [5]. In Spain, a national R & D project was initiated to create new health services for addicts and chronically ill, using technologies related to the Internet of Things and Cloud Computing[6].

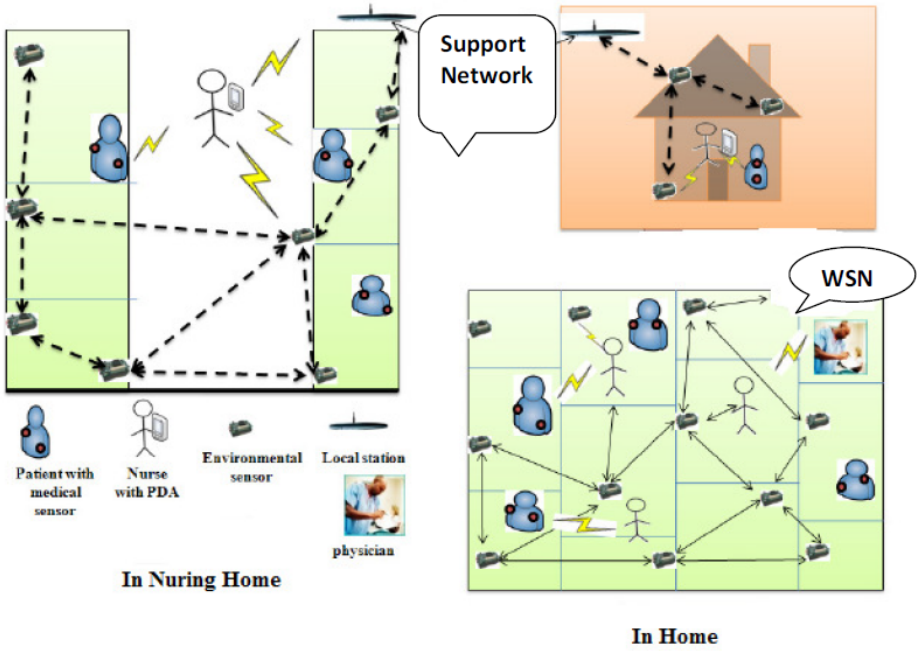
There are technological and commercial benefits of e-health by harnessing the opportunities offered by IoT. However, the main challenge of using these technologies in the field of healthcare is the protection of patient data and privacy, because the loss of the security properties may have a negative impact on the patient and the health systems in general. These impacts can be legal, ethical or financial and even can cause damage to the patient's health. According to HIPAA general rule, which is known as Standards for Privacy of Individually Identifiable Health Information in United States, a covered entity (Health Care Providers, Health Plans, etc.) must identify and protect against reasonably anticipated threats to the security or integrity of the information and protect against reasonably anticipated, impermissible uses or disclosures[7].It means that an application that collects processing and store patient's data must ensure the confidentiality and integrity of data and performs access restrictions. Furthermore the service provider must deploy a solution to measure, monitor and update the security alerts. Gope and Hwang, in [8], refer to several sample applications and research projects on e-health where security has deficiency or

pending aspects. An additional challenge for this application is the limitation of connected objects, in terms of energy, computation and memory capacity. In case of e-health using IoT technology, we must deal with strong security requirements and physical constraints of IoT devices. The research community proposes a wide range of security solutions for e-health that take into account the constraints of IoT. These solutions aimed towards two directions, those specific for e-health systems and those tailoring of security protocols for the IP-based IoT[9],to protect data and communication channels. However, malicious attacks that may compromise the IoT devices are serious threat in e-health applications. IoT Communications security: In traditional network communications, security is assured by transport (eg. TLS/SSL) or network (eg. IPSec) layers technologies, providing all the security features. In the context of IoT, the resource limitations of things make it difficult to deploy traditional security technologies, such as update, control and management of authentication and access privileges.A review of the communication security solutions for IoTis given by Keoh et al.[10]. The authors focus on solutions that will be used in conjunction with the Constrained Application Protocol (CoAP), the equivalent of http in constrained networks. The most promising solution is Datagram Transport Layer Security (DTLS) that is derived from TLS. This solution is promoted by IETF. So, many researchers consider IPsec combined with minimal IKEv2 as desirable security solutions for IoT[10]. This approach is reinforced by using 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) compressions for IPsec payload headers[9]. Abdmeziem and Tandjaouimention other proposed solutions like tailoring to Mikey-Ticket protocol for e-health applications in the context of IoT lightweight extensions to HIP DEX (Host Identity Protocol Diet Exchange) that could be generalized to DTLS and different delegation procedures of protocol's primitives to offload the computational load to third parties. However, they noticed that even these approaches reduce the computational load of the constrained devices. They break the end-to-end principle by requiring a third trusted party.

Security solutions for implementing e-health In addition to security solutions based on cryptography for e-health IoT environments [8, 9, 11, 12, 13] to control data access and authentication, some research works rely on adaptive approaches. Adaptive security solutions are in general based on risk analysis with rigorous identification of vulnerabilities. For e-health, the first vulnerability is related to the IoT device resulting from capacity limitation to implement complex security schemes. Additionally, we need a certain metric to quantify the risk and other parameters. Savola et al. [1] Propose heuristics for security metrics development, based on the risk-analysis results achieved through two view-points: the service provider's business perspective, and the end-user's perspective. Nevertheless, these analyzes don't focus on privacy and assume that data reside in a well-managed shared database on the service provider's premises. Authors, in[14], propose a risk-based adaptive security framework for IoT in eHealth. They use a game theory to analyze the monitored information and context awareness to estimate and predict dynamically the security and privacy risks and future benefits. The result of the analysis is used to make decision

and adapt reaction by adjusting different parameters (encryption parameters, security protocols and algorithms, security policies...) or by making dynamic changes in the structure of the security system. The work presented by the authors has been carried out in a research project ASSET (Adaptive Security for Smart Internet of Things e-health). In the same project, we can find in [15] references to adaptive security researches. In[16], the authors present a state of the art of game theory models for adaptive security and develop a Markov game-theoretic model for adaptive security in the IoT for e-health applications. The test and evaluation are performed by simulating an adaptive security policy focusing on authentication. This approach allows adapting the security parameters of the system according to dynamic changing of the environment, but as it is a reactive solution, it is necessary to test it under real conditions to validate the reactivity and efficiency. Finally, the solutions proposed in the literature for the safety of e-health environment are confronted principally with the IoT's security challenge that comes down to the difficulty of implementing effective security measures using heterogeneous technologies and within limited-resource devices (limitations in terms of energy, calculation and memory). This challenge is exacerbated by the dynamics of the environment induced by mobile devices. Therefore, most of the proposed solutions which are based on cryptography are not effective because they are static solutions proposed for a dynamic environment. Furthermore, these solutions are not designed to detect a compromised IoT device or an abnormal behavior. Computational intelligence as ant colony is largely used in the literature in many fields like data retrieval in Cloud Computing [17], secure building [18], to control road traffic in emergency situations [19] or to propose a dynamic routing for IoT [20]. Ant colony algorithm is based on simulating the social behavior of ants to reach a goal, like finding the shortest path or finding and storing food, which is done thanks to cooperative ants that rely on their individual experience to determine a route based on deposition and evaporation of pheromone. Hence, using an algorithm which reproduces this model can solve many complex problems. Regarding security, ant colony approach is generally used to detect intrusion in networks or to enhance network security. The intrusion detection is based on a behavior analysis (resources use, access request, protocol, etc.) or on a pattern matching, which is less efficient to detect unknown threats. Authors of [21] use an ant colony algorithm to find out vulnerabilities in networks. They apply the algorithm on a network map obtained from network scanning, and remote OS/application detection tools. To improve existing solutions, they propose to detect vulnerabilities by moving from one node to another, and by constructing a graph where ants move using a particular decision policy and a pheromone update. In [22], the authors propose to apply ant colony algorithm on a network model to analyze behaviors and to determine invasion route. This leads to identify and evaluate dynamically the system safety state, and to detect intrusion in this route in order to provide an appropriate response. Although the ant colony algorithm resolves many problems, none of these solutions consider detecting threats in e-health with IoT environment in a strongly dynamic and constringent environment.

Figure 3: **Different Dynamic Physical locations of Patient**



2.1 Model, Parameters and Relevance: Bio-inspired algorithm & Pheromone Map

We conceive a real function q , with range [0,1], , that shall express the degree of how well the requirements are fulfilled in the system state in question. A low value, below a given threshold, denotes that the system state in question is unacceptable, while a value close to 1 denotes that most requirements are well fulfilled. The function q is composed of three parts:

- security requirements that need to be fulfilled, expressed in the function q_S;
- degree of fulfilled QoS requirements, expressed in the function q_Q; and
- costs that occur due to mitigation of threats.

The function q is then composed of a product of all partial functions of:

$$i \in_{S,Q,C} : q = \prod_i q_i^{p_i} \tag{1}$$

Where,
S represnts: all reliable system sttates
Q: Acceptable states of system under possible constraints
C: Cost to mainitain essential security and qality of service

Here the p_i are the values of pheromone of ant colony agents as real numbers $0 \leq p_i < \infty$ and express the importance of a single q_i, large values indicating more importance. Pheromone value $p_i = 1$ is considered neutral. The importance of each parameter is defined by the assessor according to the nature of the requirement before assessing the $q_i$values.

Ant colony optimization is a nature-inspired intelligent algorithm initially proposed by [28] Dorigo et al., which mimics the social behaviors of biological ants to look for food. Each ant randomly starts to search without any location information of food and communicates with each other by releasing a chemical substance called pheromone in the search path. The concentration of pheromone on a given path reflects that the path is pros or cons. If the search path is not visited by more ants, its pheromone will be evaporated gradually over time. Otherwise, it is enhanced when more ants pass. As ants that arrive in the vicinity prefer to select the path with higher pheromone concentration, ants can establish a short path between their nest and food source. By this way, the later ants are gradually approaching the location of food as guided by the pheromone. This food foraging behavior of ants has been modeled in ACO algorithm. An optimization problem whose solution can be represented by a combination of components is treated as food source and an artificial ant is used to find a solution with shorter path to food source (better solution for the optimization problem). By using graphs terminology, it is assumed that the vertices and edges are the possible components of the solution, and each edge is associated with a pheromone value. A potential solution is constructed

by an ant through components selection, which is performed probabilistically based on the pheromone concentration in components. After that, the solution is assessed by an evaluation function and the components are assigned with the renewed pheromone concentrations that are proportional to its evaluated quality. Generally, the components of high-quality solution are allocated with more pheromone concentrations. Therefore, the later ants have higher probabilities to select the better components, which contribute to finding a better solution. After sufficient iterations are executed, ants will eventually gather toward a feasible and good solution. Referring Table 1, it could be evident to position ants pheromone with e-health security contexts.

Let, i and j be two successive nodes on the tour of an ant and τ_{ij}(t) be the pheromone concentration created by the ant at time t and associated with the edge of the graph joining the nodes i and j.

Let $\rho > 0$ be the pheromone evaporation rate, and $\Delta\tau_{ij}$(t) be the pheromone deposited by ant k at time t. Here, ant k traverses through node i and j.

Here, ant constructs the solution approach and deposits the pheromone for each edge of movement graph.

The ant colony optimization algorithm is based on the stochastic propagation of multiple moving agents (ants) through a graph [25]. Typically, the probability for the k^{th} ant to move from node i to node j of the graph is calculated denoted by p using eq.(3). Moreover, at each step, the amount of pheromone is updated according to:

$$\tau_{ij}(t+1) = (1-\rho)\tau_{ij}(k)v\frac{Q}{L_k} \tag{2}$$

where,

the parameter ρ describes the pheromone evaporation, $\nu = 1$ if the (i, j) edge was visited by the k^{th} ant and zero otherwise, Q is a constant and L_k is the "cost" of the k-th path (typically its length).

In the original Ant Colony System, when building a tour, ant k at the current position of city i chooses the next city j to move according to the so-called pseudorandom proportional rule as stated:

$$p_{ij}^{k} = \frac{[\tau_{ij}]^{\alpha}[\eta_{ij}]^{\beta}}{\sum_{l\in \mathrm{N\_i\hat{}k}}[[\tau_{ij}]^{\alpha}[\eta_{ij}]^{\beta}} \tag{3}$$

if j$\in {N_i}^k$, where $\eta_{ij} = 1/d_{ij}$, is a heuristic that is available a priori and α,β are the respective parameters to determine the relative influence of pheromone trail of sensing zone in real time, ${N_i}^k$ is the feasible neighborhood of moving ant k, when being at locations, which is not still listed by the ant, i.e that particular coordinate is untraversed so far.

The contents of Table 1 has become significant to represent the analogical perspective of ants and mobile devices, which are being connected with e-health application and different relevant sensors. The concept of pheromone alert can be explained with a brief system set up of e-health application. The primary reason of choosing ant's pheromone is to combat with the uncertainty in threat

Table 1: **Analogy of Mobile Objects with Ants**

e-Health IoT	**Ant Colony & Pheromone**
Mobility of patients & their smart devices as phone, tablets	Exploits Graph zone with minimum cost for health IoT
Presence of local memory device	Ant Can refer, compare and evaluate from past experience
Initial Position	Start state with transitions

detection. As chances of attack paths, pattern of data leakage and tampering poses a significant uncertain problem to sensor and IoT interfaces, especially when facing a continuously environment like patients' different states, hence appropriate measures are required. To overcome uncertainty, social insects in the proposed application would continually gather information about their surroundings [27]. The foragers at certain central position of Graph of Things often have a well-developed memory [25]. In addition, social insects can share valuable information, such as safety, quality and authenticity of information flow towards a particular patient [26]. The proposed approach corresponds to the following salient points:

- A patient has been investigated with medical check up in different environments like home, clinic, dispensing room or from information on travel of the patient. and he has to be monitored continuously through wireless sensors and IoT devices.

- Similar to device interaction of IoT, a GoT (Graph of Things) for different functions of q concerning different events can be formulated. GoT can be defined as consuming and curating stream data sources of IoT to provide simple interface to filter, aggregate, enrich, and analyze graph-based patterns to visualize business in real-time, detect urgent situations, and automate immediate actions [28].

- Pheromone alert is employed with middleware framework of IoT and GoT orientation for the sensor framework. The patient positioning him at different places starting from home, travel, waiting in the clinic, and on the treatment phases. A group of ants can be positioned on any two random successive nodes of linked graph of either IoT or GoT.

- The amount of pheromone deposition to reinforce the possibility of data threats from sensors and IoT devices, the following broad outlines:

- Process of Replication: Each ant makes copies of itself. Replicated agents are placed on the node of GoT, that their parent resides on. They inherit the parent's operational parameters as well as a constant amount of information flow across the Internet and Graph of Things. Mutation may occur at the probability of $1/n_b$ to randomly alter each of the inherited operational parameters. n_b denotes the number of operational parameters of each ant). Probabilistically, one operational parameter is altered via mutation. Each child agent contains the sensor data from its predecessors or parents during the traversal of GoT, and carries it to a initial or starting position. Different ants may choose different paths for initial position (where to traverse) depending on their operational and positional parameters.

- Swarming [32]: Each agent may swarm (or merge) with others at an intermediate node on its way to a terminal node. On each intermediate node, it waits for a particular period (t_w) for other agents to arrive at the node. If it meets the ant agents migrating to the same terminal point, it merges with them and aggregates their sensor data. It also uses the operational parameters of the best one in those swarming/aggregating agents in terms of performance objectives. The swarming behavior is intended to save resource consumption by aggregating multiple agents and reducing the number of data transmissions. If swarming behavior returns abnormal event, then the intrusion in linked /aggregated data to be monitored for possible threats.

- Pheromone sensing and migration: On each intermediate node toward a starting point or node, each h agent chooses the next-hop node in its migration by sensing three types of pheromones available on the local node: Starting point, migration and alert pheromones. Each start node periodically propagates a heuristics rule to apply pheromone to individual nodes. Their concentration decays on a hop-by-hop basis. All agents are dying on a node at the same time, a randomly selected one will survive. On each neighboring nodes, agents can sense where terminal points exist approximately, and move toward them by increasing a concentration gradient of pheromone value of terminal point. Agents emit migration pheromones on their local nodes, when they migrate to neighboring nodes. Each migration pheromone references the destination node an agent. Agents also emit alert pheromones, when they fail migrations within a time-out period. Migration failures can occur due to certain possible data integration issues or attacks, for example, node/link failures due to possible threats. Each alert pheromone references the node that an agent could not migrate to. Each of migration and alert pheromones has its own concentration, which decays by half at each duty cycle. A pheromone disappears when its concentration becomes zero. Each agent examines Eq.(4) to determine which next-hop node it migrates to.

- Mathematically, the representation will be similar to :

$$S_j = \sum_{t=1} w_t \frac{P_{t,j} - P_{t_{min}}}{P_{t_{max}} - P_{t_{min}}} \tag{4}$$

Here, weighted sum (S_j) for each neighboring node j, and moves to a node that generates the highest weighted sum. This could be the alert indication.

t denotes pheromone type; P_1, j , P_2 j and P_3, j represent the concentrations of starting point, migration and alert pheromones on the node j. $P_{t_{max}}$ and $P_{t_{min}}$ denote the maximum and minimum concentrations of P_t among all neighboring nodes.

2.1.1 Properties and Validation of Pheromone deposition on Internet of Things (IoT)

This work considers a few important concept concerning the properties of ant colony and pheromone. The main logical assumption for dispersing pheromone across the IoT driven Graph of Things, is important to presume certain properties and resolving the analogical model to identify the food source of ant, nest and path where the ants are being traversed. The property foraging is the prime idea to be incorporated with ants' movement across (foraging property, Refer appendix) IoT graph. In this model, food source are the pilot value(s) of any combination of sensor (specifically in terms of access control and time). Primarily, ants search for this pilot value through local pheromone deposition, if pheromone deposition differs, then it can anticipate the possible reason or threats behind it. The proposed model is population based heuristics, it signifies that if there are larger dimensions of IoTs and GoTs, then number of watch ants could be more to evoke alert signal. The primary parameters envisaged as :

- Density of foraging ants
- Density of ants returning to the nest with food
- Concentration of pheromone
- Concentration of food source
- Rate of pheromone deposition
- Rate of pheromone evaporation
- Rate of food removal by foraging ant

Categorically, the diffusion process has not been included here, instead a constant deposition of pheromone on IoT graph is assumed(Refer eq.(7)). However, pheromone deposition and evaporation times are modeled by Poisson processes: each ant has a probability unit per unit of time to lay down a pheromone and each pheromone has a probability $1/T_p$ per unit of time to disappear or to

evaporate. Pheromone deposition mediates the interactions between the ants. This interaction is non-local in both space and time (because the ant which has deposited a pheromone may have moved away quite far before another ant interacts with it). More description can be referred in [29].

3 Proposed Algorithm : *Pheromone Alert*

The proposed algorithm *pheromone alert* is a specific algorithm (based on chemical from social insects e.g. pheromone) to be applied on undirected Graph of Things, yield from sensor networks. The network orientation keeps on changing for a specific patient on study, depending on his different physical positions and states, however protocol of all communications across the health sensors remain the same. The primary objective of the pheromone alert algorithm is to measure the possibility of threats, data leakage or attacks on the basis of deposition, duration and evaporation of pheromone across any random nodes of sensor graph yield through e-health application and interaction with a patient. The diffusion processes foster computational intelligence, so that IoT driven paradigm of sensor network can be monitored through social insect's pheromone. The different phases are:

- Injection of pheromone, which defines how fast a particular pheromone is released across the nodes of graph G,
- Evaporation rate, which determines how quickly the pheromone strength fades over time,
- Influence or impression, that characterizes how much the pheromone influences the physical map of sensor organization. It means that distribution of pheromone on GoT can also indicate critical points, from where e-health application may suffer vulnerable attacks.

While formulating the proposed algorithm, pheromone deposition and evaporation process are important. Formalization of the processes for deposition and evaporation across nodes of graph can be defined as follows:

3.1 Formal Proposition: Pheromone Deposition

Let $\rho > 0$ be the pheromone evaporation rate, and $\Delta\tau_{ij}$ (t) be the pheromone deposited by ant k at time t :

$$\tau_{ij}(t) = (1-\rho)\tau_{ij}(t-1) + \sum_{k=1}^{m} \Delta_{ij}^{k}(t) \tag{5}$$

From eq.(5), the difference can be expressed as $\tau_{ij}(t) - \tau_{ij}(t-1) = -\rho\tau_{ij}(t-1) + \sum_{k=1}^{m} \Delta_{ij}^{k}(t)$.

Conventionally, including differential operator D $\Longrightarrow \frac{d\tau_{ij}}{dt}$ and finally the expression of pheromone deposition across edge is given as :

$$D = -\rho\tau_{ij}(t-1) + \sum_{k=1}^{m} \Delta_{ij}^{k}(t) \tag{6}$$

$\implies (D+\rho)ij = 0 \implies D = -\rho$ is the complementary form.

Considering the stable state of IoT protocol and constant deposition of pheromone across IoT graph G, the complementary function and its particular integral is recombined at $\tau_{ij}(t)$ =C_k.

Hence, final deposition value of pheromone is evaluated as :

$$\tau_{ij}(t) = D + \sum_{k=1}^{m} C_k/\rho \tag{7}$$

3.1.1 Formal Proposition : Pheromone Evaporation

Let the pheromone evaporation ρ at time t be ρ_t, where the value of ρ_t, lies in the closed interval [0, 1]. Now the recurrence relation for the evaporation of pheromone at time (t + 1) is given by [36] :

$$\rho_{t+1} = \alpha\rho_t + \beta(1-\rho_t) = k\rho_t + \beta \tag{8}$$

where α, β are two constants, such that $0 \leq \alpha, \beta \leq 1$ and k= α−β

3.2 Expected Output

Monitoring and Eavesdropping on Patient Vital Signs

- Cost = Sensor jammed (level 1) Threats to Information When in Transit
- Damage = Deliberate collisions caused on GoT(level lI)
- Selective forwarding: In multi-hop environment [7,54,56,57], sensor packets (i.e., health data or environmental data) are expected to be forwarded to the base station or remote server via multi-hop routing. In this threat, malicious nodes may refuse to forward certain messages (e.g., ECG, temperature, etc.) and may simply drop them, so that they cannot be broadcast further. This threat can be stronger if the attacker is explicitly included in the routing path: potency (collisions) = collisions caused/ cost (level III)
- Sinkhole threat: In this threat, an attacker tries to attract all neighboring nodes to establish routes through a malicious node: potency (map difference) = ∑map differences caused /cost of traversal (level IV)
- Sybil Attack: In this attack, a compromised node presents multiple fake identities to other neighboring nodes in the network. With this broader expected output, the high level description of algorithm is presented, however the algorithm can be extended for more pheromone mark ups and levels of authentication of e-health vulnerabilities.

Logical representation of the patients' states are given as the classification of sensor's paths under different states. In the section 2.1 Eq. (1) describes brief about the objective function q for the entire IoT repositories. Referring the classical ant colony model as in eq.(2) and (3), basic elements of the proposed solution is the classification rule induction on the basis of attribute terms associating e-health diagnostic sensor based parameters. An Ant colony algorithm is used here for classification to quantify the logical level of vulnerability, path or attacks in the form of IF-THEN classification rules. The generic form is :

IF (conditions) THEN (class), where conditions follow the form (term1) AND (term 2) AND ... AND (term n).

The class to be predicted by the classification rule is represented by the THEN part corresponding to the rule's consequent and the IF part corresponds to the rule's antecedent. An instance that satisfies the IF part will be assigned the class predicted by the rule. Bursa and Lhotska (2007) in their work [37] described the clustering techniques used through ant colonies. Their study revealed two types of biological signals: Electrocardiograms (ECG) and Electroencephalogram (EEG). Electro-cardiograms (ECG) an electrical recording of heart activity is one of the most important diagnostics techniques used in patients. It's processing consists of seven stages: signal pre-processing, signal transfer and/or storage, digital signal processing and feature extraction, clustering of the similar data, signal classification and expert validation. From the ECG signal, eight features have been automatically extracted and two classes have been used (normal cardiac action and abnormal cardiac action) for the above mentioned study. Electroencephalogram (EEG) is an electrical recording of brain activity which is used in order to classify stages of sleep. The EEG recordings used contain eight EEG channels, Electrooculogram (EOG), Electromyogram (EMG), Respiratory channel (PNG) and Electrocardiogram (ECG). All these recordings have been classified by a medical expert into four classes (wake, quiet sleep, active sleep, movement artifact). The sensors and IoT devices are incorporated. The recordings are validated as real time and any bifurcation of recorded values could be senses as alert for possible threats with initial pheromone value deposited on random nodes of *Graph of Things(GoT).*

4 Data & Implementation

The initial data source for instantiation of the proposal is the Machine Learning data Repository (UCI)[1]. The standard raspberry Pi interface has been used and ACO-Pants 0.5.2 implementation of the ACO Meta-Heuristic also accomplished. Synthetic data set has been envisaged for pheromone trailing, intensity and direction across the nodes of graph G. Table 2 is the extraction of parameters being referred in the simulation model.

In Figure 3, plot of the experiments are presented. Fewer pheromone depositions are performed towards initial traversal of ants across health sensors in different physical states (q) of patients. Definitely, the cycle could be completed

[1] http://archives.ics.uci.edu/ml/datasets/MHEALTH+Dataset

Algorithm 1 High Level Description of Proposed Algorithm *Pheromone Alert*

Input: Initialization of values S= 0; t = current time ; t[ ]=null; =100 initial alert pheromone value (say 100 is threshold value)

T= time stamp (consider 10 hrs of inspection) , Graph G , patient state q, Constants : α, β, IoT$\in$ *GoT* $\in$G , R = φ /* R: set of roots */

Output: Classification of threats or vulnerabilities as **Level 1, Level II, Level III or Level IV**

/* Separate functions could be invoked*/

begin

for each v$\in$S /* S : Set of nodes in vulnerable area*/

if v has no incoming edge

R =R$\bigcup$ findR (v)

end for

findR (node u)

R'= ϕ

if u is not yet visited

mark u is visited

else

return φ

if u has no outgoing edge return {u}

for each e(u,v)

R' = R' $\bigcup$ findR(v)

end for

return R'

end findR /* Identification of possibility*/

t[ ]= Recorded values of signal (pheromone) for patient initial state

while (each(t[ ]) matches with pilot _pheromone_value || actual _pheromone_value)

Display as linked value to the recorded pheromone unit on graph G;

Increment S value until end of signal and position value as per eq. (1);

end while

Set of nodes that match for given signal on Graph G ={1,2,3,....,n}

do

for all nodes of Graph G ={1,2,.....,n}

Choose node i with random probability

Repeat for relevant GoT

do pheromone updating and pheromone evaporation

end for

Choose next immediate node $j \in s$ with probability until s= null probation t[ ]= tokens (pheromone) while (each (t[ ]) matches with pilot_pheromone _value|| actual_pheromone value)

Evaluate pheromone updating as per eq.(3), (5) & (6)

Calculate pheromone evaporation as per eq. (8)

Detect Levels of Output

if actual pheromone_value >pilot _pheromone_value$\geq$ 100 units

Pick Edge of Graph G as either of LI to L IV

end if

for all IoT$\in$ *GoT*

do pheromone updating and pheromone evaporation; // eq. (5), (6) & (8)

end for

Repeat until G is traversed

end

Figure 4: Effect of Pheromone Deposition & Traversal on IoT

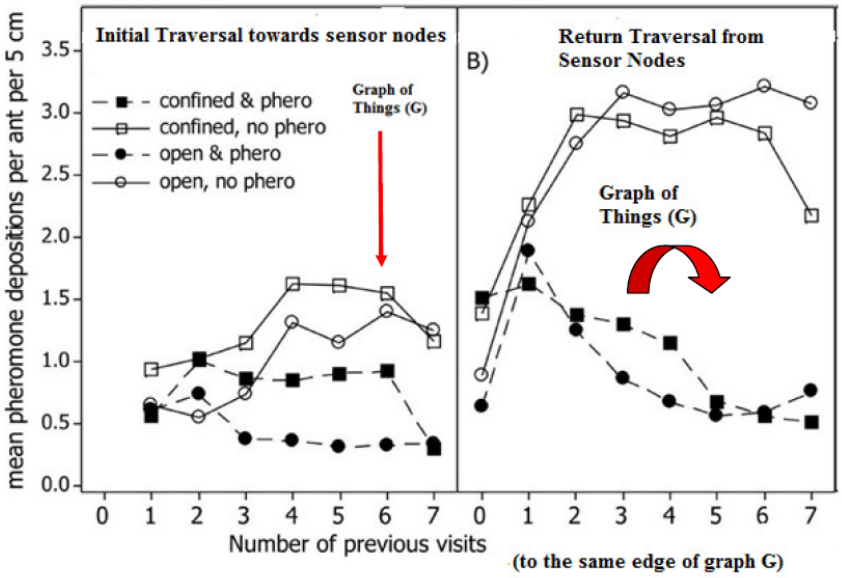


Table 2: **Numerical Values of Ants' Parameters**

Description	Value
No. of Ants	200
Speed of Ant	2 cm/s
Pheromone deposition rate	.2 s−1
Pheromone lifetime	100 s
Threat Detection radius	5 cm

once the ants compare the pilot values of pheromone and actual deposition value. The value could be different due to the possibility of intermediate data leakage and threats. Hence, on the reverse traversal, when ants are retuning to their initial position (swarming process, referred in section 2.1), pheromone deposition was lower, if pheromone was allowed to build up, and was higher if pheromone was continually removed (B). Outgoing ants deposited less pheromone, if they would go on to c on their upcoming committee a false alert decision. Returning ants deposited more pheromone, if they had just performed an error value on the current visit. This is driven by the likelihood of depositing pheromone at all, rather than by pheromone deposition intensity. Data from both ants, which did and did not deposit pheromone are merged in this figure. Data from all open treatments, and both bifurcations, have been merged for clarity. Not all the ants are positioned and deployed for pheromone deposition, as initially 2 random nodes were selected for movement on IoT graph.

4.1 Evaluation of Results

The initial data set was referred from UCI, although for security level classification, data set was not directly available. Hence, synthetic data set was created in consultation of UCI. The distribution is known and the novelty of algorithm is tested.

The dataset is a two-dimensional dataset consisting of four clusters arranged as a square. Data elements for each individual cluster are generated using the normal distribution, $N(\overrightarrow{\mu}, \overrightarrow{\sigma})$. The number of clusters, the sizes of the individual clusters, the mean value, $\overrightarrow{\mu}$ and vector of the standard deviation, $\overrightarrow{\sigma}$ for each normal distribution are used to generate this set. That is, the normal distributions of data elements pertaining to this formulation are (N(−5,2),N(−5,2)),(N(5,2),N(5,2)), (N(−5,2),N(5,2)) and (N(5,2),N(−5,2)). The dataset is initialized to 100 data elements. The idea can be referred from [39].

The set up of IoT and yielded GoT can be formulated as graph G and thereby considering the following parameters for initial statistical validation :

Table 3: **Evaluation and Post Implementation Parameters**

Parameters	**Initial**	**Mean**	**SD**
Edge	5	8	1.4
Step Size	0.1	0.1	0
Complement	1	5.07	4.48
Detection of Threat as Difference	1	1.5	0.5
Evaporation(%)	0.01	0.06	0.04
Residual Values	0	1.01	0.81

- Maximum Edge Length - the maximum number of steps on each edge;
- Step Size - equates to a fraction of a Standard Deviation;
- Ant Complement - an integral unit representing the number of ants present per feature per node;
- Detection Range for Ordinal Dimensions - steps above or below a mean value (refer eq.(6), (7), (8) ;
- Quantity of Pheromone Deposited - an integral value representing the pheromone in the proposed ;
- Evaporation Rate - a percentage applied to pheromone quantity;
- Residual Parameter - a percentage of the sum of all pheromones on selected edges.

Table 3 snaps about the statistical measures of the parameters under consideration to demonstrate vulnerability pattern classification on IOT graph using pheromone alert algorithm.

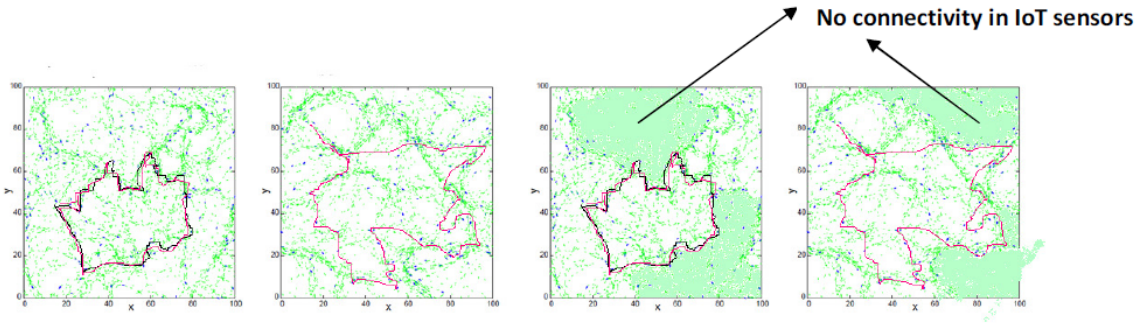
However, the classification is compared (Refer Table 4) with standard precession, Recall and Jaccard coefficients for mean value and SD. For simple illustration, an initial deposition value is required that connects two nodes in a way that the pheromone scent is strong enough to survive the impact of evaporation for a predetermined amount of time. Functionally, this is determined by the time required for the ant to traverse the longest edge of sensor graph and still adequate pheromone on the first step (considering constant deposition on the nodes at random probability). Given that the average edge lengths used are of approximately 8 steps, this implies an ant takes 8 time cycles to traverse an edge. Hence, the pheromone on the edge must survive for 8 time cycles. If the amount deposited is 25 units, subject to an evaporation rate of 10%, after 10 steps it has nearly completely evaporated. The evaporation parameter is important, as the classification of vulnerability or threat is irrelevant, where there is no pheromone. It denotes that either the connectivity of sensor node are not being established or *Graph of Things (GoT)* has not been produced.

Table 4: **Statistical Benchmarking of *Pheromone Alert***

Synthetic Data Set from UCI Results	**Mean**	**SD**
Precession	0.98	0.01
Recall	0.94	0.021
Jaccard	0.92	0.02

As in the presented model the approach of pheromone trail is important parameter, hence experimental simulation is made on IoT sensor to demonstrate with respect to different pheromone deposition on sensor connectivity, considering the changing physical locations of patients. Simulation parameters are chosen accordingly and the execution is accomplished with Python standard library. The ants are represented in blue and the pheromones in green. Red mark up denotes the IoT connectivity and where no pheromone is visible, it signifies no connectivity across IoT sensors (refer numerical values of Table 2). These all possible positions are dynamically simulated with respect to the movement of patient.

Figure 5: **Pheromone Deposition & IoT interaction,** at t= 500 s, 1000s, 1500s & 2000s



5 Conclusion

The presented chapter described a novel approach by utilizing computational intelligence in security aspects of IoT (Internet of Things) primarily towards e-health application. The prime objective of the contribution is to measure the degree of threat, vulnerability or attack in case of dynamic data grabbing for a patient pertaining to different physical locations like from home to diagnostic center. It is assumed that sensors of health centric paradigm are interconnected and in turn they produce a connected graph. The intermediate protocol for exchanging information across the sensors remains homogeneous and thus intelligent agents like social insects could traverse across the interconnected graph and inspect the scope and tendency of the nodes. If the pilot standard value formulated for IoT sensors against time out and access point is found to be deviated, then ant can sense the scope of possible vulnerable conditions across the node of sensors and alert signals are initiated towards main dash-board control. The entire functional unit is pivoted on the movement of pheromone, the chemical which can remotely communicate the connections across the sensor nodes under observation. The proposed model measured the pheromone deposition and evaporation amount to quantify the level and classification of e-health data exchange process. Several relevant parameters of ant colony, pheromone map and their analogical perspectives with IoT have been deployed. Experimentation is performed keeping the synthetic data set derived from public repository data source. At present, the security measures of IoT in e-health solicits conventional data integrity measures, instead of computational intelligence. The proposed model can justify such positioning of intelligent social insects to measure the degree of vulnerability and risk impact. Initially, the deposition of pheromone and no pheromone and evaporation of pheromone in sensor connectivity graph are being considered to classify the possible risk level. The extended plug-in software can be compatible with Rashbesrry pi for more classification of risks. The autonomic control of application, after the detection of possible vulnerability, can also be developed to control the inference and decision support level of data center administrator. The more such application will enhance for higher precision of e-health security in IoT paradigm.

References

[1] R. M. Savola, P. Savolainen, A. Evesti, H. Abie, and M. Sihvonen, Risk-driven security metrics development for an e-health IoT application, in Information Security for South Africa (ISSA), 2015, 2015, pp. 1–6.

[2] C. Doukas, T. Pliakas, and I. Maglogiannis, Mobile healthcare information management utilizing Cloud Computing and Android OS, Conf. Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. IEEE Eng. Med. Biol. Soc. Annu. Conf., vol. 2010, pp. 1037–1040, 2010.

[3] W. T. Tang, C. M. Hu, and C. Y. Hsu, A mobile phone based homecare management system on the cloud, in 2010 3rd International Conference on Biomedical Engineering and Informatics, vol. 6, pp. 2442–2445, 2010.

[4] M. S. Karunarathne, S. A. Jones, S. W. Ekanayake, and P. N. Pathirana, Remote Monitoring System Enabling Cloud Technology upon Smart Phones and Inertial Sensors for Human Kinematics, in 2014 IEEE Fourth International Conference on Big Data and Cloud Computing (BdCloud), pp. 137–142, 2014.

[5] K. K. F. Tsoi, Y. H. Kuo, and H. M. Meng, A Data Capturing Platform in the Cloud for Behavioral Analysis among Smokers: An Application Platform for Public Health Research, in 2015 IEEE International Congress on Big Data, pp. 737–740, 2015.

[6] D. Gachet, M. de Buenaga, F. Aparicio, and V. Padrón, Integrating Internet of Things and Cloud Computing for Health Services Provisioning: The Virtual Cloud Carer Project, in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 918–921, 2012.

[7] O. for C. R. (OCR), Summary of the HIPAA Privacy Rule, HHS.gov, 07-May-2008. [Online]. Available: http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. [Accessed: 28-Jun-2016].

[8] P. Gope and T. Hwang, BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network, IEEE Sens. J., vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[9] M. R. Abdmeziem and D. Tandjaoui, An End-to-end Secure Key Management Protocol for e-Health Applications, Comput Electr Eng, vol. 44, no. C, pp. 184–197, May 2015.

[10] S. L. Keoh, S. S. Kumar, and H. Tschofenig, Securing the Internet of Things: A Standardization Perspective, IEEE Internet Things J., vol. 1, no. 3, pp. 265–275, Jun. 2014.

[11] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems," IEEEACM Trans. Comput. Biol. Bioinforma. IEEE ACM, vol. 13, no. 3, pp. 401–416, Jun. 2016.

[12] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A Medical Healthcare System for Privacy Protection Based on IoT," in 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 2015, pp. 217–222.

[13] A. Sharma, T. Goyal, E. S. Pilli, A. P. Mazumdar, M. C. Govil, and R. C. Joshi, "A Secure Hybrid Cloud Enabled architecture for Internet of Things," in 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 274–279.

[14] H. Abie and I. Balasingham, "Risk-based Adaptive Security for Smart IoT in eHealth," in Proceedings of the 7th International Conference on Body Area Networks, ICST, Brussels, Belgium, Belgium, 2012, pp. 269–275.

[15] K. Habib and W. Leister, "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures," in 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), 2015, pp. 1–5.

[16] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in 2014 IEEE International Conference on Communications (ICC), 2014, pp. 920–925.

[17] K.Sriprasadh and M.Prakash Kumar, "Ant Colony Optimization Technique for Secure Various Data Retrieval in Cloud Computing," International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014.

[18] Anita and Dr. S. S. Tyagi, "Providing Security for the Building Using Ant Colony Optimization Technique," International Journal of Scientific and Research Publications (IJSRP), 2013.

[19] "Secure distributed system inspired by ant colonies for road traffic management in emergency situations." [Online]. Available: https://www.researchgate.net/publication/288649044_Secure_distributed_system_inspired_by_ant_c [Accessed: 08-Jul-2016].

[20] Y. Lu and W. Hu, "Study on the Application of Ant Colony Algorithm in the Route of Internet of Things," Int. J. Smart Home, vol. 7, no. 3, pp. 365–374.

[21] Y. Wang and C. Wang, "Based on the Ant Colony Algorithm is a Distributed Intrusion Detection Method," Int. J. Secur. Its Appl., vol. 9, no. 4, pp. 141–152.

[22] Parul Chhikara and Arun K. Patel, "Enhancing Network Security using Ant Colony Optimization," Gl obal Journal of Computer Science and Technology Network, Web & Security Vo l ume 1 3 Issue 4 Version 1.0, 201AD.

[23] SENSEI,EUFP7project,onlineathttp://www.sensei-project.eu

[24] IoT-A,EUFP7project,onlineathttp://www.iot-a.eu

[25] Harald Naumann , IOT/M2M COOKBOOK , Copyright © 2015 Harald Naumann, Neustadt, Germany.

[26] Amelie Gyrard, Pankesh Patel, Soumya Kanti Datta, Muhammad Intizar Ali, Semantic Web meets Internet of Things (IoT) and Web of Things (WoT), International Conference on Semantic Web, Kobe, Japan, October 2016.

[27] David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese Internet of Things: Architectural Framework for eHealth Security, Journal of ICT, Vol. 3 & 4, 301–328, River Publishers, 2014.

[28] Ant Colony Optimization Marco Dorigo Thomas Stutzle, A Bradford Book The MIT Press,Massachusetts, 2004.

[29] Diestel, R. Graph Theory, electronic edition; Springer-Verlag: Heidelberg, Germany, 2005.

[30] Atay, F.; Stojmenovic, I.; Yanikomeroglu, H. Generating Random Graphs for the Simulation of Wireless Ad Hoc, Actuator, Sensor, and Internet Networks. In Proc. 8th IEEE Symposium on a World of Wireless, Mobile and Multimedia Networks WoWMoM, Helsinki, Finland, June 2007.

[31] E. Bonabeau, M. Dorigo, and G. Theraulaz. Inspiration for optimization from social insect behaviour. Nature 406:39– 42, Jul. 2000.

[32] J. P. Hecker, K. Letendre, K. Stolleis, D. Washington, and M. E. Moses. Formica ex Machina: ant swarm foraging from physical to virtual and back again. In Proceedings of the Eighth International Conference on Swarm Intelligence, 2012.

[33] M. Brambilla, E. Ferrante, M. Birattari, and M. Dorigo. Swarm Robotics: A Review from the Swarm Engineering Perspective. In IRIDIA Technical Report, 2012.

[34] D. Le-Phuoc, H. Q. Nguyen-Mau, J. X. Parreira, and M. Hauswirth. A middleware framework for scalable management of linked streams. Web Semantics: Science, Services and Agents on the World Wide Web, 0(0), 2012.

[35] R. Beckers, J. L. Deneubourg, and S. Goss. Trail laying behavior during food recruitment in the antLasius niger (L.). Insects Social, 39(1):59–72, 1992.

[36] Prasanna Kumar and G. S.Raghavendra , On the Evaporation Mechanism in the Ant Colony Optimization Algorithms, Ann.Comp. Science Ser., 9 , pp.51-56, 2011.

[37] Bursa, M., Lhotska, L.: Ant Colony Cooperative Strategy in Electrocardiogram and Electroencephalogram Data Clustering. In: Nature Inspired Cooperative Strategies for Optimization (NICSO 2007), pp. 323–333, 2007.

[38] Amorim, P., 2015. A continuous model of ant foraging with pheromones and trail formation. Proceeding Series of the Brazilian Society of Applied and Compu- tational Mathematics, Vol. 3, N. 1, 2015. http://dx.doi.org/10.5540/03.2015.003. 01.0323.

[39] Handl, J., Knowles, J., and Dorigo, M. Ant-based clustering: a comparative study of its relative performance with respect to k-means, average link and 1d-som. In Proceedings of the Third International Conference on Hybrid Intelligent Systems, IOS Press, 2003.

Appendix

Essential Definitions

- **Internet of Things (IoT)**: The internet of things (IoT) is the network of physical devices, vehicles, buildings and other accessories. The essential association and embedement could be with electronics, software, sensors, actuators, and network connectivity, which enable these objects to collect and exchange data.
- **e-health:** e-health is an accomplished interface of medical informatics, public health and business, referring to health services and information delivered or enhanced through the web centric technologies.
- **Computational Intelligence:** Computational Intelligence (CI) is an offshoot of artificial intelligence in which the emphasis is placed on heuristic algorithms such as fuzzy systems, neural networks and evolutionary computation.
- **Ant colony Optimization:** Ant colony optimization (ACO) is a population-based metaheuristic and it is basically used to find approximate solutions to difficult and hard optimization problems. In ACO, a set of software agents called artificial ants search for good solutions to a given optimization problem.
- **Pheromone:** A chemical substance that is usually produced by an animal and serves especially as a stimulus to other individuals of the same species for one or more behavioral responses

- **Pheromone Evaporation and deposition :** The process of accumulation and release of pheromone depending on the avilability of an edge to recah shotest path respectively.