IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Applications and Evaluations of *Bio-Inspired* approaches in Cloud Security: A Review

MD MANJURUL AHSAN[1], KISHOR DATTA GUPTA[2], ABHIJIT KUMAR NAG[3], SUBASH POUYDAL[2], ABBAS Z. KOUZANI[4], AND M A PARVEZ MAHMUD[4]

[1]School of Industrial and Systems Engineering, University of Oklahoma, Norman, OK 73019, USA
[2]Dept. of Computer Science, University of Memphis Memphis, Tennesse, USA
[3]Dept. of Computer Information Systems, Texas A&M University-Central Texas, Texas, USA
[4]School of Engineering, Deakin University, Geelong, VIC 3216, Australia

Corresponding author: M A PARVEZ MAHMUD (e-mail: m.a.mahmud@deakin.edu.au).

ABSTRACT Cloud computing gained much popularity in the recent past due to its many internet-based services related to data, application, operating system, and eliminating the need for central hardware access. Many of the challenges associated with cloud computing can be specified as network load, security intrusion, authentication, biometric identification, and information leakage. Numerous algorithms have been proposed and evaluated to solve those challenges. Among those, bio-inspired algorithms such as Evolutionary, Swarm, Immune, and Neural algorithms are the most prominent ones which are developed based on nature's ecosystems. Bio-inspired algorithms' adaptability allows many researchers and practitioners to utilize them to solve many security-related cloud computing issues. This paper aims to explore previous research, recent studies, challenges, and scope for further analysis of cloud security. Therefore, this study provides an overview of bio-inspired algorithms application and evaluations, taking into account cloud security challenges, such as Identity and Authentication, Access Control Systems, Protocol and Network Security, Trust Management, Intrusion Detection, Virtualization, and Forensic.

INDEX TERMS Cloud Computing, CyberSecurity, Evolutionary Algorithm, Swarm Intelligence, Neural Network

ABBREVIATION

IAS Identity and Authentication Security.
NN Neural Network.
GA Genetic Algorithm.
ACS Access Control Systems.
ID Intrusion Detection.
NF Network Forensics.
PNS Protocol and Network Security.
TM Trust Management.
PSO Particle Swarm Optimization.
WSN Wireless Sensor Network.
SI Swarm Intelligence.
VAN Vehicle Ad-hoc Network.

I. INTRODUCTION

CLOUD computing, maintained by a third party (via the internet), is the ability to access a set of computing resources composed of hardware, storage, networks, interfaces, and services [1]. Using these resources, users can access infrastructures, computing power, applications, and services on demand. It enables users to access their information, application, and data anywhere based on their needs. The privilege of cloud computing above conventional computing comprises agile, scalable, cost-efficient, and device and location independence [2].

Based on the facility type, cloud computing can be divided into three categories [3], such as public cloud (cloud service provider responsible for cloud management, distribution, and selling to the general public), private cloud (a company owns the cloud responsible for distribution and selling), and hybrid cloud (owned and distributed by several companies) [4]. Cloud computing service can be divided into three categories, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [5] as shown in Figure 1. Security is a crucial aspect of everyday computing, and as such, cloud computing is vehemently

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

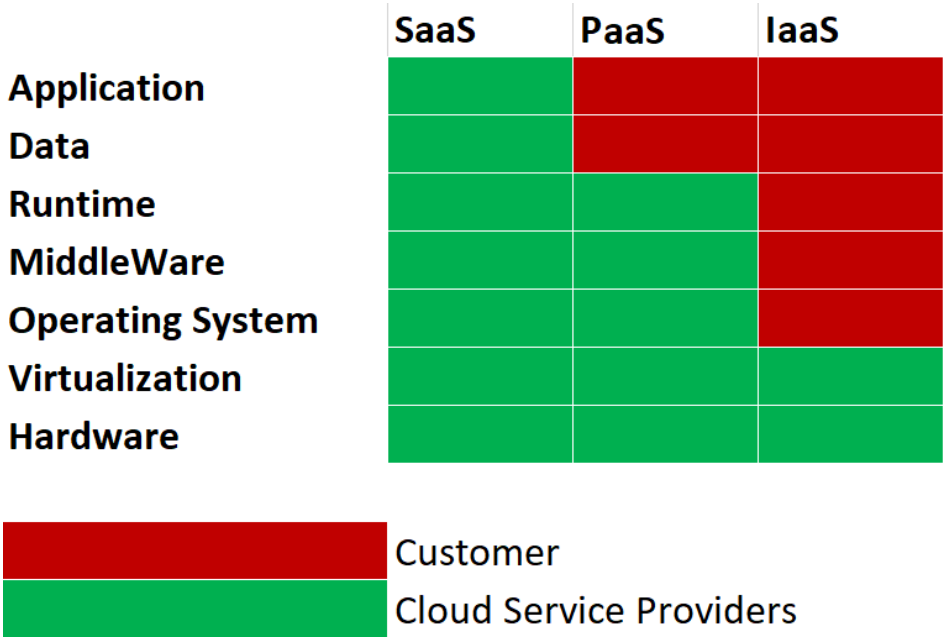

FIGURE 1. Layers architecture of cloud service for different component.

related to security due to sensitive and vital data stored on the cloud. Recently, lots of research is ongoing to answer the challenges of Big Data in cloud computing. Some of these challenges are related to information security, privacy, regulations, and performance issues. Apart from these, the risk of malicious insiders and the failure of cloud services are drawing attention to the consumer and retailers.

According to the Synopsis Cloud Security threat report (2018), 53% of organizations survey confirmed they have insider threats in their cloud system [6]. The culprit for the Marriott chain hotel data breach incident was an insider threat [7]. In addition, Application Programming Interface (API) in security is becoming more critical as it is the universal gateway for users to interact with cloud services. In 2018, British Airways hacked due to the instability of API within their cloud infrastructure [8]. Apart from this, other attacks like malware attack, cross-cloud attack, side-channel attacks are also rising at large.

The current age of Cyber Warfare makes big data and cloud computing a lucrative target for adversaries worldwide. A vast number of applications, services, and data storage transfers within the cloud are increasing due to convenience facilities (i.e., numerous storage, loss prevention, mobility), even though they do not provide enough security.

A. SECURITY CHALLENGES IN CLOUD-COMPUTING

Security in big data has three essential viewpoints: information assurance, security protocols, and data protection [9]. Security management for distributed computing aims to solve big data management issues, preserve the integrity of systems, and protect cyberspace from threats [10]. Big data security focuses on real-time dynamic security observations to identify any potential threat/vulnerability or even unusual behaviors. While keeping the data access speed at a feasible level, there is always a risk of confidential information leakages.

As big data heavily relies on cloud computing, cloud computing security aspects are required to be thoroughly evaluated. The concern behind this is that cloud computing security is not the same as traditional computing security [11]. There are several layers in a cloud computing network, such as wireless network distribution, peer-to-peer systems, and virtualization platforms [12]. Hence, just protecting different blocks may not be enough to secure the systems entirely. After the full system starts to work, unique security issues might arise in the individual blocks. Also, security challenges associated with small parts of cloud computing from the mobile browser, web engine to Linux server kernel, arise at an alarming rate. Cloud computing inherits them, which makes the security of cloud computing more challenging (see Table 1).

TABLE 1. Threats in Big data infrastructure

Assets	Representation
Infrastructure	Interoperability, Monitoring, Accountability
Virtualization	VM lifecycle, Container, context awareness
Resources&Tasks	Resource location, Task scheduling, offloading
Distribution	Cooperation N-tier management 'Soft state'
Mobility	Connectivity, Seamless hand off
Programmability	Usability, Session management

It seems integral for security providers to come up with new solutions to protect the viability/usability of cloud systems. Different types of algorithms are employed to protect the cloud, such as Encryption, Sobol sequence, Stripping algorithms, and Biologically inspired algorithms [13]. Re-

searchers who are working with innovative algorithms such as different machine learning algorithms or other cryptographic computations to face off the challenges are considering nature-inspired algorithms in their research. Table 2 presents different domains and factors in cloud computing and proposed mechanisms to mitigate the challenges associated with cloud security using different algorithms. This paper intends to provide an overview of the application and evaluation of bio-inspired algorithms—Evolutionary, Swarm, Immune, and Neural Network—in cloud security, taking into account published literature from 2010 to March 2020. The study outcomes expect to serve as a subsidy for current and future researchers, practitioners, and the general public to understand the overall trend, importance, and limitations of bio-inspired algorithms.

The rest of the paper is organized as follows: section II describes different bio-inspired algorithms, Section III provides an overview of past recent research trends, Section IV reviews the current work in cloud security, Section V defines the challenges, opportunities, and future research areas in the improvement of bio-inspired algorithms. Finally, Section VI draws research conclusions and future directions in cloud security.

II. BIO-INSPIRED ALGORITHMS

Living systems exist in nature, follow some systematic procedures to fulfill their needs, and it is possible to define that procedure mathematically. These procedures inspired mathematicians to develop some algorithms, and these algorithms are now known as the biologically inspired algorithm. In general, biologically inspired algorithms can be classified into four sections, such as Evolutionary algorithms, Swarm algorithms, Immune algorithms, and Neural algorithms [13].

A. EVOLUTIONARY ALGORITHMS

Evolutionary algorithms are inspired by the evolution theory, proposed by Charles Darwin [27]. It is a population-based algorithm that finds the best result using biological phenomena such as reproduction, mutation, recombination, and selection. Some prominent examples of Evolutionary algorithms are Genetic Programming (GP), Gene Expression programming (GEP), and the Strength Pareto Evolutionary Algorithm. GP mainly works by encoded computer problem solutions known as the population to gene like structure and try to find out the best by using different evolutionary techniques. The behavior of DNA-RNA replication inspires the development of GEP. It works as a genotype-phenotype system, where a genome transfers genetic information, and phenotype adapts with the environment. The application of Evolutionary algorithms as a means of cloud security can be observed in Access Control Systems [14], Protocol Network Security [15], and Trust Management [16].

B. SWARM ALGORITHMS

Some insects or animals' behavior has inspired researchers to solve many problems in science and engineering (i.e., swarms of bees, the flock of birds). Swarm Intelligence (SI), a sub-field of artificial intelligence, is inspired by biological swarms' intelligent behavior and solves real-world problems by simulating such natural actions. The algorithms are postulated from the collective knowledge, observed in nature, such as a group of birds or fish's movement or how they behave as a singular unit. It has several characteristics, such as adaption, scalability, speed, autonomy, parallelism, and fault tolerance [28]. Some well-known examples are the Ant System, Ant Colony System, and Bacterial Foraging Optimization algorithm. Ant Colony algorithm is based on ants' behaviors–randomly searching for food and finding the optimal solution to return the food to its colony; the Bees algorithm is slightly different as the search is not random in the beginning. On the other hand, Bacterial Foraging Optimization is another inspiring example of SI, where bacteria's formation based on environmental parameters were inspired to develop a sophisticated algorithm for multi-agent optimization. The implementation of Swarm algorithms in cloud security can be found in the following fields: Authentications [17], [18], Forensics [19], and Virtualizations [20].

C. IMMUNE ALGORITHMS

Immune systems of living beings become an example of sophisticated defense algorithms. For example, the human body can use its prior knowledge of harmful bacteria to prepare for future defense. The Immune algorithms are adaptive and best for developing a dynamic defense algorithm for network security and privacy. Some examples of these algorithms are the Clonal and Negative Selection, Artificial Immune Recognition, Immune Network, and Dendritic Cell algorithm. A detailed explanation regarding these algorithms can be found in [29]. The Clonal Selection algorithm is best known for optimization and in the area of pattern analysis. A Negative Selection algorithm is widely used for anomaly detection; it prepares standard and unseen features, making it better suited, especially in defense techniques where the attacker's presence is unknown. Similarly, the Dendritic Cell algorithm is another example of an Immune algorithm that works in musicale and layered. Few applications in cloud security domains that use Immune algorithms include Identity and Authentication [21], [22], Protocol and Network Security [23].

D. NEURAL ALGORITHMS

Neural algorithms are developed based on how neurons within the human brain interact with each other. Some notable Neural algorithm examples are Perceptron, Back-propagation, and Hopfield Network. The Perceptron is used as a single information organizing cell. Different neural networks are developed using Perceptron– Feed-Forward and Recurrent are some well-known examples. The Hopfield network concept was developed based on how the old memory worked with the neuron and proposed by Hopfield in 1982 [30].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

TABLE 2. Important Domain and Factors for the different class of algorithm

Class	Characteristics	Favourite Domain	Most used Algorithms	Factors
Evolutionary Algorithms	Based on reproduction, recombination etc	Optimization	Genetic	Access Control Systems [14] Protocol and Network Security [15] Trust Management [16]
Swarm Algorithms	Collective intelligence	Graph problem	Genetic Programming Ant Colony Firefly Swarm Optimization	Identity and Authentication [17], [18] Forensic Analysis [19] Virtualization [20]
Immune Algorithms	Dynamic defense adaption	Classification	Negative Selection Clonal Selection	Identity and Authentication [21], [22] Protocol and Network Security [23]
Neural Algorithms	Interconnected group of function as cell	Prediction	Convolutional Neural Network Recurrent Neural Network	Identity and Authentication [24], [25] Forensic Analysis [26]

Figure 2 demonstrates the evolution of nature-inspired algorithms over time in cloud security. Most of the research related to security in cloud computing is based on meta-heuristics, while current research emphasizes hyper-meta heuristic.

III. ANALYSIS OF RESEARCH TRENDS

To represent the extent of a literature survey of nature-inspired algorithms in cybersecurity, we developed a four step framework: (i) web-based database search and review, (ii) reference analysis, (iii) abstract probe, and (iv) entire text review. To identify the potential research paper for literature review, we used different keywords to search for articles on the online database, such as Google Scholar, the Web of Science, IEEE, and Springer. The keywords used during the screening process were cybersecurity, Evolutionary algorithm, Swarm algorithm, Immune algorithm, and Neural algorithm. Relevant published articles from 2010 to June 2020 are included in this paper, but some essential papers from different years, published before 2010 are also included due to their significant contribution to this field/scope of work. The screening process yielded more than 7000 papers related to bio inspired algorithms (among them around 1127 was related to cybersecurity). After careful review based on the number of citations, the relevance of cloud security, and publication on a reputable journal (i.e., IEEE, Springer), more than 100 papers have been taken into account in this literature. Table 3 shows the number of papers published in bio-inspired fields until 2020 on different domains.

From Table 3, it is evident that more than half of the referenced literature considered Neural Networks (NN). Swarm algorithms seemed less prevalent in security research. However, some notable and productive work were observed in the Access Control Systems (ACS) and Intrusion Detection (ID) with Swarm Intelligence (SI). Nearly half of the Immune algorithm in security research has been done in Intrusion Detection. NN dominates the chart when it comes to security sectors like Forensic areas. Table 3 also revealed that ACS and ID research is the predominant area of focus currently. Also, a decent amount of literature considered non-traditional fields like Forensics and Virtualization in their study. On the other hand, identity and authentication rely merely on traditional cryptography, where research and development focus seem minimal. And, Trust Management is relatively new, and not much progress has made over the years.

In conclusion, the utilization of bio-inspired algorithms in cloud security-related research are neck to neck for Immune and Evolutionary, Swarms are way behind, and Neural algorithms are far ahead. However, further assessment is needed to evaluate those evidence regarding security in cloud computing, which is briefly in detail in section IV.

IV. LITERATURE REVIEW

A. IDENTITY AND AUTHENTICATION SECURITY

Identity and Authentication Security (IAS) are significant concerns for cloud computing, and most IAS rely on cryptographic performances [31] or other computational complexity [32]. As shown in Figure 3, there are many layers in cloud computing and ensuring security related issues such as confidentiality, integrity, and data availability is hard to establish on each layer [24]. Bio-inspired algorithms are used by many researchers to tackle those issues. For instance, [33] presented a new security architecture for user identification that includes two-factor authentication. Their method proposed to keep login data, and encryption/decryption in one database, and rest uploaded accessories on different databases. They noted that this approach would stop any harmful or corrupted files uploaded by hackers or attackers in a cloud system.

In IAS, most security-related works have been constructed using NN algorithms, and more often applied to Keystroke and face identifications [17], [18], [24], [34]. For example, Wei et al. (2011) [19] briefly analyzed NN in password authentication systems; similarly, [35] developed password verification techniques for multi-server architecture using Neural algorithms. However, authentication research using SI did not explore that much. Still, some of the notable works that draw attention is as follows: the author(s) in [17] used Particle Swarm for palm and face identity; [18] used Immune algorithms for signature identification; [21], [22], [36], [37] developed a negative authentication system using Negative Selection algorithms. Apart from this, some studies also distilled promising results for the authentication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

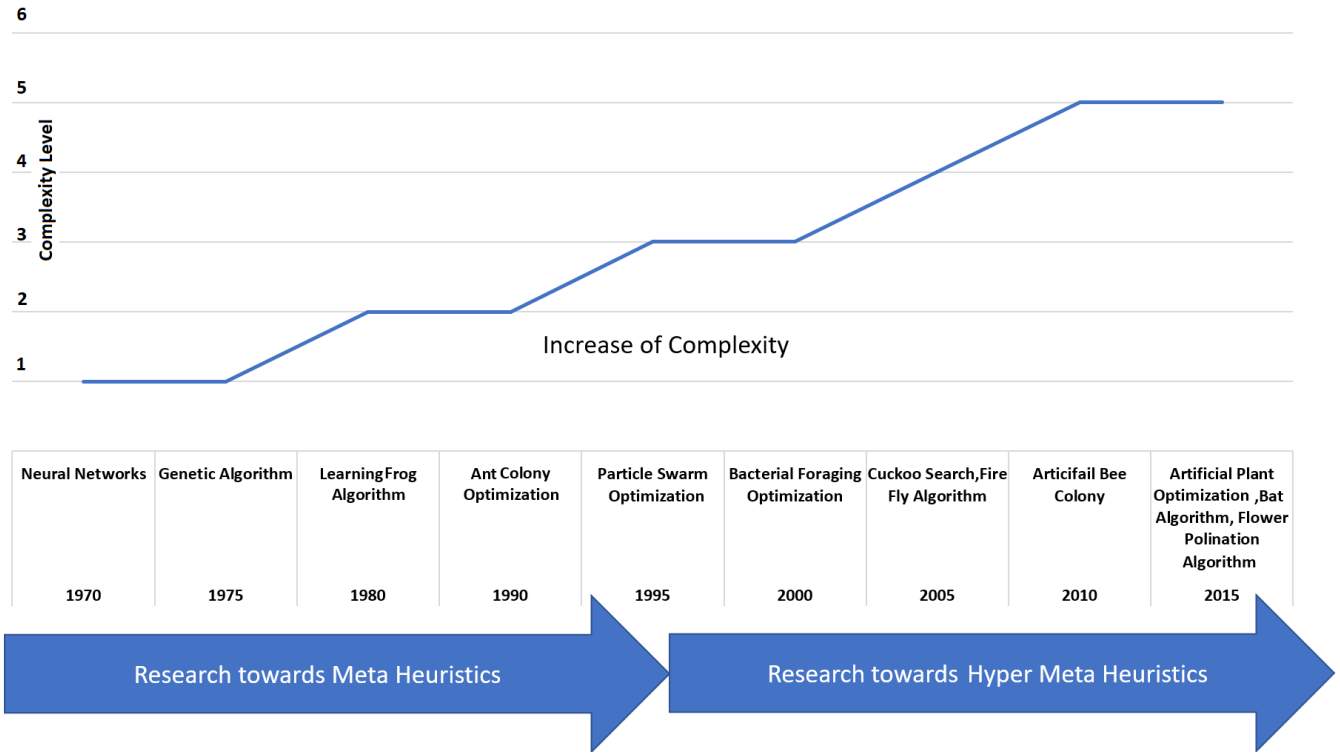

FIGURE 2. Graphical illustration of nature-inspired algorithms evolution over the time.

TABLE 3. Research papers on different cloud computing security functions

Algorithms	Identity and Authentication	Access Control Systems	Protocol and Network Security	Trust Management	Intrusion Detection Systems	Privacy	Virtualization	Forensics	Total
Evolutionary Algorithms (Genetic Algorithms,Strength Pareto Evolutionary Algorithm, etc.)	40	386	124	65	431	130	124	42	1342
Swarm Algorithms (e.g Ant colony, Bees Algorithm, etc.)	13	235	90	37	154	58	78	25	690
Immune Algorithms (e.g Clonal Selection Algorithm, Negative Selection Algorithm, Artificial Immune Recognition System, etc.)	25	160	172	24	435	140	15	35	1006
Neural Algorithms(Perceptron, Back-propagation, Hopfield Network, etc.)	106	1805	368	88	965	582	110	325	4349
Total	184	2586	754	214	1985	910	327	427	7387

process considering the GA based approach with adaptive selections [34], [38].

B. ACCESS CONTROL SYSTEMS

The Access Control Systems (ACS) are restricted to digital assets based on user privilege. In the cloud computing system, asset management and maintenance are the most vulnerable side of a security breach. Probably, the reason behind the most biology-inspired algorithms concentration on ACS. As cloud systems work with ever-expanding data growth, ACS requires to be adaptive. The adaptive nature of Evolutionary algorithms inspired security researchers to design ACS using GA. For example, Yadav et al. (2020) developed a secure ACS cloud computing, an integrated DNA Morse code-base systems considering collision, man-in-the-middle, and internal attacks [14].

Some notable works tried to use cloud users' attributes to design effective access control systems [40], [41]. Among all the nature-inspired algorithms, Swarm algorithms introduced by Di Caro et al. (1999) [42], gained much popularity for developing security in the ACS [43]–[46]. For example, A study conducted by [46] proposed the Mutual Trust-Based Access Control model (MTBAC) in cloud computing. [44] introduced SI based systems for routing in mobile net-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

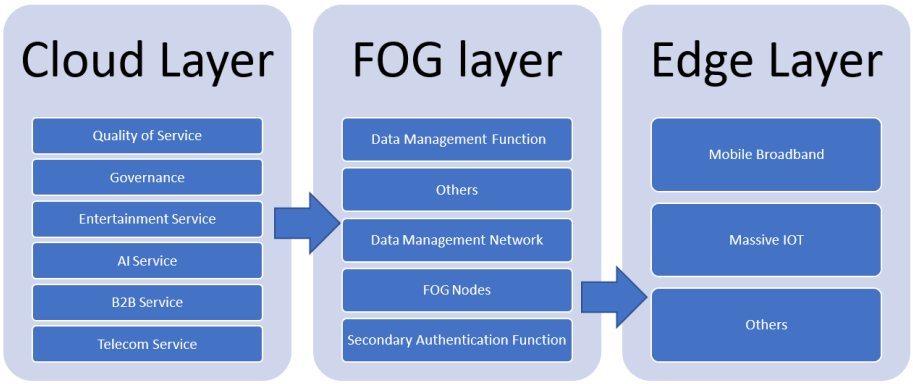

FIGURE 3. Two new network functions designed to attenuate the impact of authentication traffic, generated by secondary authentication on the 5G home network, such as Secondary Authentication Function (SAF) and Authentication Data Management Function (ADMF). Primarily, the secondary authentication operates by SAF process. The SAF gets requests from the user, processes the request, and interacts with ADMF to increase the audibility of communique environment [39].

works. [45] uses Ant Colony Clustering and Linear Genetic Programming in web-based mining.

In ACS, Immune algorithms are mostly used to solve resource allocation [47], [48] and the hierarchical key design for access control [49], [50]. Apart from this, some literature considered NN in ACS designs [51], [52]. For instance, [51] uses Feed-Forward NN; similarly, [52] uses NN to optimize resources and classify new resources for parental control systems. Figure 4 displayed an encryption-based system—the data owner provides encryption keys for the user to access stored encrypted data—in a cloud server.

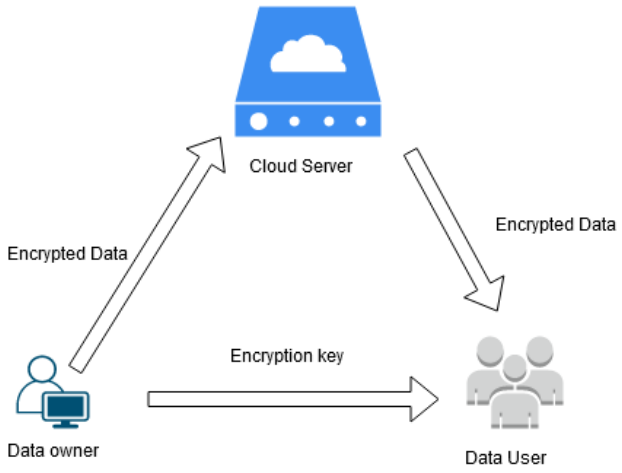

FIGURE 4. A simplified encryption based Access Control Systems.

C. PROTOCOL AND NETWORK SECURITY

Merging different layers of cloud computing requires to develop adequate Protocol and Network Security (PNS). Biology inspired algorithms are also widely used to design faster network routing and effective security protocols. For instance, [53] and [54] aims to develop wireless network routing using Evolutionary algorithms. Bashkar et al. (2014) [15] introduced a notable work by securing cluster-based data aggregation in Wireless Sensor Networks (WSN) using GA. Sing et al. (2014) [55] also developed a mobile ad-hoc network using GA.

These works inspired several researchers to design more network protocols using adaptive natures [56], [57]. Most recent works are now aiming to improve the quality service on routing protocols [23], [58], [59]. Rathee et al. (2019) [60] proposed an Ant Colony Optimization based WSN system for energy balancing in secure routing. They have considered network lifetime, QoS, and security as the primary factor during the experiment. They showed that their proposed model QEBSR performed better than the other two existing models: distributed energy balanced routing model and energy-efficient routing model. [56], [57] used the ACO to develop WSN and routing protocols, and later improved by Misra et al. (2010) [61]. In 2012, Zungeru et al. (2012) summarized all of the SI effort to develop PNS [62].

A study conducted by Mazhar et al. (2007) [23] proposed an Artificial Immune system associated with the Bee algorithm (BeeAIS) to improve Protocol and Network Security. Simultaneously, Hou et al. (2018) [58], Chhabra et al. (2018) [59] and Zhang et al. (2018) [63] worked to improve QoS for WSN. Another useful project using the Immune algorithm in the area of network security was done by Abo et al. (2015) in 2015 [64], where the Immune algorithm was applied to improve the lifetime and stability period of WSN. Meanwhile, Neural Networks (NN) algorithms are also thoroughly used in this field. NN mostly used to improve the hopping and optimizing the network route [65]–[67].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

D. TRUST MANAGEMENT

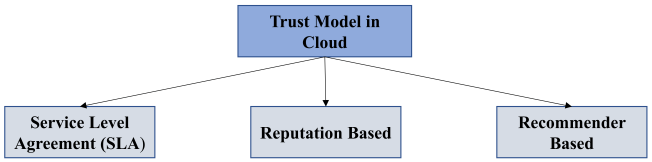

FIGURE 5. Different types of trust model in cloud security.

Trust Management (TM) is becoming more and more important as social media content starts to dominate cloud computing. Nevertheless, still, the amount of research in this field is insufficient. Service level agreement, recommender, and reputation-based models are some of the trust models in cloud security, as shown in Figure 5. Several studies stated promising results in the last few years by using Evolutionary and Immune algorithms in cloud computing [16], [68], [69]. Tahta et al. (2015) [16] developed a peer to peer systems for TM using GA. Tau et al. (2006) [68] improved trustworthiness using Immune algorithms (IA); it inspires more researchers to use IA in Trust Management [69] [70].

[71] introduced an anti-attack TM scheme for the Vehicular Ad-hoc network, an example of adaptive forgetting element-based strategies that develop trustworthy VAN networks by avoiding malicious vehicles and assisting with trusted vehicles. [72] proposed an optimized trust-aware recommender system using GA. In this paper, the author developed a model for choosing the most suitable nodes for the skeleton of recommender searching. Using this method, they were able to reduce the skeleton's maintenance cost more than 90%. On the other hand, the NN is also used to develop a trust model. However, most of its notable works are regarded to classify or optimize data/networks' reputations. For example, [73] developed a distributed network systems, which later proved helpful in cloud computing [74]. Even though the NN-based approach is used extensively in cloud computing due to its advantage in trust management, the NN models have some disadvantages: lower accuracy [75], unable to handle local optimal and convergence [76] problems, and fail to process multi-class attacks [77]. Therefore, continuous evolution is required.

E. INTRUSION DETECTION

Intrusion Detection (ID), one of the most researched topics in cyber-attack, is divided into three categories—Specification-based, Anomaly-based, and Signature-based—as shown in Figure 6. Some bio-inspired algorithms, such as Immune and Neural algorithms, are proven to be useful to detect intrusion due to their optimized classification techniques. [78] describes the application of Immune-based algorithms in ID systems; [79] presents a case study to tailor the bio-inspired algorithm for ID. On the other hand, Wang et al. (2018) [80] proposed an improved Immune algorithm for industrial cloud storage. Alaparthy et al. (2018) [81] analyzed a multi-level ID system based on the Immune algorithm.

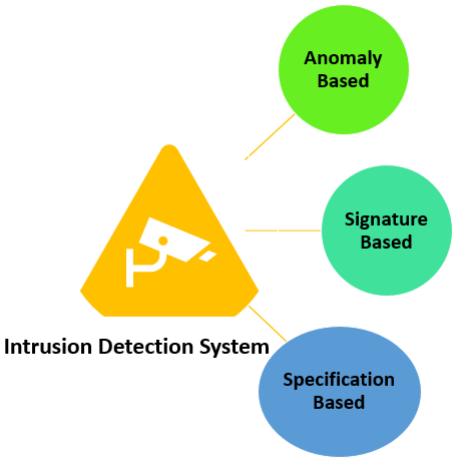

FIGURE 6. Different types of Intrusion detection.

Many studies address the application of ANN in ID. For example, Tran et al. [82] Proposed ANN-based adaptive boosting and probabilistic methods; Alarcon et al. [83] introduced Adopted Recurrent Neural Networks for low false alerts and better accuracy. However, one of the most significant drawbacks of their proposed method is that it requires high processing power and is also unable to detect insider attacks.

Some researchers also attempt to use the Genetic Algorithm (GA), but it was found that Immune algorithms were more effective than GA to Intrusion Detection [84]–[86]. Nonetheless, several studies have used the Neural net over the years [87]–[89]. For instance, in 2018, [89] developed a Genetic tree-based rule induction for network ID systems; Deshai et al. (2016) [90] introduced a Fuzzy Logic-based algorithm, known as Fuzzy-GA ID. The paper [91] adopted a short-term memory system with a RNN for Intrusion Detection and Tang et al. (2018) [88] tested SDN with RNN for Intrusion Detection.

F. PRIVACY

Previously, Privacy issues were categorized as Identity and Authentication issues or a matter of ACS and managed by Access Control. As the internet age grows, Privacy issues become more complicated and contemplated as an individual pivotal threat in cloud computing. Several techniques were proposed to tackle those threats, using the nature-inspired algorithm (i.e., Neural Network, Evolution, and Immune); for instance, Yuan et al. (2014) introduced an NN-based algorithm using back-propagation for preserving privacy in cloud computing [92]. Said et al. (2018) developed a Clustering Coefficient based Genetic Algorithm (CC-GA) for detecting communities in social networks [93].

As social networks' applications are continuously grow-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

ing, it becomes necessary to analyze the network communities' structure and their potential features in terms of privacy concerns. Besides, large scale social networks also need excessive storage space, which leads to high computation cost. Considering the risk of social user privacy leakage in the clustering process, Bian et al. (2019) proposed a Markov Clustering algorithm (DP-MCL) with different privacy premise [94]. The algorithm (DP-MCL) stores the social network as an input in the adjacency matrix. It compresses the network sizes to minimize the network scale based on different privacy and guaranteed accurate clustering; however, they did not consider reducing that vast social network in an efficient and timely manner during the study.

When the data set becomes more abundant, it is common for users to store their data in a cloud more often. However, to ensure better security, data stored as an encrypted form. However, if those data have multiple owners, then problem raises as it becomes difficult to store as an encrypted form due to the different keys while it is also necessary to keep the communication cost minimum for the user's satisfaction. Resolving those issues, Li et al. (2017) [95] proposed a deep learning approach for multi-key privacy-preserving in cloud computing. The algorithm combines double decryption and Fully Homomorphic Encryption (FHE) to improve the communication facility and minimum cost. However, they did not test their model performance in a real-world scenario; also, the cost reduction was not significant.

G. VIRTUALIZATION

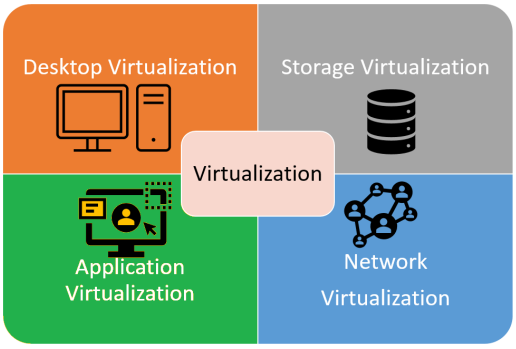

FIGURE 7. Different facility of Virtualization in Cloud systems.

Virtualization is a system that supports distributing an individual physical instance of an asset or an application between many consumers. Different digital technology, such as desktop, storage, and application, can be virtualized through cloud systems as shown Figure 7. Most of the cloud Virtualization problem is resource allocation problem, also known as NP-Hard; and, finding exact solutions is complicated for large scale data [96]. In virtual security, the most widely used biological inspired algorithm is the Evolutionary algorithm. Tang et al. (2015) [97] developed an energy-efficient virtual machine for data centers. Khan et al. (2016) [98] used a GA to give a solution for in-network sensor data annotation in virtualized WSN. Additionally, Lee et al. (2017) [99] also worked with Virtualization to improve cluster performance using a GA. Weng et al. (2018) [80] proposed a PSO based framework to solve the VMP problem by extending original PSO to discrete searching space. [100] proposed an energy efficient algorithm using a heuristic algorithm, called MinPR for virtual machine placement optimization (considered power consumption and resource efficiency). Using MinPR, authors were able to prioritize the power efficient ones over all the active physical machines, to reduce resource wastage by maximizing and balancing resource utilization. However, they did not consider the dependency between VMs and the data center network topology.

[101] proposed an Ant Colony Optimization (ACO) heuristic algorithm to host the VMs into PMs. They performed a local search with ACO that significantly improved the solution by minimizing the number of PMs. Cao (2019) [102] proposed a multi-objective GA. Their goal was to minimize energy consumption and communication traffic, which caused performance bottlenecks. In addition, Usman (2019) [96] proposed a new approach to reduce resource wastage and increase energy efficiency for VM allocation using Flower Pollination in the cloud data-center. The distribution employs a strategy called Dynamic Switching Probability (DSP). Using DSP frameworks, they were able to find the optimal solution quickly and balance the exploration of the global search and the local search. Their proposed method outperformed Genetic-Algorithms for Power-Aware (GAPA) by 21.8%, the Order of Exchange Migration (OEM) Ant Colony system by 21.5%, and First-Fit Decreasing (FFD) by 24.9%. However, their proposed method did not consider the multi-objective approach of E-FPA to consolidate the data center resource, which may need to be investigated. Also, the optimal solution is not highly scalable. Besides, Khurana and Singh (2019) [103] also uses FPA based algorithms along with GWO to improve VM efficiency. To conduct the experiment, they have considered the following parameters: the number of tasks, the number of workflows, the number of VM, the MIPS, and the number of processors. However, their method has a high computational cost.

The author in [104] proposed a method for VM placement by OH-BAC algorithm. They have considered the following parameters for their study: load balance, CPU utilization, memory, bandwidth, storage size, and memory. Using OH-BAC techniques, they were able to find the optimal PM with the least power consumption. However, their proposed method needs more Service Level Agreement (SLA) time per Active Host (SLATAH).

Another study conducted by Liu et al. [105] formulated VMP with a reliability model and analyzed its complexity with an approximation algorithm. Their proposed model proved to be effective and efficient in solving traffic-aware and reliability guaranteed VMP problems. However, they did not consider some VM related challenges such as VM backups or VM migration during their experiment. Verma et al. (2018) [106] studied the influence of five different

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3027841, IEEE Access

parameters to develop an optimized virtual machine. The examined factors were broker cost, time duration, bandwidth, ram speed, and overall cost. The authors used the Honey Bee approaches for balancing load across the virtual machines and were able to maximize the throughput. However, during this experiment, some of the essential factors, such as server CPU power and memory, which also plays a vital role in VM efficiency, were not considered.

Many past recent studies considered data security as the most significant security challenge in cloud computing. [107] proposed a Firefly Swarm approach for developing new connections in social networks based on big data analysis. [20] offered Bacterial Foraging to prevent security threats on the flow of big-data information. [108] developed a novel hybrid bio-inspired algorithm using a Multilayer Perceptron (MLP) to handle big data security. However, even with significant advantages, bio-inspired algorithms (such as Bacterial Foraging, Swarm approach, and MLP) are often not suitable for scalability– vulnerable considering fault tolerance, and agility.

H. FORENSICS

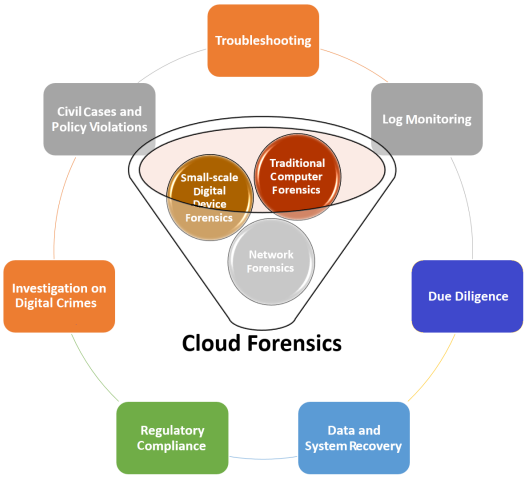

FIGURE 8. Illustration of cloud Forensics and the usage area in security.

Cloud Forensics is the combination of traditional computer Forensics, small-scale digital device Forensics, and network Forensics. Cloud Forensics usage includes troubleshooting, log monitoring, due diligence, data, and system—recovery, regulatory compliance, investigation on digital crimes, civil cases, and policy violations as illustrated in Figure 8. Cloud Forensics becomes popular in law enforcement in order to understand and track criminal activity by gathering information from digital devices like smartphones, computers, and smart sensors. Over the years, biology-inspired algorithms have not been explored much in this field. Additionally, no specific or substantial techniques have been developed to serve as a guide for cloud technology. Therefore, current tools and techniques are insufficient to succeed in proper Forensics reports due to the lack of adequate training and compatibility issues [3]. Mukkamala et al. (2003) [26] proposed a Neural Network approach to identify the significant features for network Forensics analysis.

Many security challenges associated with cloud Forensics includes false alert and unanimous attack in the systems. To deal with these issues, more often, the bio-inspired based approach is utilized. For example, [109] proposed an NN based technique; [110] suggested a combined kernel PCA and GA to reduce training time and [111] developed a fuzzy logic and ANN-based techniques for anomaly detection.

Forensics identification can be classified as fingerprint, facial recognition, log analysis, and user data analysis. Law enforcement agencies more often use facial recognition techniques to identify person or crime investigation [112]. While using existing algorithms, it is possible to achieve up to 100% accuracy; for Forensics identification, it is not that easy. The challenges faced by this discipline consist of several factors, and among them, the quality of the image itself is the biggest problem. For example, most of the CCTV's digital video recorder (DVR) is normally kept at resolution 720 pixel wide with H.264 compression. After some time, the video resolution was sampled at a smaller size to accommodate more recording space. Beyond that, signal noise, color noise, illumination problems also cause many dead ends to Forensics analysis. To deal with these issues, several studies have proposed a solution, based on a bio-inspired algorithm [19], [112], [113]. [19] proposed Particle Swarm Optimization (PSO) method associated with Support Vector Machine (SVM), named by PSO-SVM for facial recognition in cloud forensic. Even though proposed PSO-SVM methods hypothesized good accuracy, the performance deteriorated with random values while velocity is calculated. To overcome that issue, [112] proposed a modified feature extraction method named as AAPSO-SVM. Here, researchers showed that their proposed method performed better than traditional bio-inspired algorithms such as ABC, PSO, and PSO-SVM, and achieved up to 85% accuracy. Another study conducted by [113] compares three existing techniques proposed by the previous work, such as PSO-SVM, AAPSO-SVM, and OPSO-SVM [19], [112]. Their result illustrated that AAPSO-SVM performed better compared to other algorithms. Even though authors in [113] found AAPSO-SVM as the best algorithm compared to the other two, [114] suggested that PSO-SVM based method should be used in classification stage- as it performed better than other algorithms when using with AAM (feature extraction techniques).

Most of the cloud Forensics relates to virtual evidence like facial recognition. However, fingerprint is also considered as cloud Forensics, even though it is physical evidence. We did not consider fingerprints as cloud security related issues during this literature. However, in fingerprint detection, several studies showed promising results using bio-inspired algorithms. For example, [115], achieved 90% accuracy using PSO-SVM.

Still, cloud Forensics faces several issues such as tenancy, integrity, privacy, and Encryption. Addressing those issues,

Pandi et al. (2020) found the lacking of advanced tools as the main culprit behind the progress of Forensics analysis in the current environment. [116]. On the other hand, existing techniques fail to reduce leaking confidential information—documents, images, and videos—of victims from end devices like smartphones and tabs [117]. Several studies often suggest difficulty accessing the evidence using logs as another hinder in cloud Forensics investigation [118], [119]. [120] argued that the problem could be solved if logs through the eucalyptus cloud environment. In general, issues, like data fragment [119], lack of trust issues [121], and cloud infrastructure isolation [4], are still some of the challenges faced by cloud Forensics till days. However, the typical limitations of all nature-inspired algorithms have to deal with time complexity issues [109]–[111]. Additional challenges associated with cloud Forensics are the unification of log formats, synchronization of timestamps, the exponential increase of digital devices accessing the cloud, and ineffective encryption key management [122]

Table 4 lists a list of papers organized primarily based on the problem domain, security function, algorithm, and application. Most of the articles published between 2018 to 2020 were presented along with previous literature, and interested readers are recommended for further assessment based on their needs.

V. DISCUSSION AND POTENTIAL REMARKS

Based on the presented literature of security on cloud computing, this segment describes the general findings of the existing research and the future direction of cloud computing studies considering nature-inspired algorithms.

Most of the papers prioritize the following elements in their experiments: task scheduling [96], [123], [124], biometric identification [112], [125], network optimization [60], [126]–[129], and network stability [123], [130], [131]. ACO may be very promising when implemented to single-goal optimization, even though more common GA have somewhat overtaken. A few efforts have been made to regulate ACO to a multi-objective paradigm, which is an exciting avenue; this is perhaps deserve further study. In combination with optimization objective capabilities, the possibility of metaheuristics might also improve network performance and require additional attention.

The lack of proper security, cloud computing is accessible for hackers/attackers to misuse this platform. Moreover, a model developed with existing algorithms such as Fuzzy Logic, Swarm Intelligence, and Neural Network is still unable to secure the network entirely. Additionally, with big data, it is becoming difficult for the traditional algorithm to extract features, especially in cloud Forensics, or to optimize the model, mostly for customer satisfaction. Thus, it is necessary to introduce a more sophisticated and advanced strategy to develop a secure network. Compared to the traditional approach, sophisticated algorithms, like deep learning, ANN, or CNN based methods, gained lots of popularity because of their better accuracy on large datasets. As a result, recently, researchers are using a deep learning-based approach constantly to address cybersecurity issues. However, one of the significant drawbacks of those algorithms is that they are time-consuming and need to find a better way to handle the time complexity issues. Additionally, researchers may also consider optimizing the routing time, authentication time, and network cost for further study.

VI. CONCLUSION

In conclusion, this research survey provided a comprehensive analysis of the latest research techniques and algorithms related to biologically inspired algorithms used in cloud computing. The referenced literature mainly focused on two bio-inspired algorithms: PSO and NN approach to tackling maximum cloud computing security-related problems. Additionally, Algorithms like the Ant Colony, Fruitfly, and Grasshopper drew interest to decipher specific issues among researchers. However, some of the studies also developed a secured network system using the GA method. Most of the results were simulation-based and did not integrate with another matching, learning, forecasting models; therefore, a potential future application might be interesting considering multi-objective optimization using GA based approach. Finally, we would like to suggest some of the possible scopes, shortly for researcher and practitioner as a brainstorming concept: reducing the reaction time and maximizing VM's resource allocation considering the QoS factor; improving the load stability in WSN using RCNN learning; SVM-PSO based community Forensics and RNN techniques for Intrusion Detection.

TABLE 4: Literature emphasized on cybersecurity. ACS– Access Control Systems; ID– Intrusion Detection; NF– Network Forensics; PNS– Protocol and Network Security; IA– Identity and Authentication; TM– Trust Management; VR– Virtualization; P– Privacy; PSO– Particle Swarm Optimization; CNN– Convolutional Neural Network; GA– Genetic Algorithm; ANN– Artificial Neural Network; DL– Deep Learning; VAN– Vehicle Ad-hoc Network; WSN– Wireless Sensor Network; DNN– Deep Neural Network; SI– Swarm Intelligence; NN– Neural Network.

Reference	Problem Domain	Security Function	Algorithm	Application
Al Zoubi et al. [123]	Task Scheduling	ACS	Grasshopper optimization	Reduce makespan upto 10%
Daweri et al. [132]	Optimization	ACS	Cuttlefish algorithm	Continuous optimization
Suarez et al. [79]	Anomaly detection	ID	Multiple algorithm	Feature selection from natural algorithm
Koroniotis et al. [133]	Quality of service	NF	PSO and DL	Enhance NF
Al hawaitat et al. [134]	WS	PNS	PSO	Jamming attack
Shi et al. [135]	Anomaly detection	P	ADAID[1]	Presented unsupervised clustering
Usman et al [96]	VM allocation	VR	EFPA[2]	Energy-oriented allocation
Singh et al [103]	VM migration	VR	HBGA[3]	Energy reduction
Naik et al. [130]	VM allocation	VR	Fruit fly	Reduce host migration
Meng & Pan [136]	Optimization	VR	FFOA	solve MKP[4]
Mosa & Paton [126]	VM placement	VR	GA	Reduce response time & maximize resources utilization
Duan et al. [137]	Information leakage	P	DL	Protect server
Festag & Spreckelsen [138]	Data leakage	P	DL	Detection of protected health information
Chari et al. [125]	Quality of service	IA	DL	Generate password via cognitive information
Li et al. [139]	Signal processing	IA	GA	Feature extraction via EEG signal
Saini & Kansal [127]	WSN	ACS	SI	Reduce energy consumption and increase network life time
Chen et al. [140]	Biometric identification	IA	CNN	Proposed GSLT-CNN using human brain EEG
Cao & Fang [141]	Multilayer defense scenario	ACS	SI	Found proficient IPSO elucidating extensive WTA problem
Aliyu et al. [124]	Resource allocation	ACS	Ant colony	Illustrated faster convergence optimize makespan time
Poonia [142]	VAN	ACS	SI	Found significant difference in VANET routing protocol and Swarm based protocol
Verma et al. [128]	WSN	PNS	GA	Reduce cluster head selection
Harizan & Kuila [143]	WSN	PNS	PSO,DE,GA, and GSA	Found GA and GSO performed better
Sampathkumar et al. [131]	WSN	PNS	Glowworm SI	Improve load balancing and routing strategies in WSN
Sahu & Saho [144]	WSN	PNS	SI	Robotics WSN
Vijayan & Rubasundram [145]	Fraud prediction	TM	ANN	Predict fraudulent in financial reporting
Eziama et al. [146]	VAN	TM	DNN	Detect malicious node efficiently
Rathee et al. [60]	WSN	PNS	Ant colony	Optimized network life time, QoS, and security

[1]Artificial Immune network and Density peak
[2]Energy-oriented Flower Pollination
[3]Hypercube based Genetic Algorithm
[4]multidimensional knapsack problem

TABLE 4: Cont.

Reference	Problem Domain	Security Function	Algorithm	Application
Aslan & Sen [147]	VAN	TM	GA	Improve the security of the network
Ghosh et al. [129]	Feature extraction	ID	GA	Reduce features to classify network packet
Tan et al. [148]	Real time network attack intrusion	ID	NN	Able to detect in network precisely
Haider et al. [149]	DDos Attack detection	ID	Deep CNN	Improve accuracy and reduce time complexity
Tang et al. [150]	Web attacks through encoder-decoder	ID	RNN	signature-based WAFs with RNN
Li et al. [24]	Keystroke analysis	IA	GA	Identity based cloud computing
Yu & Cho [25]	Keystroke analysis	IA	GA-SVM	Feature selection
Nag et al. [38]	Adaptive selection	IA	GA	Multi-factor authentication
Gupta et al. [151]	Image processing	IA	GA	Detect adversarial attacks
Dasgupta et al. [34]	Adaptive selection	IA	GA	Selection techniques for multi-factor authentication
Raghavendra et al. [17]	Palm and face recognition	IA	SI	Multi-sensor bio-metric analysis
Conti et al. [18]	Image processing	IA	Immune	Ink-on-paper fingerprints identification
Sen et al. [152]	Power distribution	VR	GA	Optimize dispatching for micro-grid energy
Yeom et al. [153], Kitchens et al. [154]	Face& Keystroke analysis	IA	NN	Person authentication using NN
Ku [155]	Keystroke analysis	IA	NN	Password authentication for multi-server architecture
Gai et al. [40]	Adaptive access	ACS	GA	Allocate multimedia data in diverse memory
Ye et al. [41]	Adaptive access	ACS	GA	QoS-aware service
Hartman et al. [42]	Scalable storage	ACS	Immune	Cost-effective storage systems
Lin et al. [46]	Trust based	ACS	Immune	A mutual trust based ACS
Tzeng [50]	Hierarchical key	ACS	Immune	Time-bound cryptographic scheme
Sen et al. [156]	DDoS attack detection	PNS	NN	Identify incoming DDoS type traffic attack

REFERENCES

[1] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure User Data in Cloud Computing Using Encryption Algorithms," International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013.

[2] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud Computing System Based on Trusted Computing Platform," in 2010 International Conference on Intelligent Computation Technology and Automation, vol. 1, pp. 942–945, IEEE, 2010.

[3] W. Yassin, M. F. Abdollah, R. Ahmad, Z. Yunos, and A. Ariffin, "Cloud Forensic Challenges and Recommendations: A Review," OIC-CERT Journal of Cyber Security, vol. 2, no. 1, pp. 19–29, 2020.

[4] W. Delport et al., Forensic Evidence Isolation in Clouds. PhD thesis, University of Pretoria, 2014.

[5] V. Roussev, I. Ahmed, A. Barreto, S. McCulley, and V. Shanmughan, "Cloud Forensics–Tool Development Studies & Future Outlook," Digital Investigation, vol. 18, pp. 79–95, 2016.

[6] S. Process and F. Release, "Synopsys Inc," 2018.

[7] H. S. Chen and J. Fiscus, "The Inhospitable Vulnerability," Journal of Hospitality and Tourism Technology, 2018.

[8] S. Atouati, X. Lu, and M. Sozio, "Negative Purchase Intent Identification in Twitter," in Proceedings of The Web Conference 2020, pp. 2796–2802, 2020.

[9] T. Lu, X. Guo, B. Xu, L. Zhao, Y. Peng, and H. Yang, "Next Big Thing in Big data: The Security of the ICT Supply Chain," in 2013 International Conference on Social Computing, pp. 1066–1073, Sep. 2013.

[10] S. Kim, N. Kim, and T. Chung, "Attribute Relationship Evaluation Methodology for Big Data Security," in 2013 International Conference on IT Convergence and Security (ICITCS), pp. 1–4, Dec 2013.

[11] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.

[12] L. M. Vaquero and L. Rodero-Merino, "Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing," SIGCOMM Comput. Commun. Rev., vol. 44, pp. 27–32, Oct. 2014.

[13] J. Brownlee, Clever Algorithms: Nature-Inspired Programming Recipes. Jason Brownlee, 2011.

[14] M. Yadav and M. Breja, "Secure DNA and Morse Code Based Profile Access Control Models for Cloud Computing Environment," Procedia Computer Science, vol. 167, pp. 2590–2598, 2020.

[15] L. Bhasker, "Genetically Derived Secure Cluster-Based Data Aggregation in Wireless Sensor Networks," IET Information Security, vol. 8, no. 1, pp. 1–7, 2014.

[16] U. E. Tahta, S. Sen, and A. B. Can, "GenTrust: A Genetic Trust Management Model for Peer-to-Peer Systems," Applied Soft Computing, vol. 34, pp. 693–704, 2015.

[17] R. Raghavendra, A. Rao, and G. Hemantha Kumar, "Multisensor Biometric Evidence Fusion of Face and Palmprint for Person Authentication Using Particle Swarm Optimisation (PSO)," International Journal of Biometrics, vol. 2, no. 1, p. 19, 2010.

[18] V. Conti, G. Pilato, S. Vitabile, and F. Sorbello, "Verification of Ink-on-Paper Fingerprints by Using Image Processing Techniques and a New Matching Operator," Proc. of VIII Convegno AI* IA, 2002.

[19] J. Wei, Z. Jian-Qi, and Z. Xiang, "Face Recognition Method Based on Support Vector Machine and Particle Swarm Optimization," Expert Systems with Applications, vol. 38, no. 4, pp. 4390–4393, 2011.

[20] K. Ahmad, G. Kumar, A. Wahid, and M. M. Kirmani, "Intrusion Detection and Prevention on Flow of Big Data using Bacterial Foraging," in Handbook of Research on Securing Cloud-Based Databases with Biometric Applications, pp. 386–411, IGI Global, 2015.

[21] D. Dasgupta and R. Azeem, "An Investigation of Negative Authentication Systems," in Proceedings of 3rd International Conference on Information Warfare and Security, pp. 117–126, 2008.

[22] D. Dasgupta, D. Ferebee, S. Saha, A. K. Nag, K. P. Subedi, A. Madero, A. Sanchez, and J. Williams, "G-nas: A Grid-Based Approach for Negative Authentication," in 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), pp. 1–10, IEEE, 2014.

[23] N. Mazhar and M. Farooq, "BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc," in Artificial Immune Systems, pp. 370–381, Springer, 2007.

[24] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," in IEEE International Conference on Cloud Computing, pp. 157–166, Springer, 2009.

[25] E. Yu and S. Cho, "GA-SVM Wrapper Approach for Feature Subset Selection in Keystroke Dynamics Identity Verification," in Neural Networks, 2003. Proceedings of the International Joint Conference on, vol. 3, pp. 2253–2257, IEEE, 2003.

[26] S. Mukkamala and A. H. Sung, "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques," International Journal of Digital Evidence, vol. 1, no. 4, pp. 1–17, 2003.

[27] C. Darwin, The Origin of Species. PF Collier & son New York, 1909.

[28] E. Bonabeau, M. Dorigo, D. d. R. D. F. Marco, G. Theraulaz, G. Théraulaz, et al., Swarm Intelligence: from Natural to Artificial Systems. No. 1, Oxford University Press, 1999.

[29] D. Dasgupta, An Overview of Artificial Immune Systems and Their Applications, pp. 3–21. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999.

[30] J. J. Hopfield, "Neural Networks and Physical Systems with Emergent Collective Computational Abilities," Proceedings of the National Academy of Sciences, vol. 79, no. 8, pp. 2554–2558, 1982.

[31] D. Dasgupta, A. Roy, and A. Nag, Advances in User Authentication. Springer, 2017.

[32] K. D. Gupta, M. L. Rahman, D. Dasgupta, and S. Poudyal, "Shamir's Secret Sharing for Authentication without Reconstructing Password," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0958–0963, IEEE, 2020.

[33] S. Kumar, S. A. A. Jafri, N. Nigam, N. Gupta, G. Gupta, and S. Singh, "A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing," in IOP Conference Series: Materials Science and Engineering, vol. 748, p. 012026, IOP Publishing Ltd., 2020.

[34] D. Dasgupta, A. Roy, and A. Nag, "Toward the Design of Adaptive Selection Strategies for Multi-factor Authentication," computers & security, vol. 63, pp. 85–116, 2016.

[35] L.-H. Li, L.-C. Lin, and M.-S. Hwang, "A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks," IEEE Transactions on Neural Networks, vol. 12, no. 6, pp. 1498–1504, 2001.

[36] D. Dasgupta, A. Roy, and A. Nag, "Negative Authentication Systems," in Advances in User Authentication, pp. 85–145, Springer, 2017.

[37] D. Dasgupta, A. K. Nag, D. Ferebee, S. K. Saha, K. P. Subedi, A. Roy, A. Madero, A. Sanchez, and J. R. Williams, "Design and Implementation of Negative Authentication System," International Journal of Information Security, vol. 18, no. 1, pp. 23–48, 2019.

[38] A. K. Nag, D. Dasgupta, and K. Deb, "An Adaptive Approach for Active Multi-Factor Authentication," in 9th annual symposium on information assurance (ASIA14), p. 39, 2014.

[39] S. Gong, A. El Azzaoui, J. Cha, and J. H. Park, "Secure Secondary Authentication Framework for Efficient Mutual Authentication on a 5G Data Network," Applied Sciences, vol. 10, no. 2, p. 727, 2020.

[40] K. Gai, M. Qiu, and H. Zhao, "Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing," IEEE Transactions on Cloud Computing, 2016.

[41] Z. Ye, X. Zhou, and A. Bouguettaya, "Genetic Algorithm Based QoS-Aware Service Compositions in Cloud Computing," in International Conference on Database Systems for Advanced Applications, pp. 321–334, Springer, 2011.

[42] J. H. Hartman, I. Murdock, and T. Spalink, "The Swarm Scalable Storage System," in Distributed Computing Systems, 1999. Proceedings. 19th IEEE International Conference on, pp. 74–81, IEEE, 1999.

[43] M. Dorigo, M. Birattari, et al., "Swarm Intelligence," Scholarpedia, vol. 2, no. 9, p. 1462, 2007.

[44] G. Di Caro, F. Ducatelle, and L. M. Gambardella, "Swarm Intelligence for Routing in Mobile Ad Hoc Networks.," in SIS, pp. 76–83, 2005.

[45] A. Abraham and V. Ramos, "Web Usage Mining Using Artificial Ant Colony Clustering and Linear Genetic Programming," in Evolutionary Computation, 2003. CEC'03. The 2003 Congress on, vol. 2, pp. 1384–1391, IEEE, 2003.

[46] G. Lin, D. Wang, Y. Bie, and M. Lei, "MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing," China Communications, vol. 11, no. 4, pp. 154–162, 2014.

[47] Z.-J. Lee and C.-Y. Lee, "A Hybrid Search Algorithm with Heuristics for Resource Allocation Problem," Information Sciences, vol. 173, no. 1-3, pp. 155–167, 2005.

[48] K. Mori, M. Tsukiyama, and T. Fukuda, "Immune Algorithm with Searching Diversity and its Application to Resource Allocation Problem," IEEJ Transactions on Electronics, Information and Systems, vol. 113, no. 10, pp. 872–878, 1993.

[49] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks," Wireless Networks, vol. 12, no. 1, pp. 63–78, 2006.

[50] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering, vol. 14, no. 1, pp. 182–188, 2002.

[51] T. W. Chow and Y. Fang, "A Recurrent Neural-Network-Based Real-Time Learning Control Strategy Applying to Nonlinear Systems with Unknown Dynamics," IEEE Transactions on Industrial Electronics, vol. 45, no. 1, pp. 151–161, 1998.

[52] N. Dimitrova and R. Jasinschi, "System for Parental Control in Video Programs Based on Multimedia Content Information," Feb. 3 2015. US Patent 8,949,878.

[53] M. Adnan, M. Razzaque, I. Ahmed, and I. Isnin, "Bio-Mimic Optimization Strategies in Wireless Sensor Networks: A Survey," Sensors, vol. 14, no. 1, pp. 299–345, 2014.

[54] K. Biswas, V. Muthukkumarasamy, and K. Singh, "An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks," IEEE Sensors Journal, vol. 15, no. 5, pp. 2801–2809, 2015.

[55] R. Singh, P. Singh, and M. Duhan, "An Effective Implementation of Security Based Algorithmic Approach in Mobile Adhoc Networks," Human-Centric Computing and Information Sciences, vol. 4, no. 1, p. 7, 2014.

[56] S. K. Dhurandher, S. Misra, M. S. Obaidat, and N. Gupta, "An Ant Colony Optimization Approach for Reputation and Quality-of-Service-Based Security in Wireless Sensor Networks," Security and Communication Networks, vol. 2, no. 2, pp. 215–224, 2009.

[57] M. Farooq and G. A. Di Caro, "Routing Protocols for Next-Generation Networks Inspired by Collective Behaviors of Insect Societies: An Overview," in Swarm Intelligence, pp. 101–160, Springer, 2008.

[58] R. Hou, L. Zhang, Y. Zheng, Y. Chang, B. Li, T. Huang, and J. Luo, "Service-Differentiated QoS Routing Based on Ant Colony Optimisation for Named Data Networking," Peer-to-Peer Networking and Applications, pp. 1–11, 2018.

[59] G. S. Chhabra, G. Verma, and P. S. Patheja, "Efficient Fuzzy Ant Colony-Based Multipath QoS Aware Routing Protocol in Mobile Ad Hoc Network," International Journal of Mobile Network Design and Innovation, vol. 8, no. 4, pp. 225–234, 2018.

[60] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," IEEE Transactions on Engineering Management, 2019.

[61] S. Misra, S. K. Dhurandher, M. S. Obaidat, P. Gupta, K. Verma, and P. Narula, "An Ant Swarm-Inspired Energy-Aware Routing Protocol for Wireless Ad-hoc Networks," Journal of systems and software, vol. 83, no. 11, pp. 2188–2199, 2010.

[62] A. M. Zungeru, L.-M. Ang, and K. P. Seng, "Classical and Swarm Intelligence Based Routing Protocols for Wireless Sensor Networks: A Survey and Comparison," Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1508–1536, 2012.

[63] H. Zhang, A. Bochem, X. Sun, and D. Hogrefe, "A Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization Routing in Vehicular Ad hoc Networks," in 2018 IEEE Intelligent Vehicles Symposium (IV), pp. 1071–1078, IEEE, 2018.

[64] M. Abo-Zahhad, S. M. Ahmed, N. Sabor, and S. Sasaki, "Mobile Sink-Based Adaptive Immune Energy-Efficient Clustering Protocol for Improving the Lifetime and Stability Period of Wireless Sensor Networks," IEEE Sensors Journal, vol. 15, no. 8, pp. 4576–4586, 2015.

[65] J. A. Boyan and M. L. Littman, "Packet Routing in Dynamically Changing Networks: A Reinforcement Learning Approach," in Advances in Neural Information Processing Systems, pp. 671–678, 1994.

[66] H. E. Rauch and T. Winarske, "Neural Networks for Routing Communication Traffic," IEEE Control Systems Magazine, vol. 8, no. 2, pp. 26–31, 1988.

[67] M. K. M. Ali and F. Kamoun, "Neural Networks for Shortest Path Computation and Routing in Computer Networks," IEEE Transactions on Neural Networks, vol. 4, no. 6, pp. 941–954, 1993.

[68] L. Tao, "An Immune Based Model for Network Monitoring," Chinese Journal of Computers, vol. 9, p. 001, 2006.

[69] M. Firdhous, O. Ghazali, and S. Hassan, "Trust Management in Cloud Computing: A Critical Review," ArXiv Preprint ArXiv:1211.3979, 2012.

[70] K. D. Gupta, D. Dasgupta, and S. Sen, "Smart Crowdsourcing Based Content Review System (SCCRS): An Approach to Improve Trustworthiness of Online Contents," in International Conference on Computational Social Networks, pp. 523–535, Springer, 2018.

[71] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," IEEE Access, vol. 8, pp. 21077–21090, 2020.

[72] W. Yuan and D. Guan, "Optimized Trust-Aware Recommender System Using Genetic Algorithm," Neural Network World, vol. 27, no. 1, p. 77, 2017.

[73] W. Song and V. V. Phoha, "Neural Network-Based Reputation Model in a Distributed System," in E-Commerce Technology, 2004. CEC 2004. Proceedings. IEEE International Conference on, pp. 321–324, IEEE, 2004.

[74] B. Zong, F. Xu, J. Jiao, and J. Lv, "A Broker-Assisting Trust and Reputation System Based on Artificial Neural Network," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, pp. 4710–4715, IEEE, 2009.

[75] J. Gómez, C. Gil, R. Baños, A. L. Márquez, F. G. Montoya, and M. Montoya, "A Pareto-Based Multi-Objective Evolutionary Algorithm for Automatic Rule Generation in Network Intrusion Detection Systems," Soft Computing, vol. 17, no. 2, pp. 255–263, 2013.

[76] J. Z. Lei and A. A. Ghorbani, "Improved Competitive Learning Neural Networks for Network Intrusion and Fraud Detection," Neurocomputing, vol. 75, no. 1, pp. 135–145, 2012.

[77] S. Rastegari, P. Hingston, and C.-P. Lam, "Evolving Statistical Rulesets for Network Intrusion Detection," Applied Soft Computing, vol. 33, pp. 348–359, 2015.

[78] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune System Approaches to Intrusion Detection–A Review," Natural Computing, vol. 6, no. 4, pp. 413–466, 2007.

[79] G. Suárez, L. Gallos, and N. Fefferman, "A Case Study in Tailoring a Bio-Inspired Cyber-Security Algorithm: Designing Anomaly Detection for Multilayer Networks," in 2018 IEEE Security and Privacy Workshops (SPW), pp. 281–286, IEEE, 2018.

[80] W. Wang, L. Ren, L. Chen, and Y. Ding, "Intrusion Detection and Security Calculation in Industrial Cloud Storage Based on an Improved Dynamic Immune Algorithm," Information Sciences, 2018.

[81] V. T. Alaparthy and S. D. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory," IEEE Access, vol. 6, pp. 47364–47373, 2018.

[82] T. P. Tran, L. Cao, D. Tran, and C. D. Nguyen, "Novel Intrusion Detection Using Probabilistic Neural Network and Adaptive Boosting," ArXiv Preprint ArXiv:0911.0485, 2009.

[83] V. Alarcon-Aquino, C. A. Oropeza-Clavel, J. Rodriguez-Asomoza, O. Starostenko, and R. Rosas-Romero, "Intrusion Detection and Classification of Attacks in High-Level Network Protocols Using Recurrent Neural Networks," in Novel Algorithms and Techniques in Telecommunications and Networking, pp. 129–134, Springer, 2010.

[84] M. S. Hoque, M. Mukit, M. Bikas, A. Naser, et al., "An Implementation of Intrusion Detection System Using Genetic Algorithm," ArXiv Preprint ArXiv:1204.1336, 2012.

[85] S. M. Bridges, R. B. Vaughn, et al., "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection," in Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109–122, 2000.

[86] M. Pillai, J. H. Eloff, and H. Venter, "An Approach to Implement a Network Intrusion Detection System Using Genetic Algorithms," in Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, pp. 221–221, South African Institute for Computer Scientists and Information Technologists, 2004.

[87] G. Karatas and O. K. Sahingoz, "Neural Network Based Intrusion Detection Systems with Different Training Functions," in Digital Forensic and Security (ISDFS), 2018 6th International Symposium on, pp. 1–6, IEEE, 2018.

[88] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep Recurrent Neural Network for Intrusion Detection in Sdn-Based Networks," in 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), pp. 202–206, IEEE, 2018.

[89] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Dendron: Genetic Trees Driven Rule Induction for Network Intrusion Detection Systems," Future Generation Computer Systems, vol. 79, pp. 558–574, 2018.

[90] A. S. Desai and D. Gaikwad, "Real Time Hybrid Intrusion Detection System Using Signature Matching Algorithm and Fuzzy-GA," in Advances

in Electronics, Communication and Computer Technology (ICAECCT), 2016 IEEE International Conference on, pp. 291–294, IEEE, 2016.

[91] S. Althubiti, W. Nick, J. Mason, X. Yuan, and A. Esterline, "Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection," in SoutheastCon 2018, pp. 1–5, IEEE, 2018.

[92] J. Yuan and S. Yu, "Privacy Preserving Back-Propagation Neural Network Learning Made Practical with Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 212–221, 2014.

[93] A. Said, R. A. Abbasi, O. Maqbool, A. Daud, and N. R. Aljohani, "CC-GA: A Clustering Coefficient Based Genetic Algorithm for Detecting Communities in Social Networks," Applied Soft Computing, vol. 63, pp. 59–70, 2018.

[94] J. Bian and S. Li, "Research on a Privacy Preserving Clustering Method for Social Network," in 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), pp. 29–33, IEEE, 2019.

[95] P. Li, J. Li, Z. Huang, T. Li, C.-Z. Gao, S.-M. Yiu, and K. Chen, "Multi-Key Privacy-Preserving Deep Learning in Cloud Computing," Future Generation Computer Systems, vol. 74, pp. 76–85, 2017.

[96] M. J. Usman, A. S. Ismail, H. Chizari, G. Abdul-Salaam, A. M. Usman, A. Y. Gital, O. Kaiwartya, and A. Aliyu, "Energy-Efficient Virtual Machine Allocation Technique Using Flower Pollination Algorithm in Cloud Datacenter: A Panacea to Green Computing," Journal of Bionic Engineering, vol. 16, no. 2, pp. 354–366, 2019.

[97] M. Tang and S. Pan, "A Hybrid Genetic Algorithm for the Energy-Efficient Virtual Machine Placement Problem in Data Centers," Neural Processing Letters, vol. 41, no. 2, pp. 211–221, 2015.

[98] I. Khan, J. Sahoo, S. Han, R. Glitho, and N. Crespi, "A Genetic Algorithm-Based Solution for Efficient in-Network Sensor Data Annotation in Virtualized Wireless Sensor Networks," in Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual, pp. 321–322, IEEE, 2016.

[99] G. Lee, N. Tolia, and P. Ranganathan, "Computing Cluster Performance Simulation Using a Genetic Algorithm Solution," Oct. 10 2017. US Patent 9,785,472.

[100] S. Azizi, D. Li, et al., "An Energy-Efficient Algorithm for Virtual Machine Placement Optimization in Cloud Data Centers," Cluster Computing, pp. 1–14, 2020.

[101] X.-F. Liu, Z.-H. Zhan, J. D. Deng, Y. Li, T. Gu, and J. Zhang, "An Energy Efficient Ant Colony System for Virtual Machine Placement in Cloud Computing," IEEE Transactions on Evolutionary Computation, vol. 22, no. 1, pp. 113–128, 2016.

[102] G. Cao, "Topology-Aware Multi-Objective Virtual Machine Dynamic Consolidation for Cloud Datacenter," Sustainable Computing: Informatics and Systems, vol. 21, pp. 179–188, 2019.

[103] N. Singh and V. Dhir, "Hypercube Based Genetic Algorithm for Efficient VM Migration for Energy Reduction in Cloud Computing," Statistics, Optimization & Information Computing, vol. 7, no. 2, pp. 468–485, 2019.

[104] M. Gamal, R. Rizk, H. Mahdi, and B. E. Elnaghi, "Osmotic Bio-Inspired Load Balancing Algorithm in Cloud Computing," IEEE Access, vol. 7, pp. 42735–42744, 2019.

[105] X. Liu, B. Cheng, Y. Yue, M. Wang, B. Li, and J. Chen, "Traffic-Aware and Reliability-Guaranteed Virtual Machine Placement Optimization in Cloud Datacenters," in 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), pp. 91–98, IEEE, 2019.

[106] N. Verma, V. Sharma, M. Kashyap, and A. Jha, "Heuristic Load Balancing Algorithms in Vulnerable Cloud Computing Environment," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 424–429, IEEE, 2018.

[107] E. D. Raj and L. D. Babu, "A Firefly Swarm Approach for Establishing New Connections in Social Networks Based on Big Data Analytics," International Journal of Communication Networks and Distributed Systems, vol. 15, no. 2-3, pp. 130–148, 2015.

[108] X. Pu, S. Chen, X. Yu, and L. Zhang, "Developing a Novel Hybrid Biogeography-Based Optimization Algorithm for Multilayer Perceptron Training Under Big Data Challenge," Scientific Programming, vol. 2018, 2018.

[109] X. Tong, Z. Wang, and H. Yu, "A Research Using Hybrid RBF/Elman Neural Networks for Intrusion Detection System Secure Model," Computer Physics Communications, vol. 180, no. 10, pp. 1795–1801, 2009.

[110] F. Kuang, W. Xu, and S. Zhang, "A Novel Hybrid KPCA and SVM with GA Model for Intrusion Detection," Applied Soft Computing, vol. 18, pp. 178–184, 2014.

[111] G. Abou Haidar and C. Boustany, "High Perception Intrusion Detection System Using Neural Networks," in 2015 Ninth International Conference on Complex, Intelligent, and Software Intensive Systems, pp. 497–501, IEEE, 2015.

[112] S. N. H. S. Abdullah, M. H. Abdulameer, N. A. Zamani, F. Rahim, K. A. Z. Ariffin, Z. Othman, and M. Z. A. Nazri, "2.5 D Facial Analysis via Bio-Inspired Active Appearance Model and Support Vector Machine for Forensic Application," 2017.

[113] S. K. Abbas, H. H. M. AlKaraawi, and M. Q. Dhahir, "Comparative Study Of SVM-Based Classification Techniques for Human Facial Recognition,"

[114] A. H. Mohsin, I. M. Rahi, and R. A. Hussain, "A Study of 2.5 D Face Recognition for Forensic Analysis,"

[115] R. H. A. Al_Sagheer, J. Mona, A. Abdulmohson, and M. H. Abdulameer, "Fingerprint Classification Model Based on New Combination of Particle Swarm Optimization and Support Vector Machine,"

[116] G. S. Pandi, S. Shah, and K. Wandra, "Exploration of Vulnerabilities, Threats and Forensic Issues and its Impact on the Distributed Environment of Cloud and its Mitigation," Procedia Computer Science, vol. 167, pp. 163–173, 2020.

[117] H. Chung, J. Park, S. Lee, and C. Kang, "Digital Forensic Investigation of Cloud Storage Services," Digital Investigation, vol. 9, no. 2, pp. 81–95, 2012.

[118] D. R. Rani, S. N. Sultana, and P. L. Sravani, "Challenges of Digital Forensics in Cloud Computing Environment," Indian Journal of Science and Technology, vol. 9, no. 17, pp. 90–100, 2016.

[119] K. Ruan and J. Carthy, "Cloud Computing Reference Architecture and its Forensic Implications: A Preliminary Analysis," in International Conference on Digital Forensics and Cyber Crime, pp. 1–21, Springer, 2012.

[120] J. Shah and L. G. Malik, "An Approach Towards digital Forensic Framework for Cloud," in 2014 IEEE International Advance Computing Conference (IACC), pp. 798–801, IEEE, 2014.

[121] D. Liu, J. Lee, J. Jang, S. Nepal, and J. Zic, "A Cloud Architecture of Virtual Trusted Platform Modules," in 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 804–811, IEEE, 2010.

[122] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results," Digital Investigation, vol. 10, no. 1, pp. 34–43, 2013.

[123] H. Al-Zoubi, "Efficient Task Scheduling for Applications on Clouds," in 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 10–13, IEEE, 2019.

[124] M. Aliyu, M. Murali, A. Y. Gital, and S. Boukari, "Efficient Metaheuristic Population-Based and Deterministic Algorithm for Resource Provisioning Using Ant Colony Optimization and Spanning Tree," International Journal of Cloud Applications and Computing (IJCAC), vol. 10, no. 2, pp. 1–21, 2020.

[125] S. N. Chari, B. J. Edwards, T. Lee, I. M. Molloy, and Y. Park, "Deep Learning for Targeted Password Generation with Cognitive User Information Understanding," Jan. 21 2020. US Patent 10,540,490.

[126] A. Mosa and N. W. Paton, "Optimizing Virtual Machine Placement for Energy and SLA in Clouds Using Utility Functions," Journal of Cloud Computing, vol. 5, no. 1, p. 17, 2016.

[127] A. Saini and A. Kansal, "Hybrid Approach to Reduce Energy Utilization in Wireless Sensor Network using Bio-Inspired Technique," 2019.

[128] S. Verma, N. Sood, and A. K. Sharma, "Genetic Algorithm-Based Optimized Cluster Head Selection for Single and Multiple Data Sinks in Heterogeneous Wireless Sensor Network," Applied Soft Computing, vol. 85, p. 105788, 2019.

[129] J. Ghosh, D. Kumar, and R. Tripathi, "Features Extraction for Network Intrusion Detection Using Genetic Algorithm (GA)," in Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough, pp. 13–25, Springer, 2020.

[130] B. B. Naik, D. Singh, A. B. Samaddar, and S. Jung, "Developing a Cloud Computing Data Center Virtual Machine Consolidation Based on Multi-Objective Hybrid Fruit-Fly Cuckoo Search Algorithm," in 2018 IEEE 5G World Forum (5GWF), pp. 512–515, IEEE, 2018.

[131] A. Sampathkumar, J. Mulerikkal, and M. Sivaram, "Glowworm Swarm Optimization for Effectual Load Balancing and Routing Strategies in Wireless Sensor Networks," Wireless Networks, pp. 1–12, 2020.

[132] M. S. Al Daweri, S. Abdullah, and K. Z. Ariffin, "A Migration-Based Cuttlefish Algorithm With Short-Term Memory for Optimization Problems," IEEE Access, vol. 8, pp. 70270–70292, 2020.

[133] N. Koroniotis and N. Moustafa, "Enhancing Network Forensics with Particle Swarm and Deep Learning: The Particle Deep Framework," ArXiv Preprint arXiv:2005.00722, 2020.

[134] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved Security Particle Swarm Optimization (PSO) Algorithm to Detect Radio Jamming Attacks in Mobile Networks," Quintana, vol. 11, no. 4, 2020.

[135] Y. Shi and H. Shen, "Anomaly Detection for Network Flow Using Immune Network and Density Peak.," IJ Network Security, vol. 22, no. 2, pp. 337–346, 2020.

[136] T. Meng and Q.-K. Pan, "An Improved Fruit Fly Optimization Algorithm for Solving the Multidimensional Knapsack Problem," Applied Soft Computing, vol. 50, pp. 79–93, 2017.

[137] J. Duan, J. Zhou, and Y. Li, "Privacy-Preserving Distributed Deep Learning Based on Secret Sharing," Information Sciences, 2020.

[138] S. Festag and C. Spreckelsen, "Privacy-Preserving Deep Learning for the Detection of Protected Health Information in Real-World Data: Comparative Evaluation," JMIR Formative Research, vol. 4, no. 5, p. e14064, 2020.

[139] Y. Li, L. Wu, T. Wang, N. Gao, and Q. Wang, "EEG Signal Processing Based on Genetic Algorithm for Extracting Mixed Features," International Journal of Pattern Recognition and Artificial Intelligence, vol. 33, no. 06, p. 1958008, 2019.

[140] J. Chen, Z. Mao, W. Yao, and Y. Huang, "EEG-Based Biometric Identification with Convolutional Neural Network," Multimedia Tools and Applications, pp. 1–21, 2019.

[141] M. Cao and W. Fang, "Swarm Intelligence Algorithms for Weapon-Target Assignment in a Multilayer Defense Scenario: A Comparative Study," Symmetry, vol. 12, no. 5, p. 824, 2020.

[142] R. C. Poonia, "A Performance Evaluation of Routing Protocols for Vehicular Ad Hoc Networks with Swarm Intelligence," International Journal of System Assurance Engineering and Management, vol. 9, no. 4, pp. 830–835, 2018.

[143] S. Harizan and P. Kuila, "Nature-Inspired Algorithms for k-Coverage and M-Connectivity Problems in Wireless Sensor Networks," in Design Frameworks for Wireless Networks, pp. 281–301, Springer, 2020.

[144] B. N. Sahu and S. K. Sahoo, "A Constructional Approach of Robotics Wireless Sensor Networks,"

[145] V. Vijayan and G. A. Rubasundram, "Artificial Neural Network (ANN): An Artificial Intelligent (AI) Tool to Predict Fraudulent Financial Reporting and Financial Distress.," International Journal of Psychosocial Rehabilitation, vol. 24, no. 2, 2020.

[146] E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, and L. M. Jaimes, "Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning," in 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1–6, IEEE, 2018.

[147] M. Aslan and S. Sen, "Evolving Trust Formula to Evaluate Data Trustworthiness in VANETs Using Genetic Programming," in International Conference on the Applications of Evolutionary Computation (Part of EvoStar), pp. 413–429, Springer, 2019.

[148] M. Tan, A. Iacovazzi, N.-M. M. Cheung, and Y. Elovici, "A Neural Attention Model for Real-Time Network Intrusion Detection," in 2019 IEEE 44th Conference on Local Computer Networks (LCN), pp. 291–299, IEEE, 2019.

[149] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K.-K. R. Choo, and J. Iqbal, "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," IEEE Access, vol. 8, pp. 53972–53983, 2020.

[150] R. Tang, Z. Yang, Z. Li, W. Meng, H. W. Q. Li, Y. Sun, D. Pei, T. Wei, Y. Xu, and Y. Liu, "ZeroWall: Detecting Zero-Day Web Attacks through Encoder-Decoder Recurrent Neural Networks," INFOCOM, 2020.

[151] K. D. Gupta, D. Dasgupta, and Z. Akhtar, "Determining Sequence of Image Processing Technique (IPT) to Detect Adversarial Attacks," ArXiv Preprint ArXiv:2007.00337, 2020.

[152] S. Sen, K. D. Gupta, S. Poudyal, and M. M. Ahsan, "Agenetic Algorithm Approach to Optimize Dispatching for a Microgrid Energy System with Renewable Energy Sources,"

[153] S.-K. Yeom, H.-I. Suk, and S.-W. Lee, "Person Authentication from Neural Activity of Face-specific Visual Self-representation," Pattern Recognition, vol. 46, no. 4, pp. 1159–1169, 2013.

[154] F. Kitchens, S. Sharma, and Q. Booker, "Identity Authentication Based on Keystroke Latencies Using a Genetic Adaptive Neural Network," Sept. 24 2009. US Patent App. 11/112,337.

[155] W.-C. Ku, "Weaknesses and Drawbacks of a Password Authentication Scheme Using Neural Networks for Multiserver Architecture," IEEE Transactions on Neural Networks, vol. 16, no. 4, pp. 1002–1005, 2005.

[156] S. Sen, K. D. Gupta, and M. M. Ahsan, "Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS Attack," in Proceedings of International Joint Conference on Computational Intelligence, pp. 49–60, Springer, 2020.

MD M. AHSAN Received MS in Industrial Engineering from Lamar University, USA, in 2018. Currently, he is pursuing the PhD degree in Industrial and Systems Engineering from University of Oklahoma, Norman, USA from 2019−present.He currently holds a Graduate research assistant position at University of Oklahoma. His research interest includes image processing, computer vision, deep learning, machine learning, model optimization.

KISHOR DATTA GUPTA is a Ph.D. student and Research assistant in Computer science dept. at University of Memphis. He is currently working toward his Ph.D. degree and his research interests includes Image processing, computer vision, machine learning, deep learning and big data analysis.

DR. ABHIJIT KUMAR NAG is an assistant professor in Computer Information Systems department at Texas AM University-Central Texas since 2017. He obtained his Ph.D. in Computer Science from the University of Memphis. Previously he received his master's in Computer Engineering from the University of Memphis. His primary research interest includes various authentication approaches, mainly continuous authentication and multifactor authentication systems. His other research interests include evolutionary algorithms, internet of things, cloud computing, bioinspired/ nature-inspired computing, and big data. He is an inventor of a utility patent on Adaptive Multi-factor Authentication system. He is a co-author of a graduate-level textbook- Advances in User Authentication. Dr. Nag serves as a reviewer for many reputable peer-reviewed journals and conferences. Dr. Nag provided a tutorial talk on Computational Intelligence in User Identity Management in IEEE SSCI conference in 2017.

SUBASH POUYDAL doing phd at University of Memphis in computer security. He is Interest in ransomware and malware detection by NLP techniques.

PROF. ABBAS KOUZANI received his B.Sc. degree in Computer Engineering from Sharif University of Technology, Iran, his M.Eng. degree is Electrical and Electronic Engineering from University of Adelaide, Australia, and his Ph.D. degree in Electrical and Electronic Engineering from Flinders University, Australia. He was a lecturer with the School of Engineering, Deakin University, and then a Senior Lecturer with the School of Electrical Engineering and Computer Science, University of Newcastle, Australia. Currently, he is a Professor with the School of Engineering, Deakin University, Australia. He provides research leadership in embedded, connected, and low-power devices, circuits, and instruments that incorporate sensing, actuation, control, wireless transmission, networking and IoT, data acquisition/storage/analysis, AI, energy harvesting, power management, and fabrication for tackling research questions relating to a variety of disciplines including healthcare, ecology, mining, infrastructure, automotive, manufacturing, energy, utilities, and agriculture. Has produced over 370 publications including 1 book, 17 Book Chapters, 180 Journal Papers, and 181 fully refereed Conference Papers. He has 3 patents and 2 pending patents. He has been involved in over $15 million research grants, and has managed projects and delivered research solutions to over 25 Australian and International companies. He received several wards including "Outstanding Contribution to Scholarly Publication Award", School of Engineering, Deakin University, 2019. He has supervised 24 research fellows/assistants, and produced 28 Ph.D. and 6 Masters by Research completions. Currently, he is involved in supervision of 12 PhD students. He is the Director of Deakin University's Advanced Integrated Microsystems (AIM) research group.

DR. M. A. PARVEZ MAHMUD received his B.Sc. degree in Electrical and Electronic Engineering and Master of Engineering degree in Mechatronics Engineering. After the successful completion of his Ph.D. degree with multiple awards, he worked as a Postdoctoral Research Associate and Academic in the School of Engineering at Macquarie University, Sydney. He is currently an Alfred Deakin Postdoctoral Research Fellow at Deakin University. He worked at World University of Bangladesh (WUB) as a 'Lecturer' for more than 2 years and at the Korea Institute of Machinery and Materials (KIMM) as a 'Researcher' for about 3 years. His research is focused on Energy Sustainability, Secure Energy Trading, Microgrid Control and Economic Optimization, Machine Learning, Data Science, and Micro/nanoscaled Technologies for Sensing and Energy Harvesting. He accumulated experience and expertise in machine learning, life cycle assessment, sustainability and economic analysis, materials engineering, microfabrication, and nanostructured energy materials to facilitate technological translation from the lab to real-world applications for the better society. He has produced over 50 publications, including 1 authored book, 3 Book Chapters, 29 Journal Papers, and 21 fully refereed Conference Papers. He received several awards including "Macquarie University Highly Commended Excellence in Higher Degree Research Award 2019". He was involved in teaching engineering subjects in the electrical, biomedical and mechatronics engineering courses at the School of Engineering, Macquarie University for more than 2 years. Currently, he is involved in the supervision of 6 PhD students at Deakin University. He is a key member of Deakin University's Advanced Integrated Microsystems (AIM) research group. Apart from this, he is actively involved with different professional organizations, including Engineers Australia and IEEE.