Retraction Notice

The Editor-in-Chief and the publisher have retracted this article, which was submitted as part of a guest-edited special section. An investigation uncovered evidence of systematic manipulation of the publication process, including compromised peer review. The Editor and publisher no longer have confidence in the results and conclusions of the article.

HA did not agree with the retraction.

JEI Journal of
Electronic Imaging

RESEARCH PAPER

Cyber-security trust model through adaptive cloud authentication protocol for web application

Hatim Alsuwat*
Umm Al-Qura University, College of Computers and Information Systems, Department of Computer Science,
Makkah, Saudi Arabia

ABSTRACT. The development and growth of internet-based technologies brings challenges in cyber-security from cyberattack organizations. It is necessary to develop an appropriate cyber-security scheme through a structured machine learning algorithm implemented in the cloud architecture. The aim of our research is to design a cloud-based architecture using an adaptive cloud authentication protocol to develop the trust model for cyber-security systems. Here, the structure learning of Bayesian networks (SL_BN) is developed with an ensemble architecture of machine learning that is integrated with the support vector machine and adaptive fuzzy-based genetic algorithm (SVM_AFGA). The fuzzy logic sets rules for using web applications at the authorized web address. The experimental results show that parametric analysis based on the cyber-security authentication model is based on median delay, transmission level overhead, and security of the network. Moreover, the parameters based on the SL-BN ensemble architecture are average runtime, accuracy, and network efficiency.

© 2023 SPIE and IS&T [DOI: 10.1117/1.JEI.32.4.042109]

Keywords: cyber-security; structure learning; Bayesian network; machine learning; adaptive cloud authentication protocol; support vector machine and adaptive fuzzy-based genetic algorithm

Paper 230137SS received Feb. 7, 2023; revised May 1, 2023; accepted May 3, 2023; published May 23, 2023.

1 Introduction

Over the last few years, cloud computing (CC) has gained the attention of researchers, businesses, governments, and consumers in industry and academia.[1] With the evolution of CC investment and the development of information technology (IT) infrastructure, cloud consumers employ cloud resources and a pay-as-you-go model with broad network access with elastic resources.[2] The National Institute of Standards and Technology (NIST) has characterized CC as a service designed for a ubiquitous environment. In CC, the service access is based on demand for configurable resource computation, applications, services, and storage. These services could be provided with fewer management efforts while reducing the required interactions with customers.[3]

CC is represented as per the NIST; it enables a ubiquitous environment and service access based on demand for configurable resource computation for different networks, applications, services, storage, and so on, which can be provided and released with minimal management and desired service interaction with the customers.[3]

CC comprises four key points: (1) a computing resource pool with an on-demand access mechanism, (2) scalable and dynamic services, (3) ease of installation and maintenance of the

*Address all correspondence to Hatim Alsuwat, Hssuwat@uqu.edu.sa

1017-9909/2023/$28.00 © 2023 SPIE and IS&T

user machines, and (4) independent devices. Based on the needs of the owner, cloud services are private, community, public, or hybrid clouds.[4] In CC, security is a vital role for withstanding different threats that plague the cloud infrastructure market. CC comprises different security issues and layers in the cloud architecture to evaluate the relationship between variables. The cyber-security threats in the cloud environment are based on vulnerability, attacks, and threats.[5,6]

The problem areas in CC represent potential vulnerabilities that can lead to security breaches and compromises in the cloud environment. For instance, cloud data integrity issues can arise if data are not stored securely or if data are tampered with during transit. Similarly, a lack of cloud accountability can make it difficult to trace the source of a security breach or data loss. Repository auditing and user revocation issues can also lead to unauthorized access to sensitive information. Inefficient energy usage can create additional costs and environmental concerns. The integrity and consistency of data in the cloud can be compromised if proper measures are not taken to ensure data protection. Finally, trust management, data deduplication, and due diligence issues can further exacerbate cloud security risks.

In recent years, cyber-security has been a major concern in a vast range of scenarios that take into consideration different contexts and actors' impact on the national infrastructure security, applications, services, security, and stability of the structure.[7] Cybersecurity is a growing concern in terms of agenda, legitimate, and illegitimate at attack type and levels. To achieve the scrutiny, cybersecurity concepts have been applied over a vast range of applications for consumers and providers.[8] With the evolution of telecommunication infrastructure, conventional systems and IT networks developing a unified architecture is a challenging factor. On the other hand, with increases in the usability of individual computer networks, it is highly difficult to maintain network boundaries with physical and logical terms. For maintaining a country's economy, increasing the interconnectivity and accessibility is considered to be a critical factor for computer-based application systems.[9] The cyber capability of a country is considered an integral part of borderless cyberspace. In developing countries, internet utilization is significantly high, which leads to the growth of cyberspace. The significant advancement in ownership largely comprises mobile devices that can be accessed with the internet, which expands the country's cyberspace economy.[10] Globally, cyberspace expansion is exponentially increased with the improvement of security. The advancement in the internet system's success is attributed to the consideration of entry barriers and openness. However, cyber-security is a factor partly responsible for cyberspace in terms of cyber warfare, terrorism, and crime.

1.1 Fundamental Concepts of Cyberattack

Cyberattacks are an emerging threat to CC for information operations. Cyberattack information is integrated based on the consideration of the capabilities for warfare (psychological and military), computer networks, and security in support of relevant abilities for the decision-making process.[11] Figure 1 presents the illustration of the cyberattack sources in CC. Based on the United States National Museum (USNM) strategy, cyberspace computation is evaluated for its operations, computer network, attack, defense, and enabling of the utilization capabilities of the network. The evaluation is based on the computation of the attacks in the network, and defense is based on operation and information analysis without interrupting the network.[13] The CC operation is disseminated for information processing with the exploitation of the computer network operations stealing the data of the computers. In this context, to prevent cyberattacks sniffers and doors are the potential factor for software accessibility of external users at any time without interfering the computer knowledge. The data usernames and passwords are identified and stolen by cyberspace definitions and concepts.[12] Figure 1 illustrates the different sources of cyber threats in the CC.

The sources of cyber threats in the network are as follows: overthrowing the government system or catastrophic threats that affect the security, physical warfare or groundwork facilities for physical warfare, international level catastrophic destruction, the relationship between political and economic relations, extensive public health and safety, broader administration damage, and damage to the economy of nations and cyber assets.[14] In addition, cyber warfare is evaluated based on the consideration of five scenarios: cyberspace government-sponsored for information gathering in cyberattacks, an uprising of the cyberattack in the groundwork based on laying, disabling of the equipment for physical aggression, complementing with the cyberattacks, and

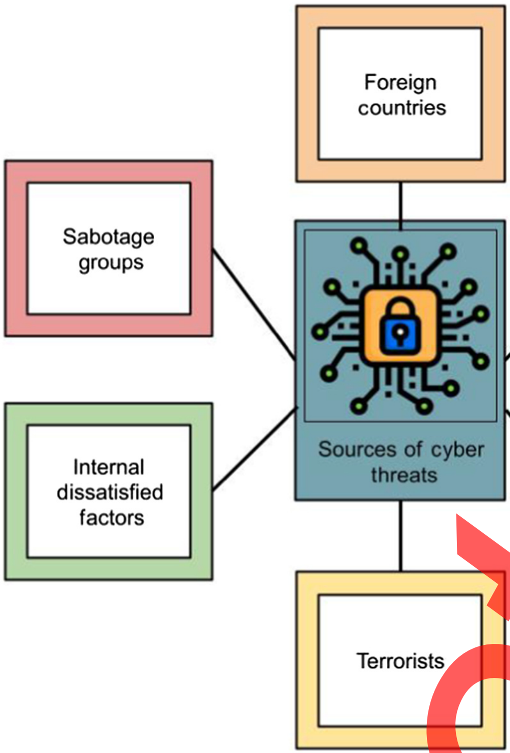

Fig. 1 Sources of cyber threats.[12]

cyberattack with destruction being the goal in cyber warfare.[15] Frequently, cyberattacks could be evaluated depending on the consideration of security threats for reversible methods for the decryption of keys.[16] In Fig. 2, the cyberattack anatomy for CC is presented.

There is a need for effective cyber-security measures to protect cloud-based systems from cyberattacks. With the increasing reliance on CC and the storage of sensitive data in the cloud, there is a greater need for a robust and reliable cyber-security scheme that can detect and prevent cyberattacks. One approach to achieving this is through the use of machine learning algorithms. Machine learning algorithms can analyze large datasets and detect patterns that may be indicative of a cyberattack. However, to be effective, these algorithms must be appropriately structured and implemented over a cloud architecture. Developing an appropriate cyber-security scheme involves several challenges, including identifying the types of cyberattacks that may occur,

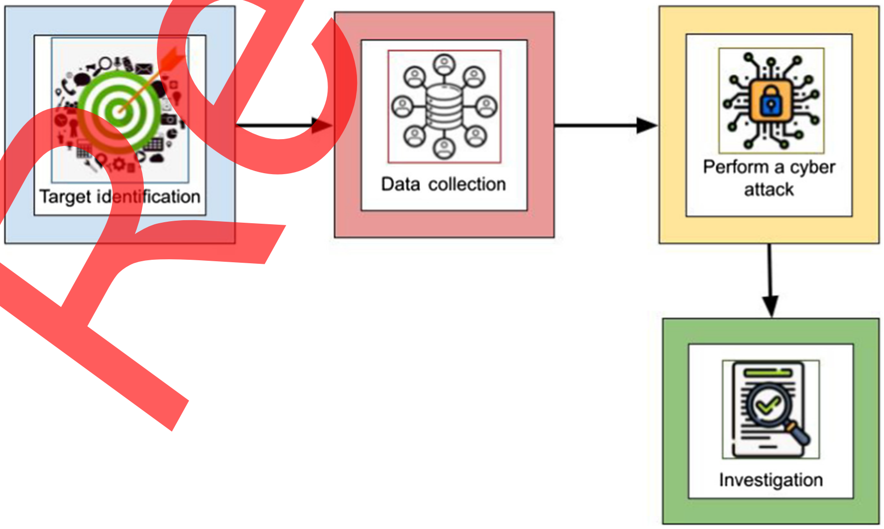

Fig. 2 Anatomy of cyberattacks.

selecting the appropriate machine learning algorithms to detect those attacks, and designing a cloud architecture that can support the efficient and effective implementation of these algorithms.

To address these concerns, this paper proposes an adaptive cloud authentication protocol (ACAP). The CAP is a mechanism or set of protocols used to authenticate users, devices, or applications accessing cloud-based services or resources. This authentication process is necessary to ensure that only authorized users or devices are allowed access to cloud resources and unauthorized access attempts are blocked. The CAP typically involves the exchange of credentials, such as usernames and passwords, between the user or device and the cloud-based service provider. Various authentication mechanisms can be used in CAPs, including multi-factor authentication, biometric authentication, and token-based authentication. The goal of the CAP is to provide secure and reliable authentication and access control mechanisms to protect against unauthorized access to cloud-based resources. The major contributions of this paper are as follows:

- a cloud-based architecture using the ACAP is designed to develop a trust model for cyber-security systems;
- a structure learning-based Bayesian network is developed through ensemble architecture of machine learning, integrated with support vector machine, and adaptive fuzzy-based genetic algorithm (SVM_AFGA);
- a fuzzy logic (FL) mechanism is implemented to set rules for using web applications to an authorized web address;
- the effectiveness of the proposed model is demonstrated through parametric analysis based on the cyber-security authentication model with median delay, transmission level overhead, and network security parameters;
- the proposed model with SVM_AFGA exhibits improved performance regarding accuracy, precision, and F1-Score, reducing the rate of false positives (FPs);
- the method contributes to the development of a comprehensive and well-structured approach to cyber-security that incorporates machine learning algorithms and the cloud architecture to protect against cyberattacks in cloud-based systems.

This paper is organized as follows: related works on cloud security are presented in Sec. 2. In Sec. 3, the developed model SVM_AFGA fuzzy set and optimization model with Bayesian learning are presented. In Sec. 4, the dataset for analysis and the results are provided. The overall conclusion is presented in Sec. 5.

2 Related Work

Over several decades, IT has exhibited significant developments and advancements. CC has been utilized in a vast range of applications such as water, gas, electricity, and telephone systems. Indeed, the vast range of emerging applications are evaluated based on the requirements of the CC environment.

In Ref. 17, the authors developed a hybrid model of inter-module secure communication for system tracking and operations. The security scheme used the digital signature with the recording of the timestamp of the users. The hybrid model comprised both symmetric and asymmetric keys integrated with the message-digest Algorithm 5 within the cloud infrastructure. To encrypt data, three methods have been used: public key cryptosystems (such as Rivest-Shamir-Adleman), private key cryptosystems (such as advanced encryption standard), or hash functions (such as secure hash algorithm).

In Ref. 18, the authors developed a policy-hidden attribute-based broadcast for decryption. The model comprised the partially hidden policy for outsourced verification based on the attributes scheme ciphertext-policy attribute-based encryption. Through the access policy scheme, the hidden policy scheme was protected for private information processing. Also, the messages were processed through the revocation of the users to gain access. In Ref. 19, the authors evaluated identity-based key exposure for public auditing in the cloud model. The developed model used the infrastructure of the public key based on lattice-based delegation. The developed scheme used the private key update without modifying the key size. The scheme for key generation comprised the extraction of the key, update, generation of authentication, proof, and verification.

Moreover, the authors of Ref. 20 proposed a security scheme based on the redundant residue number system (RRNS) for secret information sharing for error corrections. The RRNS scheme comprised the rank of a number estimation for minimization of the intricacy of the decoding. The RRNS scheme comprised error detection, correction, and computation. The analysis results expressed that the efficiency and effectiveness were significantly higher and adequate. In another study,[21] the authors developed a public auditing scheme for identity privacy and traceability of cloud security. The members of the group were evaluated for authentication for privacy identification of the employed records and members in each block.

Some significant security services, such as authentication protocol, are offered in cloud computing, according to a related study.[22] The four elements that make up the complete architecture are communication, hybrid authentication protocol, cloud database, and security server. A hybrid authentication mechanism is used to ensure effective security. With the hybrid authentication protocol, data are first registered. A privacy module is then used to guarantee privacy for this data. The security key for the collected data is now offered. Functions related to databases are then carried out. Data transmission and reception are secure due to the security server. Data are stored in a cloud database.

In Ref. 23, the authors demonstrated that the Wazid et al. protocol had a high communication and storage cost and was vulnerable to attacks such as denial-of-service attacks, attacks using stolen smart cards, and attacks using privileged insider information. The authors also put forth a protocol that fixed these issues. To demonstrate its resilience against security threats, they conducted both informal and formal security analysis and simulated it using the automatic validation of internet security protocols and applications tool.

A simple authentication scheme for IoT-enabled CC systems was developed in another study.[24] To do a formal security study, a real or random model and the automatic verification program ProVerif were utilized. More evidence of its security came from a casual investigation. An innovative, elliptic curve cryptography-based, privacy-preserving multi-factor authentication technique for CC was suggested by the authors of Ref. 25. As security and privacy authentication characteristics, this protocol offered user anonymity, unlinkability, perfect forward secrecy, and session key security. The real-or-random paradigm was used to theoretically demonstrate the system's security. The authors used the Scyther security verification tools to verify the correctness characteristics of the approach. This protocol was resistant to several security attacks, including replay, user impersonating, server spoofing, password guesses, and powerful cyberattacks.

The need for computing is driven by CC features including on-demand self-service, widespread network connectivity, resource pooling, and quick adaptability. Despite these advantages, the lack of secure authentication and privacy makes this platform vulnerable to security problems and assaults, particularly in terms of communication. Strong user authentication procedures are the primary prerequisite for safeguarding the CC environment. The authors of Ref. 26 suggested potential safeguards for the cloud ecosystem in this regard. This study proposed a unique one-way hash-based two-factor secure authentication technique with the conventional user ID, password, and one-time password verification procedure that resisted brute force assault, session and accounts hijacking assault, and replay assault. Using an elliptic curve cryptosystem, the authors of Ref. 27 introduced a unique pairing-free multiserver authentication technique for mobile CC environments that weree not only effective but also devoid of security flaws.

In a similar research,[28] the authors created a model called enhanced cloud security model utilizing quantum key distribution protocol (QKDP) that incorporated quantum key cryptography to secure CC and handle data dynamics. Also, the situation of communication between three entities—cloud server, data owner, and legitimate user (LU)—was taken into account. In this situation, the quantum keys were transferred in two phases. The secure authentication scheme was constructed based on distance boundaries and secure keys that were created using hierarchical attribute-set based encryption in the second phase. The first procedure employed BB84 QKDP. Using the paradigm, the secured keys were sent to the LU through a reliable route.

The majority of studies in the literature on secure data transmission only take authenticated key agreements into account when communicating entities are being authenticated. Certain protocols lack protection against potential intrusions. To address these issues with efficiency by utilizing lightweight operations and to improve security through the application of the physical unclonable function, the authors of Ref. 29 presented authentication key agreement methods for e-Healthcare systems (PUF). PUFs contain message fingerprints that serve as authentication keys that they compute using the uniqueness and randomness of their circuits. A PUF is portable and appropriate for use in resource-constrained e-Healthcare systems.[30–33]

In recent years, there has been a significant increase in the number of researchers addressing cyber-security issues in their respective studies.[34–38] The current research gap in the field of cyber-security is the need for effective intrusion detection system (IDS) for cloud-based systems. Traditional IDS techniques are not sufficient for detecting and preventing cyberattacks in the cloud as cloud systems have complex and dynamic structures that require adaptive and scalable security solutions.[39–44] The proposed model fulfills the current research gap by incorporating an ACAP to develop a trust model for cyber-security systems. The model uses a structure learning-based Bayesian network through an ensemble architecture of machine learning, integrated with SVM_AFGA. The model also implements a FL mechanism to set rules for using web applications to an authorized web address, which is a unique approach to cyber-security in cloud-based systems. A detailed overview of the proposed model is presented in the subsequent section.

3 Bayesian ACAP

This paper concentrates on the CAP for SVM_AFGA with the cost-based model for authentication. the proposed model comprises the structure learning of Bayesian networks, and a structured learning model fuzzy-based genetic algorithm is implemented. The Bayesian network offers graphical representations of random variables with interdependencies of interconnected nodes. The Bayesian network ACAP offers links between parent and child nodes with direct links to different applications, as illustrated in Fig. 3.

The Bayesian network model incorporates two analyses: forward analysis and backward analysis. In ACAP, the Bayesian network performs analysis with forward analysis in the estimation of the predictive technique with computation of the occurrence probability prediction of the nodes based on the root node prior probabilities, with intermediate nodes being estimated with conditional probability. ACAP integrated with the SVM_AFGA with backward analysis incorporates computation technique for posterior probability updating as per the Bayes theorem of evidence I. To perform authentication, the observation is based on the estimation of the

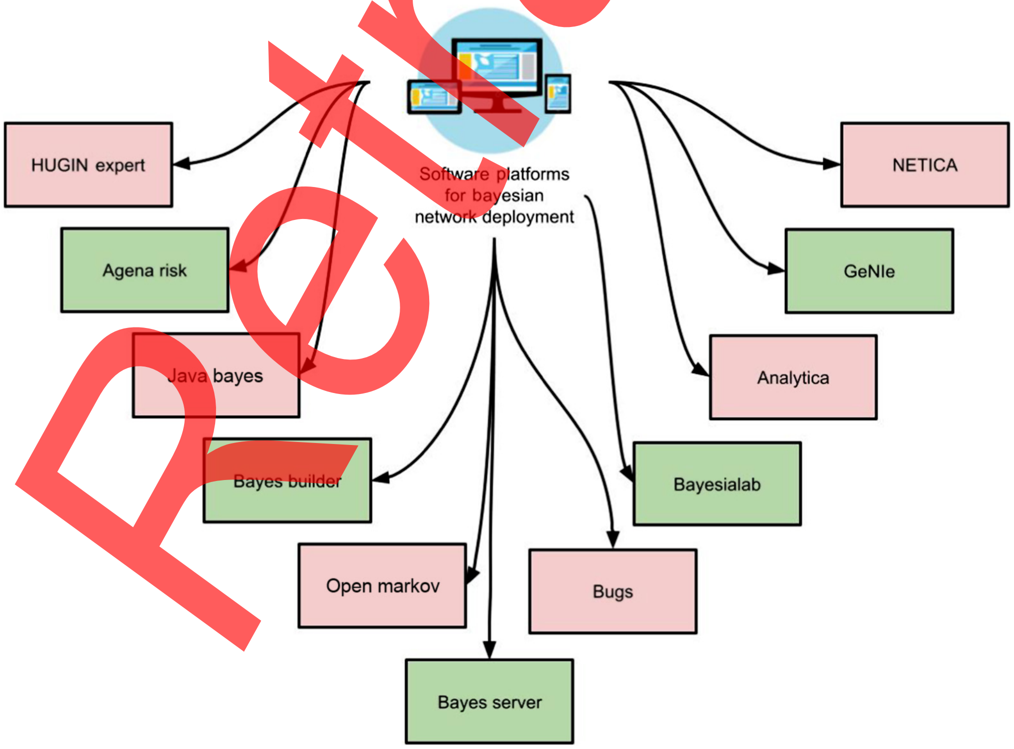

Fig. 3 Software platform for Bayesian.

consequences of certain recent incidents of the evidence. In ACAP, the posterior probability of the evidence (E) is calculated as

$$P(\mathrm{XE}) = \frac{P(X,E)}{P(E)}. \tag{1}$$

$P(X,E)$ is the joint probability of event X and evidence E is the marginal probability of the evidence E occurring, and $P(X,E)$ is the conditional probability of event X given that evidence E has occurred (i.e., the posterior probability of X given E). Hence, in Eq. (1), different authentication factors are evaluated based on the qualitative and quantitative analyses based on interdependencies and computation of the failure probabilities.

3.1 Validation of Bayesian Networks

The proposed ACAP validates the Bayesian network to evaluate the accuracy of the model. With the Bayesian approach, the security incidents are evaluated based on the incident probability with FL conditions as low, extremely low, and almost impossible. The statistics validate and verify the larger outcome of the events with occurrences that are minimal. The proposed SVM_AFGA performs validation based on consideration of three axions, which are explained as follows:

1. There is an increase or decrease in the failure posterior probabilities between the parent and child nodes.
2. There needs to be consistency in the magnitude of the variation in the child node of the parent node probability distribution.
3. The total influence with the integration of probabilities of the attributes is based on consideration of the attributes of the probabilities.

Based on these axions, the constructed Bayesian network is verified, and partial validation is performed.

3.2 Fuzzy-Based Genetic Algorithm

To improve cyber-security in the cloud, the proposed SVM_AFGA comprises the FL to perform classification and detection of cyberattacks in the network. The fuzzy interface system comprises a set of rules for characters in which the variable of input is integrated with a logical operator such as AND, NOT, and OR. The fuzzy interface system comprises the triangular and Gaussian processes with time series analysis for the estimation.

The fuzzy interface system comprises five stages: the transformation of data for input into fuzzy elements, implementation of the fuzzy operator, implication method, output group, and transformation of output data. The fuzzy membership function comprises structured learning with subtractive clustering to generate fuzzy sets with multidimensional space examination. With fuzzy C-means clustering, fuzzy sets are randomly optimized centroids.

3.2.1 *Data support vector regression with fuzzy set*

SVM is a class of support vector regression used for performing classification. This technique uses the Vapnik–Chervonenkis dimension scheme for forecasting to reduce the structural risk with the minimization principle as illustrated in Fig. 4. The estimated SVM with the linear regression model is expressed as

$$f(x) = \omega\phi(x) + b. \tag{2}$$

In Eq. (2), input space non-linear mapping is represented as $\omega\phi(x)$, and the threshold is defined as b. With time series analysis of the input vector $x_i$involved in the predicted variable y_i, the estimated goal function and constraints are denoted in Eq. (3)–Eq. (5) as

$$\min_{\omega,b,\varepsilon,\varepsilon^*} \frac{1}{2}\omega^T\omega + C\sum_{i=1}^{1}(\varepsilon_t + \varepsilon_t{}^*), \tag{3}$$

subject to

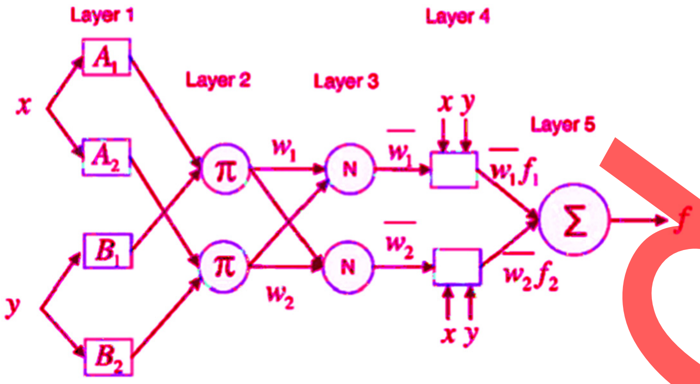

Fig. 4 Fuzzy interface.

$$(\omega^T \phi(x_i) + b) - y_i \leq \varepsilon + \varepsilon_i, \tag{4}$$

$$y_i - (\omega^T \phi(x_i) + b) \leq \varepsilon + \varepsilon_i^*. \tag{5}$$

In Eq. (3)–Eq. (5), ε_t and ε_t^* are denoted as slack variables, and the Lagrangian multiplier is represented as C. For the cloud, cyber-security authentication uses the optimization algorithm with a unique and global variable, given as

$$\min_{\alpha,\alpha^* 2} \frac{1}{2}(\alpha - \alpha^*)^T K(\alpha - \alpha^*) + \in \sum_{i=1}^{l}(\alpha - \alpha_i^*) + \sum_{i=1}^{l} z_i(\alpha - \alpha_i^*), \tag{6}$$

subject to $\sum_{i=1}^{l}(\alpha_i - \alpha_i^*) = 0$, where $K(x_i, x_j) = \phi(x_i)^T \phi(x_j)$ is the kernel function.

3.3 Genetic Optimization Model with SVM_AFGA

In the constructed model, the training samples are denoted as $(x_i, y_i)_{i=1}^{N}$, with the inputs represented as x_i and the output denoted as y_i. The formulated mathematical explanation of the dataset is represented as

$$\sum_{i=1}^{L} \beta_i g(w_i x_j + b_i) = y_i, \quad j = 1, \dots, N_i. \tag{7}$$

In Eq. (7), we denote the hidden units as L and the randomly selected input weights as w_i, those have been related to the input and the hidden units, the bias unit is denoted as b_i and β_i, denoted as hidden units toward the output. The perceptron approach is related to the simplest neural network design with the linear equation system of $\mathbf{H}\beta = y$ as

$$H(w_1, \dots, w_L, x_1, \dots, x_N, b_1, \dots, b_L) = \begin{bmatrix} g(w_1 x_1 + b_1) & \cdots & g(w_L x_1 + \mathrm{b}_L) \\ \vdots & \ddots & \vdots \\ g(w_1 x_N + \mathrm{b}_1) & \cdots & g(w_L x_N + b_L) \end{bmatrix}_{N \times L}. \tag{8}$$

In the genetic algorithm, the objective function is optimized with the optimal vector b with the generalized least square function, and the w_L is selected randomly. The GA model as a meta-heuristic algorithm comprises the optimization of the high-dimensional complex problem. To estimate the cyberattacks in the cloud system, the crossing and mutation operation is performed for deriving better solutions. The desired outcome is derived with the fitness function estimation based on the following steps:

1. Initialize the population for cyberattack detection.
2. Evaluate each variable fitness.
3. If goodness is not obtained, compute generation based on the maximal values.
4. Apply cross-over and mutation operation of the variables.
5. Generate new population candidates.

Algorithm 1 SVM_AFGM for cyberattack detection in cloud

```
Input: training dataset $\mathbf{DT} = \{P_i, Y_i\}_{i=1}^{\eta}(P_i \in \Re^n, Y_i \in \gamma)$
  Output: An ensemble algorithm $\mathbb{H}$
  Use 10-fold cross validation resampling technique to generate
training set for (second) level classifier
From $\mathbb{DT}$ split $K$ equal size subsets: $\mathbf{DT} = \{\mathbb{DT}_1, \mathbb{DT}_2, \mathbb{DT}_3, \ldots, \mathbb{DT}_k\}$
    for $k = 1$ to $K$ do
Train the (first) level classifiers
    for $m = 1$ to $M$ do
Train a classifier $\mathbb{C}_{km}$ from
    end for
  Create a training set for (second) level classifier
    for $P_i \in \mathbf{D}$ do, obtain record $\{P_i', Y_i\}$, where
$\mathbf{P}_i' = \{\mathbb{C}_{k1}(P_i), \mathbb{C}_{k2}(P_i), \mathbb{C}_{k3}(P_i), \ldots, \mathbb{C}_{kM}(P_i)\}$
    end for
  end for
  Train (second) level classifier $\mathbb{C}'$ using all sets of $\{P_i', Y_i\}$
  Train (first) level classifiers
    for $m = 1$ to $M$ do
  Train classifier $\mathbb{C}_m$ based on $\mathbb{DT}$
    end for
return $\mathbf{H}(\mathbf{P}) = \mathbb{C}'(\mathbb{C}_1(P), \mathbb{C}_2(P), \mathbb{C}_3(P), \ldots, \mathbb{C}_M(P))$
```

6. Increment the population by 1.
7. Estimate the best possible solution to computed cyberattack in the cloud.

Algorithm 1 for the computation of SVM_AFGM cyberattack prevention in the cloud is presented as follows:

The implemented ACAP and Bayesian network with structures learning reliable malicious and dynamic networks is evaluated for cyberattack detection in the cloud. In Fig. 5, the overall architectural framework for the proposed SVM_AFGA is presented.

The deployment of the proposed SVM_AFGA is implemented with the security module in the cloud for the computation of cyberattacks in the cloud. The estimation is based on the consideration of geo-distribution, latency, awareness, and mobility. Initially, the proposed model involved the computation of the network traffic with integrated choke points, switches, gateways, and routers for the reduction of network traffic overhead for the detection of suspicious activity in the network. The proposed model involves detection and classification of cyberattacks in the cloud. Table 1 presents the number of instances of normal access and cyberattacks.

Based on the obtained instances, we compute the performance of our proposed SVM_AFGA. In our analysis, the normal environment comprises 65% and the cyberattacks comprise 34.9%.

3.4 Experimental Setup

The experimental analysis of the proposed SVM_AFGA for cyberattack detection in the cloud provided significant insights into the performance of the system. The structured learning approach used in this model was shown to be effective in detecting cyberattacks in a cloud

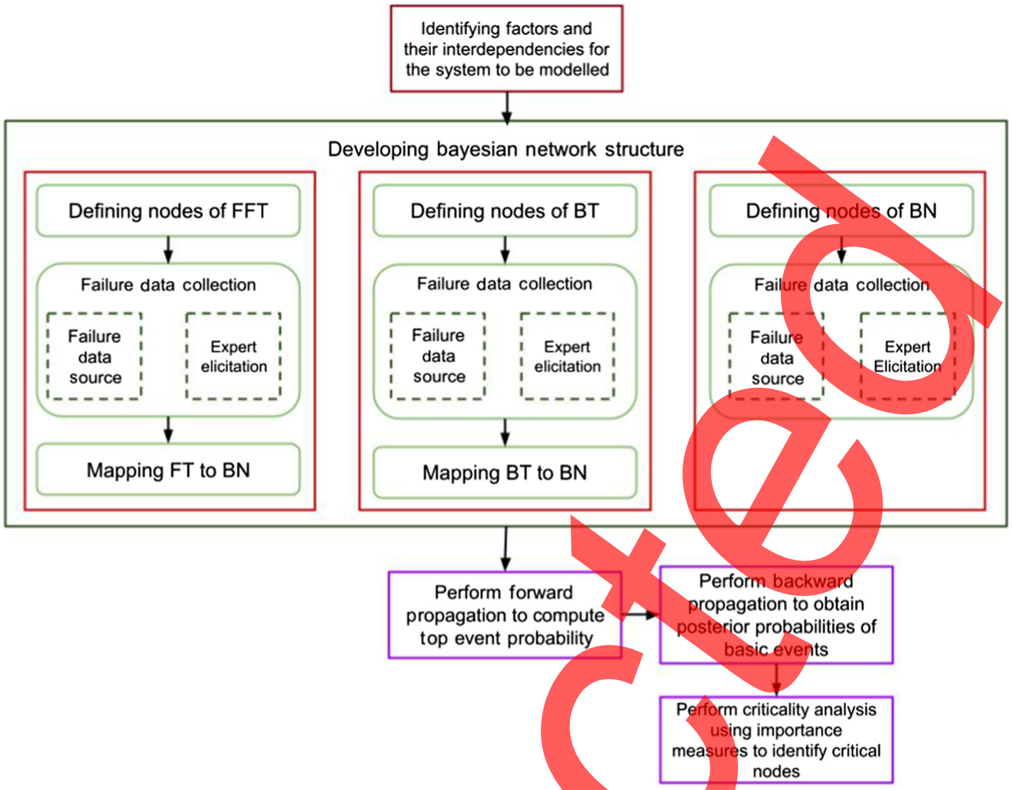
Identifying factors and their interdependencies for the system to be modelled
Developing bayesian network structure
Defining nodes of FFT
Failure data collection
Failure data source
Expert elicitation
Mapping FT to BN
Defining nodes of BT
Failure data collection
Failure data source
Expert elicitation
Mapping BT to BN
Defining nodes of BN
Failure data collection
Failure data source
Expert Elicitation
Perform forward propagation to compute top event probability
Perform backward propagation to obtain posterior probabilities of basic events
Perform criticality analysis using importance measures to identify critical nodes

Fig. 5 Overall framework of the proposed SVM_AFGA.

Table 1 SVM_AFGA instances.

Class category	Overall cases	Rate of recurrence (%)
Normal	3,00,000	65.069
Attack	1,61,043	34.931
Total	4,61,043	100

environment. The use of the Python language and the Scikit-learn library in the simulation environment allowed for accurate and efficient testing of the proposed model. The hardware used for the implementation of the proposed SVM_AFGA is also noteworthy. The use of 4 GB RAM and 2 TB hard disk ensured that the model was capable of handling large volumes of data and processing it quickly. This is particularly important in a cloud environment where data are constantly being processed and analyzed in real time. The experimental analysis also provided valuable results in terms of the accuracy, precision, detection rate (DR), F1_Score, and false alarm of the proposed SVM_AFGA. These metrics were compared with existing techniques, such as SVM-based IDS (SVM-IDS), health-guard, and sparse auto encoder-based IDS (SAE-IDS) to provide a comprehensive analysis of the proposed model's performance.

4 Experimental Results and Discussion

The experimental analysis assessed the proposed SVM_AFGA for cyberattack detection in the cloud. With structured learning, cyberattacks are conducted in the cloud environment. The dataset considered for analysis is evaluated with the Telemetry Data of IoT services (ToN_IoT) dataset. The dataset description is presented in Table 1. We compare the performance of our proposed model with current practical techniques, such as SVM-IDS, health-guard, and SAE-IDS. The performance metrics considered for analysis are accuracy, precision, false alarm rate (FAR), F1_Score, and DR.

Performance Metrics: With the proposed model, the considered evaluation matrices are described as follows:

1. True positive (TP): TP is the total number of cyberattacks in the incoming cases of our proposed model that were accurately categorized as adversarial activity.
2. True negative (TN): TN defines the total number of cases that were detected as normal that were detected as regular activity by the developed model.
3. FP: FP is a normal observation in the incoming observations that is mistakenly categorized as adversarial through the model.
4. False negative (FN): FN is an adversarial observation that is incorrectly detected as normal activity by the model.

Accuracy (AC): AC is the ratio of the properly categorized instances to the total observations in the testing set. The estimation of the classification accuracy is defined as

$$\mathrm{AC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{FN} + \mathrm{TP} + \mathrm{FP} + \mathrm{TN}}. \tag{9}$$

DR: DR is the ratio of the number of adversarial cases detected by the model to the total quantity of adversarial incidents in the testing dataset. The DR or recall is calculated as

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{FN} + \mathrm{TP}}. \tag{10}$$

Precision (PR): PR is the ratio of the number of cases of attacks to the overall cases classified by the model as

$$\mathrm{PR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}. \tag{11}$$

FAR: FAR is the ratio of the normal activity to the total normal instances in the dataset as

$$\mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}}. \tag{12}$$

F1_Score: F1 score is based on the computation of the imbalanced data for computation of the accuracy values as

$$F1 = 2 * \frac{\mathrm{RC} * \mathrm{PR}}{\mathrm{RC} + \mathrm{PR}}. \tag{13}$$

Receiver operating characteristic-area under the curve (ROC-AUC): ROC-AUC is a performance metric used in machine learning to evaluate the quality of a binary classification model. The ROC curve is a plot of the TP rate (TPR) against the FP rate (FPR) at various threshold settings. The TPR is the proportion of actual positives that are correctly identified as such, whereas the FPR is the proportion of actual negatives that are incorrectly identified as positives. The ROC curve allows for visually assessing the trade-off between sensitivity and specificity for different threshold settings.

The proposed SVM_AFGA uses the cloud authentication approach for cyberattack detection and estimation. The analysis uses the ToN_IoT benchmark dataset for the computation of the variables. The developed dataset uses ToN_IoT for two datasets: the training and testing datasets. The training involved the computation of 70% of the random sample population and 30% of the testing performed. The proposed SVM_AFGA uses Python programming in which machine learning is evaluated for the overfitting and underfitting estimation of the variables, which are explained as follows:

1. The decision tree (DT) method uses *random_state* = 0, *max_depth* = 3, *min_samples_leaf* = 1, *criterion* = *gini* and *min_samples_split* = 2
2. The Naïve Bayes (NB) method uses *class_prior* = *None*, *alpha* = 1.0 and *fit_prior* = *True*.
3. The random forest (RF) uses *random_state* = 1, *min_samples_leaf* = 6, *max_depth* = 3, *criterion* = *entropy*, *min_samples_split* = 10 and *n_estimators* = 100
4. The ensemble technique is adjusted as *average_probas* = *False*, *store_train_meta_features* = *False*, *use_clones* = *True*, *use_features_in_secondary* = *False*, *use_probas* = *False*, and *verbose* = 0.

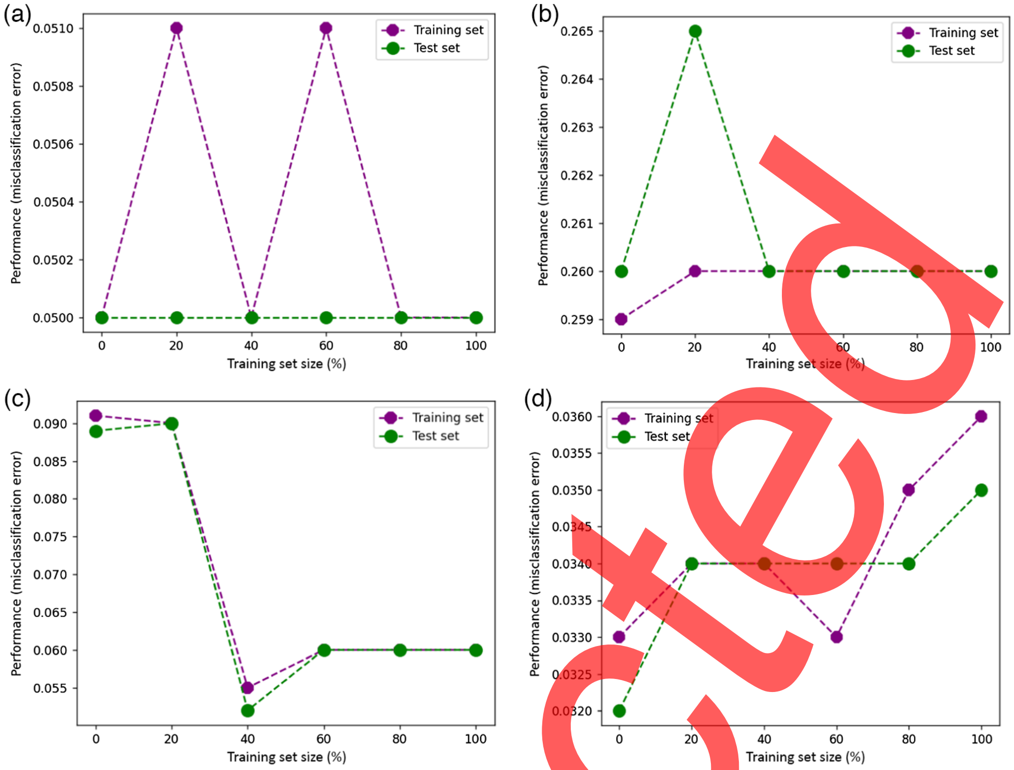

Fig. 6 Misclassification error estimation for (a) DT, (b) NB, (c) RF, and (d) SVM.

Figure 6 shows the misclassification error estimation for different classifiers. The estimation of the misclassification error is comparatively examined for the DT, NB, RF, and SVM. The evaluation shows that the misclassification error is significantly minimal for the SVM. In Fig. 7, the confusion matrix generated for the different classifiers is presented.

With the estimation of the misclassification error and confusion matrix, the classifier performance is evaluated for different classifiers. In Fig. 8, the accuracy of the different classifiers is

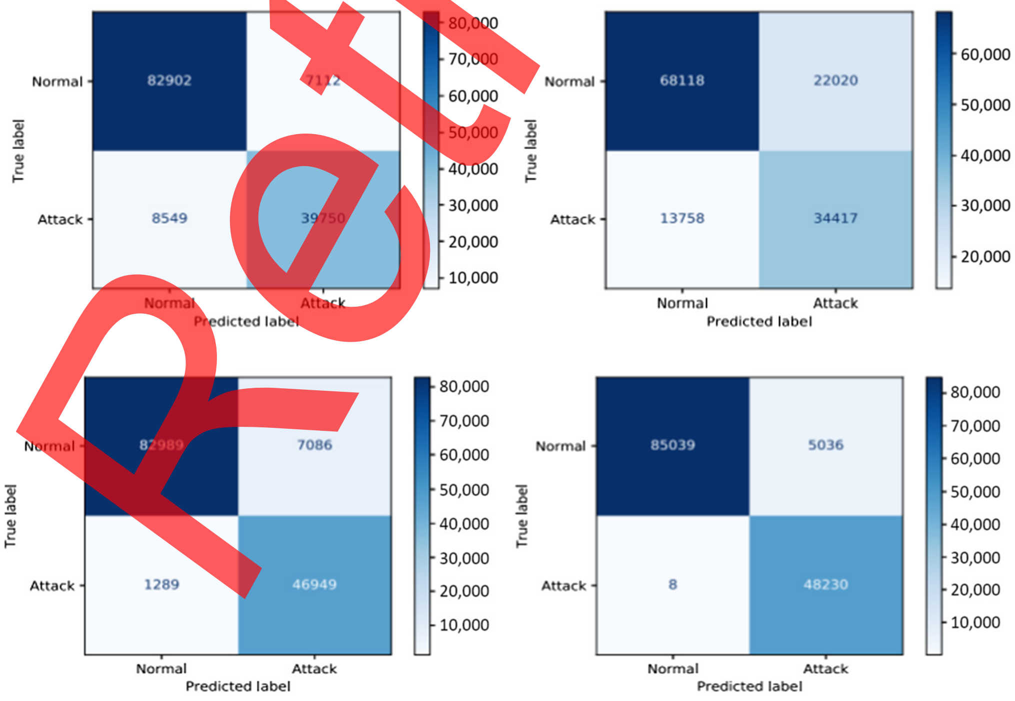

Fig. 7 Confusion matrix for different classifiers.

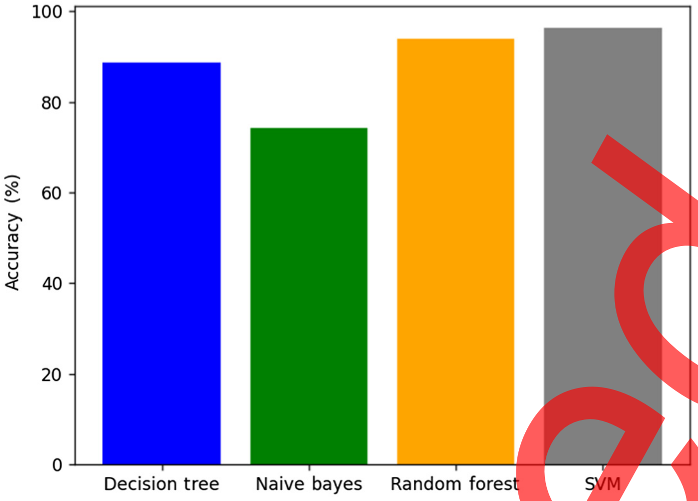

Fig. 8 Comparison of accuracy for different classifiers.

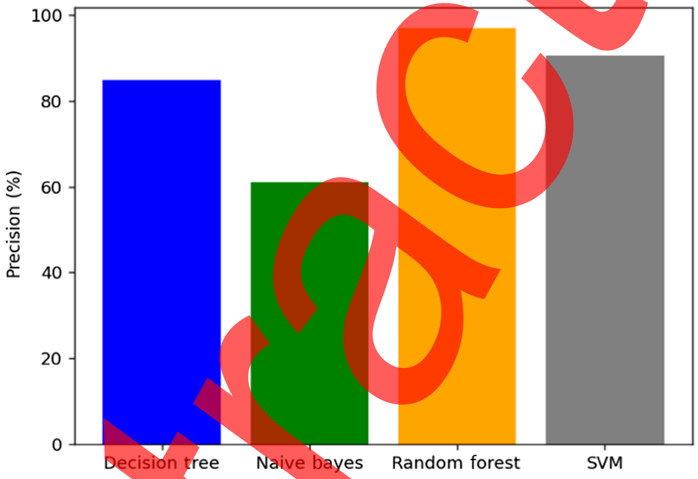

Fig. 9 Comparison of PR for different classifiers.

presented. Also, in Fig. 9, the PR value estimated for the different classifiers is considered. In Figs. 10 and 11, the classifier DRs and F1_Score are presented comparatively for the different classifiers, respectively. The FAR of the different classifiers is presented in Fig. 12.

The performance of the different classifiers is evaluated comparatively with an existing classifier, such as DT, NB, RF, and SVM. The performance analysis shows that the accuracy of the classifier is higher, whereas in an analysis of PR, the RF performance is slightly higher. Similarly, the performance of different classifiers shows that SVM exhibits an improved performance over that of the DT, NB, and RF classifiers. In Figs. 13 and 14, the validation and ROC curves of the different classifiers are presented, respectively.

The analysis of different classifiers showed that the SVM exhibits superior performance, and the proposed SVM_AFGA uses the SVM classifier for cyberattack detection. In Figs. 15 and 16, the accuracy and PR value of the proposed SVM_AFGA with the existing classifiers are presented, respectively.

The performance of the proposed SVM_AFGA for a cyberattack is comparatively examined with the existing classifiers, including SVM_IDS, health_guard, and SAE_IDS. Our experimental analysis shows that our proposed SVM_AFGA presents superior accuracy and PR value compared with the conventional techniques. In Figs. 17 and 18, the DR and F1_Score are presented. Finally, Fig. 19 illustrates the false alarm estimated for the proposed SVM_AFGA.

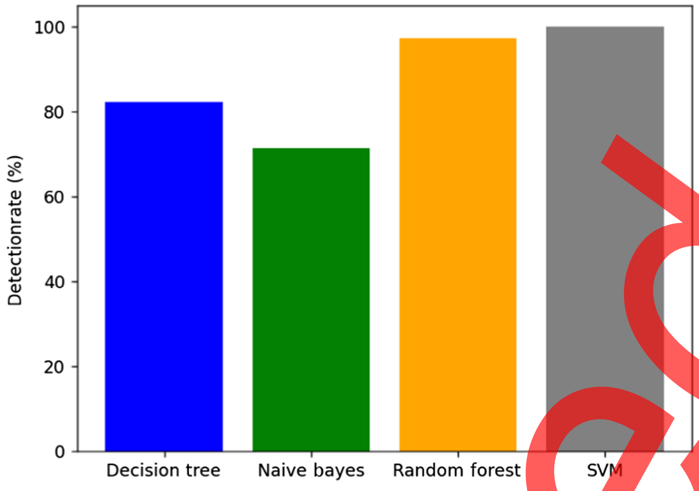

Fig. 10 Comparison of DR for different classifiers.

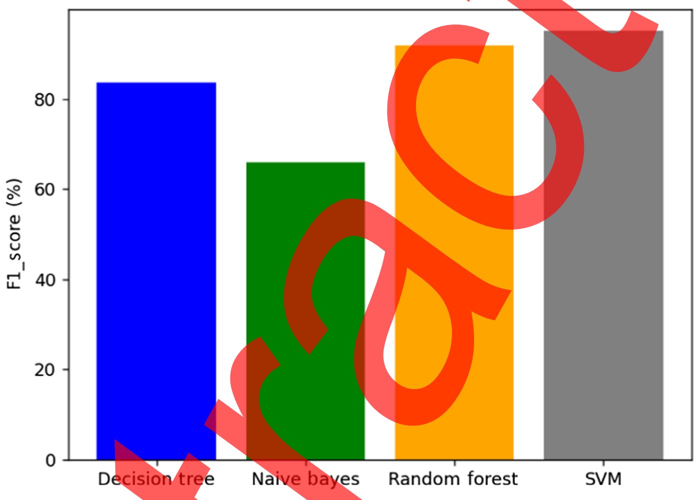

Fig. 11 Comparison of F1_Score for different classifiers.

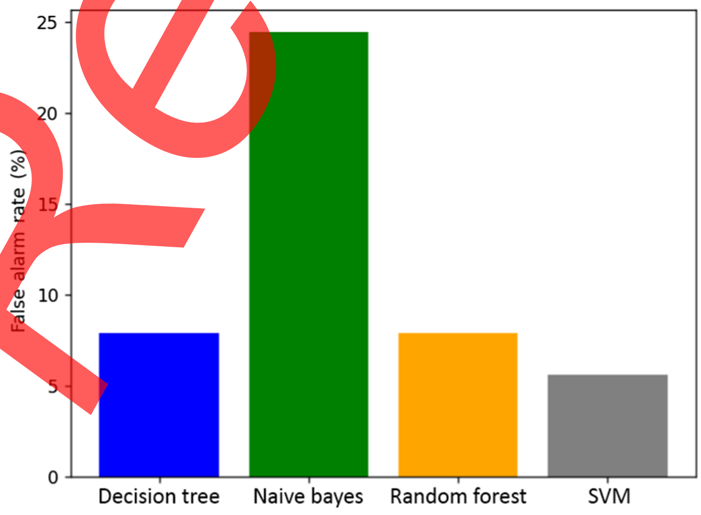

Fig. 12 Comparison of FAR for different classifiers.

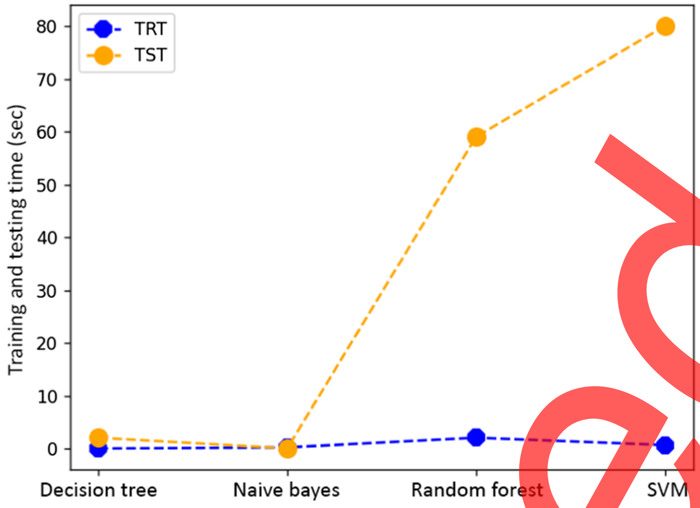

Fig. 13 Comparison of training and testing validation for different classifiers.

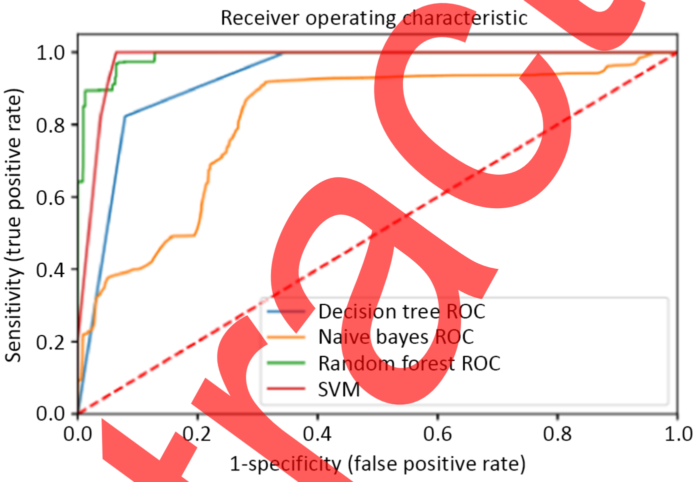

Fig. 14 Comparison of ROC for classifiers.

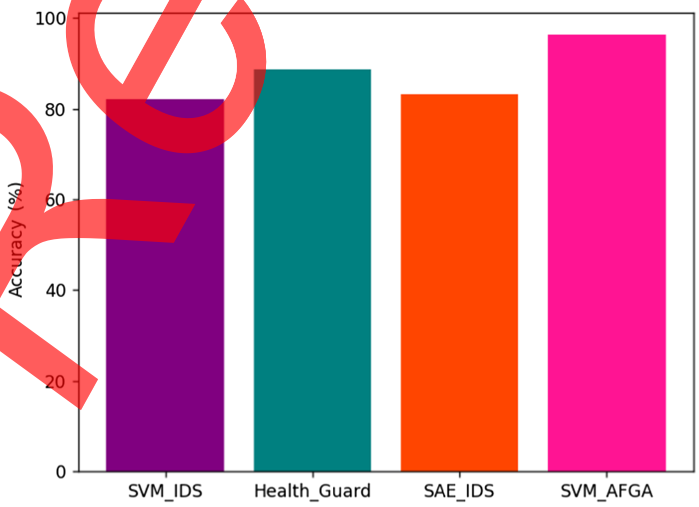

Fig. 15 Comparison of accuracy.

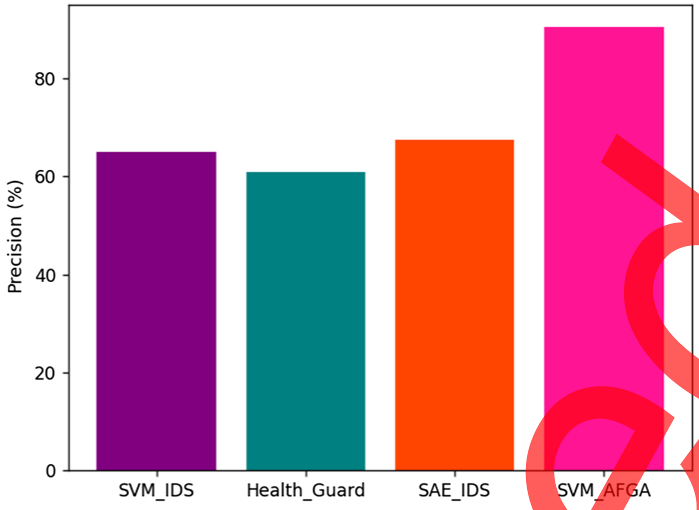

Fig. 16 Comparison of precision.

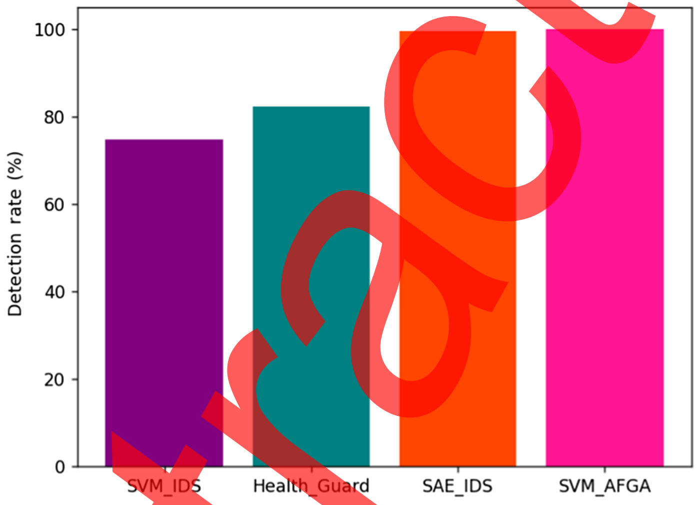

Fig. 17 Comparison of DR.

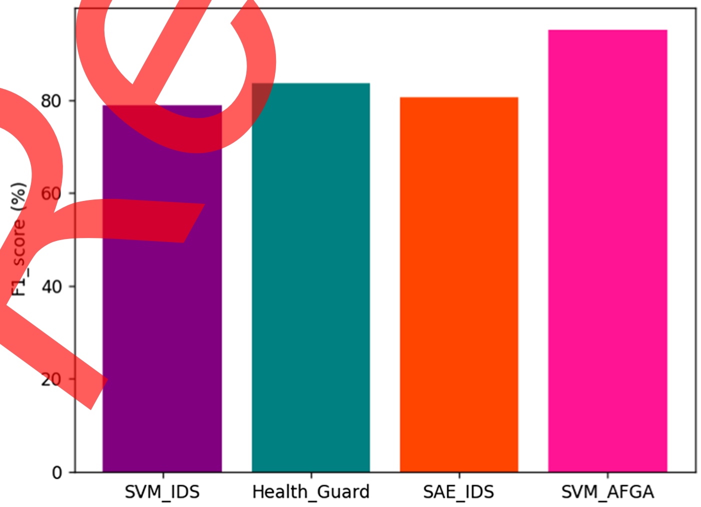

Fig. 18 Comparison of F1_Score.

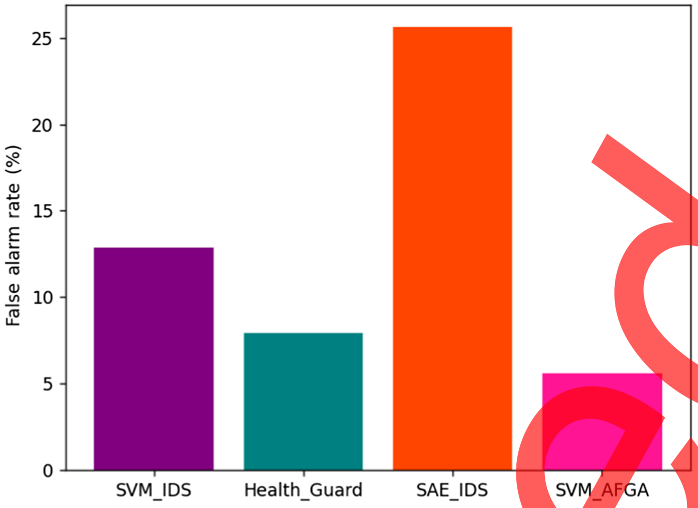

Fig. 19 Comparison of false alarm.

Table 2 Comparison of performance.

Method	Accuracy	Precision	DR	F1_Score	FAR
SVM_IDS	82	64	77	78	13
Health_guard	86	59	84	82	7
SAE_IDS	84	66	97	80	25
SVM_AFGA	96	93	98	94	5

The analysis showed that the proposed SVM_AFGA exhibits higher accuracy, precision, DR, and F1_Score with a reduced FPR. Our performance analysis showed that the performance of the proposed SVM_AFGA is higher than the conventional technique of SVM_IDS, health_guard, and SAE_IDS. In Table 2, the overall summary of the performance of the proposed SVM_AFGA is presented.

The developed SVM_AFGA exhibits ∼8% improvement in accuracy and DR compared with the conventional techniques. The computed F1_Score is increased ∼12%, and the DR significantly increased.

The proposed approach has significance because it responds to the expanding requirement for efficient cyber-security measures in light of an increase in cyberattacks on internet-based technology. The trust model for cyber-security systems may be improved by employing a cloud-based architecture based on the ACAP and a structured machine learning algorithm based on Bayesian networks and ensemble architecture. By establishing guidelines for only accessing online apps at permitted web addresses, the SVM_AFGA integration enhances the model's accuracy even further. The experimental findings show how well the suggested approach works for enhancing the metrics of network efficiency, security, average runtime, accuracy, and median latency.

5 Conclusion and Future Scope

Cyberattacks are an emerging security issue in the CC environment that threatens secure data transmission. This paper developed an SVM_AFGA for cloud architecture integrated with the cloud authentication process. The ACAP model incorporates the trust model for cyberattack detection with a structured learning Bayesian network. The performance analysis stated that the performance of the SVM classifier is effective. Hence, the proposed model uses the SVM classifier model over the adaptive fuzzy system with a genetic algorithm. The simulation performance showed that the proposed model exhibits an improved performance in terms of accuracy and correctness. In addition, the proposed SVM_AFGA's performance reduced the FAR.

Future research on CAPs can explore the integration of advanced authentication methods, such as biometric and behavioral authentication, to enhance the security of cloud-based systems. Biometric authentication can provide a more reliable and secure method of user authentication using unique physical or behavioral characteristics, such as fingerprint recognition, iris scanning, or voice recognition. Behavioral authentication can analyze a user's behavioral patterns, such as typing speed and mouse movements, to identify and authenticate users. Furthermore, the developed model can be extended and evaluated in healthcare data security with multi-user authentication. Healthcare data are sensitive and personal, and it is crucial to ensure their privacy and security. Multi-user authentication can ensure that only authorized personnel are allowed to access and view patient data. In addition, future research can explore the integration of blockchain technology into CAPs to provide a decentralized and tamper-proof authentication mechanism for cloud-based systems.

References

1. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: a survey," *Comput. Sci. Rev.* **33**, 1–48 (2019).
2. Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: a survey," *J. Healthc. Eng.* **2019**, 1–15 (2019).
3. A. Sen and S. Madria, "Application design phase risk assessment framework using cloud security domains," *J. Inf. Security Appl.* **55**, 102617 (2020).
4. M. M. Ahsan et al., "Applications and evaluations of bio-inspired approaches in cloud security: a review," *IEEE Access* **8**, 180799–180814 (2020).
5. A. K. Chitturi and P. Swarnalatha, "Exploration of various cloud security challenges and threats," in *Soft Computing for Problem Solving*, K. Das et al., eds., pp. 891–899, Springer, Singapore (2020).
6. K. Spanaki et al., "Organizational cloud security and control: a proactive approach," *Inf. Technol. People* **32**(3), 516–537 (2019).
7. C. Banse et al., "Cloud property graph: connecting cloud security assessments with static code analysis," in *IEEE 14th Int. Conf. Cloud Comput. (CLOUD)*, September, IEEE, Chicago, Illinois, United States, pp. 13–19 (2021).
8. A. B. Nassif et al., "Machine learning for cloud security: a systematic review," *IEEE Access* **9**, 20717–20735 (2021).
9. K. Muthulakshmia and K. Valarmathib, "Attaining cloud security solution over machine learning techniques," in *Smart Intelligent Computing Communication and Technology*, Vol. 38, p. 246, IOS Press (2021).
10. S. Łaskawiec et al., "Intelligent operator: machine learning based decision support and explainer for human operators and service providers in the fog, cloud and edge networks," *J. Inf. Security Appl.* **56**, 102685 (2021).
11. M. Alsharif and D. B. Rawat, "Study of machine learning for cloud assisted IoT security as a service," *Sensors* **21**(4), 1034 (2021).
12. Z. Chkirbene et al., "Cooperative machine learning techniques for cloud intrusion detection," in *Int. Wirel. Commun. and Mobile Comput. (IWCMC)*, June, IEEE, pp. 837–842 (2021).
13. A. Mondal and R. T. Goswami, "Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security," *Microprocess. Microsyst.* **81**, 103719 (2021).
14. A. K. Singh and D. Saxena, "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment," *J. Appl. Security Res.* **17**(3), 1–24 (2021).
15. M. Waqas et al., "Botnet attack detection in Internet of Things devices over cloud environment via machine learning," *Concurr. Computat. Pract. Exp.* **34**(4), e6662 (2021).
16. M. Li et al., "Distributed machine learning load balancing strategy in cloud computing services," *Wirel. Netw.* **26**(8), 5517–5533 (2020).
17. H. Abroshan, "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms," *Int. J. Adv. Comput. Sci. Appl.* **12**(6), 31–37 (2021).
18. P. Velmurugadass et al., "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today: Proc.* **37**, 2653–2659 (2021).
19. P. Chinnasamy et al., "Efficient data security using hybrid cryptography on cloud computing," in *Inventive Communication and Computational Technologies*, G. Ranganathan, J. Chen, and Á. Rocha, eds., pp. 537–547, Springer, Singapore (2021).

20. S. K. Singh, P. K. Manjhi, and R. K. Tiwari, “Cloud computing security using blockchain technology,” in *Transforming Cybersecurity Solutions using Blockchain*, R. Agrawal and N. Gupta, eds., pp. 19–30, Springer, Singapore (2021).
21. F. Thabit et al., “A new lightweight cryptographic algorithm for enhancing data security in cloud computing,” *Glob. Transit. Proc.* **2**(1), 91–99 (2021).
22. S. S. Vellela and R. Balamanigandan, “Design of hybrid authentication protocol for high secure applications in cloud environments,” in *Int. Conf. Autom., Comput. and Renew. Syst. (ICACRS)*, IEEE, Pudukkottai, Tamil Nadu, India, pp. 408–414 (2022).
23. D. Rangwani and H. Om, “A secure user authentication protocol based on ECC for cloud computing environment,” *Arab. J. Sci. Eng.* **46**, 3865–3888 (2021).
24. T. Y. Wu et al., “Rotating behind security: a lightweight authentication protocol based on IoT-enabled cloud computing environments,” *Sensors* **22**(10), 3858 (2022).
25. S. Shukla and S. J. Patel, “A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing,” *Computing* **104**(5), 1173–1202 (2022).
26. M. Shabaz, “A secure two-factor authentication framework in cloud computing,” *Security Commun. Netw.* **2022**, 1–9 (2022).
27. A. Irshad et al., “A novel pairing-free lightweight authentication protocol for mobile cloud computing framework,” *IEEE Syst. J.* **15**(3), 3664–3672 (2020).
28. K. Sundar, S. Sasikumar, and C. Jayakumar, “Enhanced cloud security model using QKDP (ECSM-QKDP) for advanced data security over cloud,” *Quantum Inf. Process.* **21**(3), 115 (2022).
29. T. F. Lee et al., “Lightweight cloud computing-based RFID authentication protocols using PUF for e-Healthcare systems,” *IEEE Sens. J.* **23**(6), 6338–6349 (2023).
30. Y. Xu et al., “C-FDRL: context-aware privacy-preserving offloading through federated deep reinforcement learning in cloud-enabled IoT,” *IEEE Trans. Ind. Inf.* **19**(2), 1155–1164 (2023).
31. O. P. Singh and A. K. Singh, “Data hiding in encryption–compression domain,” *Complex Intell. Syst.* **3**(1), 1–14 (2021).
32. A. K. Singh and M. Elhoseny, eds., *Intelligent Data Security Solutions for e-Health Applications*, Academic Press (2020).
33. A. K. Singh et al., “A survey on healthcare data: a security perspective,” *ACM Trans. Multimedia Comput. Commun. Appl.* **17**(2s), 1–26 (2021).
34. U. P. Rao et al., eds., *Blockchain for Information Security and Privacy*, CRC Press (2021).
35. P. K. Shukla et al., “Design, architecture, and security issues in wireless sensor networks,” in *Next Generation Wireless Network Security and Privacy*, pp. 211–237, IGI Global (2015).
36. R. K. Gupta et al., “An improved secure key generation using enhanced identity-based encryption for cloud computing in large-scale 5G,” *Wireless Commun. Mobile Comput.* **2022**, 1–14 (2022).
37. A. Aldaej et al., “Smart cybersecurity framework for IoT-empowered drones: machine learning perspective,” *Sensors* **22**(7), 2630 (2022).
38. D. A. Parwani et al., “Various techniques of DDoS attacks detection & prevention at cloud: a survey,” *Orient. J. Comput. Sci. Technol.* **8**(2), 110–120 (2015).
39. A. E. Hassanien et al., eds., *Security in Smart Cities: Models, Applications, and Challenges*, Springer International Publishing (2019).
40. A. K. Singh, M. Dave, and A. Mohan, “Wavelet based image watermarking: futuristic concepts in information security,” *Proc. Natl. Acad. Sci. India Sec. A: Phys. Sci.* **84**, 345–359 (2014).
41. T. A. Ahanger et al., “Securing consumer internet of things for botnet attacks: deep learning approach,” *CMC-Comput. Mater. Continua* **73**(2), 3199–3217 (2022).
42. Z. Lv, A. K. Singh, and J. Li, “Deep learning for security problems in 5G heterogeneous networks,” *IEEE Netw.* **35**(2), 67–73 (2021).
43. Z. Lv et al., “Trustworthiness in industrial IoT systems based on artificial intelligence,” *IEEE Trans. Ind. Inf.* **17**(2), 1496–1504 (2020).
44. A. Aljumah, T. A. Ahanger, and I. Ullah, “Heterogeneous blockchain-based secure framework for UAV data,” *Mathematics* **11**(6), 1348 (2023).

Hatim Alsuwat is an assistant professor of Computer Science in the College of Computers and Information Systems at Umm Al-Qura University. He received his PhD from the Department of Computer Science and Engineering at the University of South Carolina (USC) in 2019. His research interests include information security, cryptography, model drift, and secure database systems.