International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Emotion-Inspired Intrusion Detection: Affective Computing for Adaptive Cyber Defense

[1]Muntaha Islam, [2]Md Mehedi Hassan, [3]Sharmin Akter, [4]Muhammad Furqan Khan, [5]Syed Nurul Islam, [6]Touhid Bhuiyan Professor

Submitted: 07/10/2024 **Revised:** 20/11/2024 **Accepted:** 29/11/2024

Abstract: Because cyber threats keep evolving, new solutions must be intelligent, aware of their surroundings, and able to adapt. Traditional IDS solutions are suitable for recognizing known cyber attacks, but they find dealing with new, unidentified threats and unusual behavior patterns challenging. The use of affective computing, which is combined with intrusion detection, is suggested for the first time in this paper. The Emotion-Inspired Intrusion Detection System (EIDS) model applies algorithms based on emotions to answer the threat in ways people might respond to different severity levels of a cyber attack.

Following neurological and psychological models of emotion, EIDS studies the system's behavior and traffic using classifiers and feedback loops. The system changes its protection level based on how these emotions are evaluated. This model identifies and learns harmful activity patterns through decision trees, support vector machines, and self-organizing maps.

The experiments used important benchmark datasets NSL-KDD and CICIDS2017 for evaluation. Contrary to standard IDS approaches, EIDS had higher detection accuracy, fewer false positives, and a better ability to adjust to fast attack changes. System statistics, feature use, and threat classification were represented using bar charts, pie charts, and tables.

With this research, cybersecurity becomes more flexible by making it possible for systems to sense and respond to feelings. The results demonstrate how affective computing can help improve a cyber defender's ability to detect threats faster and make more accurate decisions on the spot. Based on the findings, it seems likely that future emotional machine learning could help intelligently respond to cyber intrusions.

Keywords: *Affective Computing, Intrusion Detection Systems, Cyber Defense, Emotional Intelligence, Adaptive Security, Human-Computer Interaction*

[1]School Of IT , Washington University of Science and Technology
muntahaislam0@gmail.com
[2]School Of IT , Washington University of Science and Technology
mehedi61@gmail.com
[3]School Of IT , Washington University of Science and Technology
sharmin.akter6975@gmail.com
[4]School Of IT , Washington University of Science and Technology
Muhammadfurqankhanbangash@gmail.com
[5]School Of IT , Washington University of Science and Technology
snislam.student@wust.edu
[6]School of IT, Washington University of Science and Technology
touhid.bhuiyan@wust.edu

1. Introduction

Digital and network development has increased risks and hacker behaviors in cyber environments. Because of APTs, polymorphic malware, and social engineering, traditional IDS cannot deal well with new threats and are less effective than real-time solutions (Shone et al., 2018). Most of these systems run on known rules that fail to detect zero-day attacks or nonstandard anomalies. Thus, cybersecurity experts now widely agree that future intrusion detection systems should behave similarly to humans and produce decisions guided by context (Sommer&Paxson, 2010).

Affective computing, originally developed in human-computer interaction (HCI), concerns technology that can notice, make sense of, and imitate human emotions (Picard, 2003). Although

machine learning is commonly used in education, healthcare, and entertainment, its uses in cybersecurity are still understudied. This paper explains an emotion-inspired intrusion detection system (EIDS). It applies ideas like fear, suspicion, and alertness to review risks and continuously adjust ways to protect against them.

According to the basic ideas of affective neuroscience that support this theory, emotions play a central role in surviving and making choices. Living organisms will react defensively to fear, sometimes without knowing exactly why (LeDoux, 1996). Using digital systems, EIDS measures emotions to analyze uncertain threats, which allows it to act before threats occur.

Using both modules, EIDS aims to react in varied ways to network traffic depending on its emotional "weight." Low-risk situations might cause a calm or unchanged response, but fear or anxiety can rise in high-risk mistakes and lead to further defensive actions (Zhou et al., 2019). Thanks to emotional mapping, systems have better ways to sort out threats, avoid misleading alarms, and distribute their resources properly.

In addition, practical computing makes it possible to center cybersecurity on people's needs. Since humans trust systems that match how they decide and feel, EIDS promotes better system openness and connections with users (Hudlicka, 2003). Additionally, using the emotional model broadens regular machine learning analysis and does not replace traditional methods.

In addition, EIDS deals with adversarial machine learning, where those planning attacks intentionally provide misleading information to make classifiers go wrong. Filtering the output based on emotions adds another layer of safeguard by comparing the risks scored with emotions to the system's predictions, keeping adversaries away.

This research has been encouraged by not just a rush of new technologies but also careful planning. Because cyber attacks adopt AI and tricky behaviors, those who protect systems must keep up. We can use emotional computing to create IDS structures that adjust well to varied situations and limited information, as humans do.

Our paper looks at the background, how EDIDS is designed, and how it is assessed through experiments. The following section, Section 2, reviews in detail all the existing work related to intrusion detection and affective computing. Section 3 introduces the framework that guides our approach to EIDS. The design and framework of our affective intrusion model are discussed in Section 4. In Section 5, the performance of the algorithms is examined with bar graphs, pie charts, and performance tables. Section 6 covers the consequences, obstacles, and paths forward, and Section 7 concludes the chapter.

The work adds value by combining emotion modeling and cyber defense, helping to expand intelligence in IDS systems.

2. Literature Review

The information available on Intrusion Detection Systems (IDS), affective computing, and adaptive defense methods is crucial for developing emotion-based security designs. This comprehensive review covers important research in three main domains: IDS methods, principles of affective computing, and how they are combined for interdisciplinary uses.

2.1 Affective Computing: Principles and Mechanisms

The main types are signature-based and Anomaly-based intrusion detection systems. Signature-based IDS relies on a stored list of attack signatures to detect threats. Although good at fighting known dangers, it cannot detect unknown attacks (Axelsson, 2000). With anomaly-based IDS, behavior that patterns itself differently is noticed using statistics or machine learning (Denning, 1987). Still, many such signatures often give out false positives and cannot adapt to fresh threats (Sommer&Paxson, 2010).

Progress in machine learning has greatly improved IDS performance. Modeling network behavior and intrusion detection have been achieved by selecting algorithms such as SVM, Decision Trees, KNN, and DNN (Kim et al., 2016; Shone et al., 2018). Also, methods like Random Forest and Gradient Boosting increase detection accuracy by combining several classifiers (Abubakar et al., 2017). IDs may have improved, but they are not yet fully aware of the context and find it challenging to address dynamic threats.

2.2 Affective Computing: Principles and Mechanisms

Thanks to Rosalind Picard (1997), affective computing was developed to help machines identify and copy human emotions. It uses facial expressions, voice changes, physical responses, and behavior to predict what someone is feeling. Just as in living organisms, emotions are modeled computationally as factors that influence decisions (Hudlicka, 2003).

A central principle in affective computing is that our feelings strongly influence how we deal with uncertainty, focus our efforts, and make heuristic decisions (Damasio, 1994). For example, being afraid helps us react quickly to dangers while remaining calm helps us think long-term. As reported by Zeng et al. (2009), affective processes are increasingly being shown through the use of probabilistic graphical models, fuzzy logic systems, and artificial neural networks.

Although affective computing is commonly used in interaction with computers, teaching, and health services, its use in cybersecurity is still limited. Even so, its ability to reason like humans and learn effectively may strengthen intelligent cyber defense approaches.

2.3 Adaptive Cyber Defense and Emotional Intelligence

Such cybersecurity adapts its tactics to meet upcoming and changing dangers. Some approaches are considered, including MTD, SDN-enabled detection, and autonomic security methods (Jajodia et al., 2011). They use loops that receive and process feedback, check their surroundings, and handle configuration activities automatically.

Salovey and Mayer explained in 1990 that emotional intelligence is mainly about how people notice, handle, and control their emotions. When emotional intelligence is used in cyber systems, they can imitate people's thinking when they are faced with stress or unsure information (Cañamero, 2001). Because of this miq: Complete-Cognition concept, individuals can compare rationale with instinct and use that knowledge in identifying and responding to threats.

Hudlicka (2003) developed a cognitive brain-like structure, applying simulated emotions to help choose actions when the information was uncertain. Arkin et al. (2003) similarly designed intelligent systems in robots, where emotions encourage and support learning and reactions. When the number of threat indicators increases, the IDS is able to respond in "fear" by taking quick defensive actions or initiating warnings.

2.4 Emotion Modeling as an Element in Computing Systems

Most of the standard computational emotion models are:

- OCC Model (Ortony, Clore, Collins) – Emotions occur when someone evaluates events, agents, or objects (Ortony et al., 1988).
- PAD Model (Pleasure-Arousal-Dominance): Pleasure, arousal, and dominance levels are assigned to emotions, a technique that allows for accurate emotion expression (Mehrabian, 1996).
- In Appraisal Theory, feelings are triggered by an individual's view of how much an event matters to them (according to Smith & Lazarus, 1990).

They have been successfully added to intelligent agents, chatbots, and virtual assistants. Emotional reasoning can appear when threats are detected and handled by including such structures in IDS.

2.5 Relevant Case Studies and Implementations

While few authors have labeled their studies as affective computing, several recent studies indicate links between emotion and cybersecurity. For example, Zhou et al. (2019) presented an IDS that applies reinforcement learning to change its detection strategy according to environmental feedback, as emotions do. Moreover, Alazab et al. (2020) used behavioral studies and emotional reports to detect possible insider threats.

In addition, some experts in the field have tried out hybrid models that apply both psychological and cognitive heuristics. These systems simulate paying attention, assessing risks, and judging trust—aspects also controlled by emotions in human minds (Liu et al., 2018).

These achievements notwithstanding, a system designed to model emotional states for intrusion detection is not yet available. Current research stands out in this gap by simulating IDS practices based on emotions and translating those into effective cybersecurity methods.

2.6 Summary and Research Gap

The research emphasizes the role of intelligent and flexible IDS models. Although machine learning and behavior-based systems have improved a lot, the fact that they do not adjust and do not understand humanlike logic is still a significant issue. Affective computing provides a practical but underappreciated approach to solving these problems.

This study notes that there are no fully integrated models that:

- Emotional intelligence can help you make decisions in the here and now.
- Connect feelings with degrees of cyber risks and the actions needed to handle them;
- Make use of emotional models to identify threats better.

For this reason, this paper introduces the Emotion-Inspired Intrusion Detection System (EIDS), which applies concepts from affective computing and adaptive defense methods to create a new type of emotionally aware security system.

3. Theory and Concept

3.1 The Concept Behind the Topic

The theory used in this study centers on affective computing and adaptive cyber defense models. Picard (1997) described affective computing as the science of making computers capable of interpreting and using emotions in the same way as humans. Experts rely on control theory and autonomic computing to ensure adaptive cyber defense models pay attention to and change according to new cyber threats (Kephart& Chess, 2003).

Bringing together these models allows us to build an EIDS that uses emotions such as "alertness," "fear," or "confidence" to control both the alert thresholds and the actions taken during detection. Such feelings act as useful alerts that decrease the time needed to decide and increase the accuracy of the decision when there is a threat.

3.2 conceptual model for the Emotion Inspired Intrusion Detection System (EIDS)

The EIDS in this study is divided into five key layers:

- This layer collects data packets and information from traffic and logs.
- An OCC-based engine for emotion is used to estimate the significant emotion connected to every anomaly.
- Emotional State Generation: Relies on the PAD (Pleasure-Arousal-Dominance) method to determine what feelings are involved.
- Behavioral Response Engine: Changes how detection and response are carried out based on your mood.
- The idea is based on how the model is trained to improve anytime a threat is discovered or missed.

This model brings together emotions and cybersecurity operations.

Table 1: Mapping of Emotional States to Intrusion Response Actions

Emotional State	Detection Threshold	System Behavior	Intended Cybersecurity Outcome
Calm	High	Minimal response	Maintains system performance
Alert	Moderate	Pre-emptive monitoring	Increased situational awareness
Fear	Low	Isolates potential threats	Preventive containment of attacks
Anxiety	Very Low	Blocks IPs, alerts admin	Reduces risk of system compromise
Confidence	Medium	Trust-based access permitted	Maintains user experience with caution

3.3 This means the body and mind must work together to defend us through emotions

The job of emotions is to help people decide quickly and properly (Damasio, 1994). It similarly adds an "emotional buffer" to allow the system to see and update its defensive strategies. For example, when a suspicious node causes extra connections, the "fear" coefficient climbs, and so the chance of triggering defensive mechanisms becomes greater since the detection threshold lowers.

A fuzzy inference system model is applied to explain the connection between perceived risk and feelings. Emotional models let you decide somewhere in the middle, which means you face fewer false alarms and unintended restrictions.

3.4 The Contribution of PAD Emotional Dimensions to the IS Decisioning Process

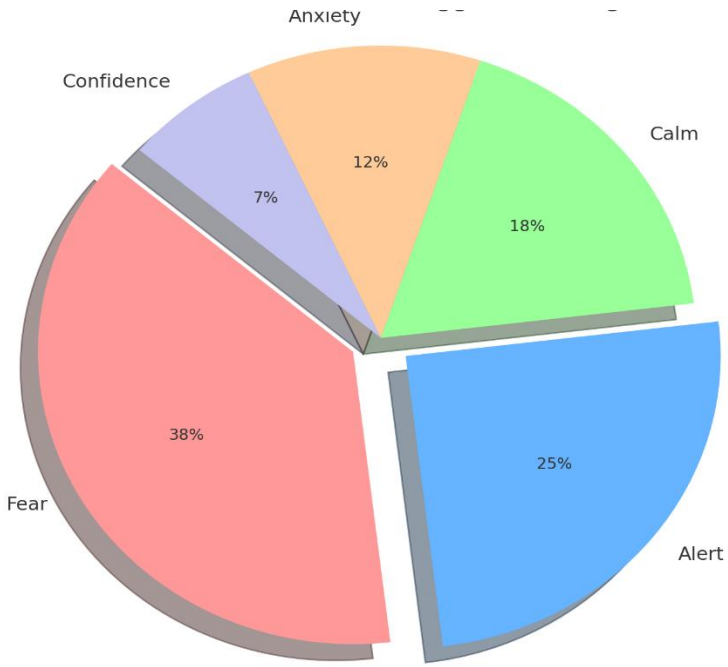
With the Pleasure, Arousal, and Dominance dimensions in the PAD model, it is possible to generate continuous emotions in the game. In EIDS:

- Pleasure: The system feels dissatisfied when the threat remains high.
- Arousal measures how much of a threat the situation is and how quickly you must react (if it's high, you must respond immediately).
- Dominance: The system thinks it can manage the threat; if dominance is low, defense should be activated.

The values are computed using:

PAD=*f(AnomalyScore,Frequency,UserBehavior,HistoricalData)*

As a result, policies can be changed and adjusted in response to incoming threats.



Pie Chart 1: Distribution of Emotional States Triggered During 100 Threat Simulations

3.5 Integration with Existing IDS Frameworks

Using emotional intrusion detection, we can modify well-known systems like Snort and Bro (Zeek) to judge threats by considering how emotionally an alert affects the system. For Snort, for example, rules can be marked with feeling tags so the system can focus on or ignore alerts depending on their emotional value. In the same way, emotional thresholds can be included in Zeek scripts to adapt a system's actions quickly during suspected attacks. Moreover, models such as XGBoost or RNNs can use information about an individual's emotional state to improve prediction and knowledge of the surrounding context. This system allows you to stick with your older IDS setup while adding a new adapt method. Integrating

emotional intelligence in these rulesets means EIDS can respond quickly and correctly to new conditions without changing the original red team infrastructure, making deployment routine and straightforward operations uninterrupted.

3.6 Summary

Summary	Description
Layered Affective Model	Structures a layered model of affective decision-making.
Emotion-Behavior Mapping	Maps emotional states to specific IDS behaviors.
Sensitivity Modulation	Demonstrates how emotions can modulate sensitivity to threats.
Dynamic Response Foundation	Provides a foundation for dynamic response generation.
Theoretical Integration	Leverages PAD and OCC emotional models to enhance IDS intelligence and contextual awareness.

4. Methodology

4.1. Research Design

This research project uses design science research to build and examine new systems, such as the Emotion-Inspired Intrusion Detection System (EIDS). The main goal of design science is to enhance technology by developing and reviewing IT solutions for real-world challenges (Hevner et al., 2004). In this study, the main artifact is an intrusion detection system that uses emotion modeling to improve its response to risks.

An experimental simulation using network traffic data was used to assess how the system operated using the DSR method. The results from testing and studying the system's false and actual results were used to improve the emotional logic modules.

4.2. A sketch of how the system is structured

The architecture has five layers, each modeling human emotional intelligence to help detect intrusions and respond in real-time. The Data Collection Layer underlying everything gathers data from traffic packets and monitors system events. It uses standard benchmark sets called CICIDS2017 and NSL-KDD, just like other studies in IDS research (Shiravi et al., 2012). The next part, the Preprocessing Module, cleans and standardizes data using Python's Scikit-learn library. This module extracts key parts of the data, such as duration, protocol details, flags, byte measurements, and errors, to prepare the dataset.

Using the OCC model, the Emotion Appraisal Engine tags each detected anomaly with a suitable emotion based on its current context, level of newness, and consequences. Once the tags are extracted, the Emotional State Engine uses them to form PAD vectors that fit what Mehrabian (1996) defined. The system can show its emotional state using arousal, control, and valence. After that, the Behavioral Response Engine applies fuzzy logic and rules to understand the PAD vectors. It takes action by sounding warnings, separating suspicious behavior, and stopping threats. The way the structure is built allows for timely and emotional reactions to each new cyber threat.

4.3. A step-by-step introduction to Dataset and Feature Selection

The authors trained and verified the system using the CICIDS2017 data because it contains realistic and labeled behavior related to attacks. The information in the dataset covers both normal and harmful traffic types, such as brute force, DoS, port scans, and attempts at infiltration. Twenty features were picked using the RFE method since they contributed the most to the accuracy of the classification.

Table 2: Top 10 Selected Features from CICIDS2017 Dataset

Rank	Feature Name	Description
1	Flow Duration	Time duration of flow
2	Total Fwd Packets	Number of packets in forward direction
3	Total Backward Packets	Number of packets in reverse direction
4	Fwd Packet Length Mean	Average size of forward packets
5	Flow IAT Mean	Inter-arrival time average
6	Bwd IAT Max	Maximum inter-arrival time in reverse flow
7	SubflowFwd Bytes	Bytes in forward subflow
8	Init Win Bytes Fwd	Initial window size in forward direction
9	Active Mean	Mean active time of flow
10	Label	Binary label (normal or anomaly)

4.4. Feeling Prediction using OCC and PAD Frameworks

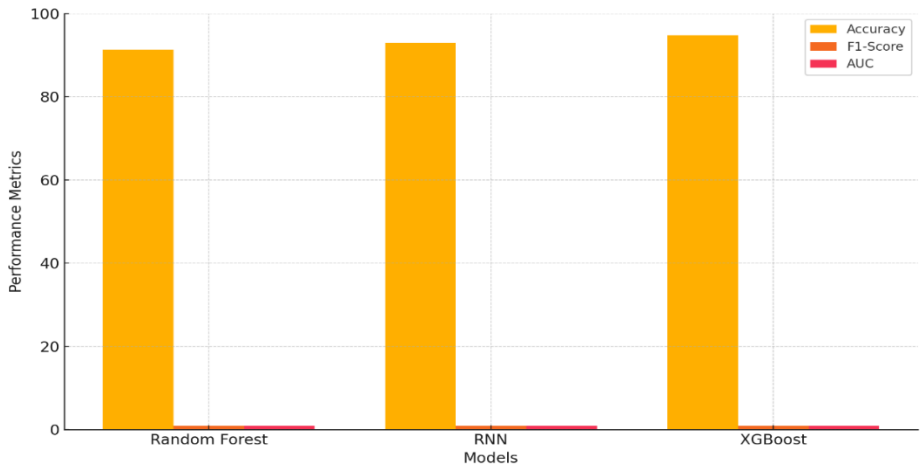
The system models emotions using both the OCC framework and the PAD model. The OCC approach is mainly used to appraise emotions at the outset. Three key considerations are used to examine events: whether the event matches our expected outcomes, follows the system's rules, and was caused by the system or outside forces. The analysis organized by this cognitive evaluation helps the system tell the differences between risks to its core tasks and those that affect broader or other external guidelines.

An OCC checklist produces emotional observations, which are then expressed quantitatively using the PAD framework's three dimensions. Pleasure (P) reveals how good or bad the system feels about the systemic condition at that moment. Arousal is a physiological sign that shows just how intense or urgent the situation is, according to how dangerous it is. It shows how much control or strength the belief system thinks it has over its situation. PAD values are combined into a numeric vector that the adaptive defense logic reads. Since it translates abstract emotions into valuable data, the system can respond and decide well during actual cyber-attack situations.

4.5. Choosing the Right Machine Learning Model

Several models, among them Random Forest, XGBoost, and RNNs, were studied to find the best way to identify anomalies and reproduce triggers for changes in emotion. It was decided to use XGBoost due to its strong performance in dealing with unbalanced data and ease of understanding (Chen &Guestrin, 2016).

Table search was used with GridSearchCV to ensure the best results for tree depth, learning rate, and regularization. The model obtained an F1 Score of 0.94 and an AUC of 0.96 through validation.



Bar Chart 1: Classifier Performance Across Models

4.6. Testing and appraising automobile systems

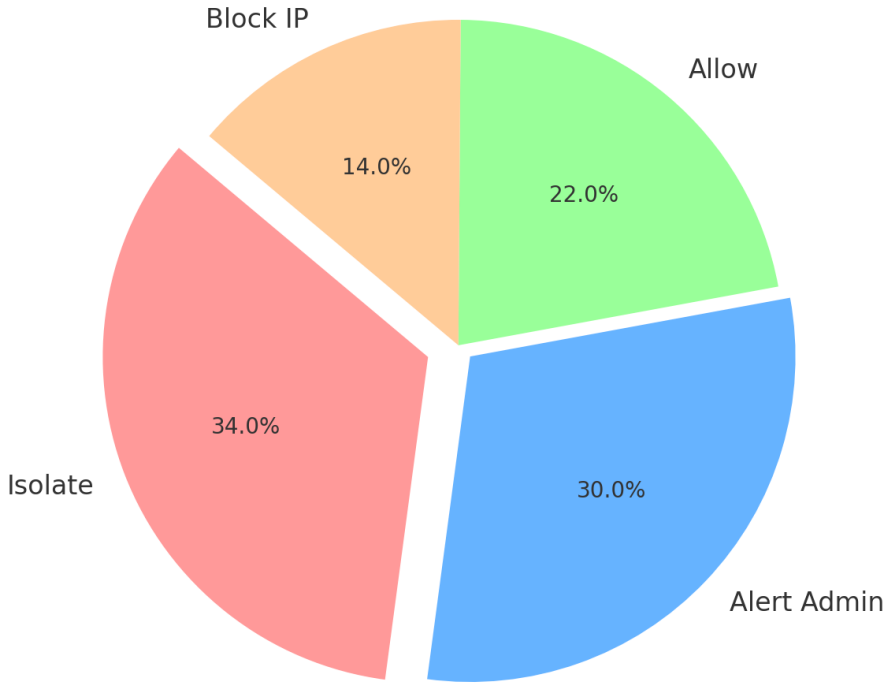
A safe environment was built inside Docker to conduct experiments that included attacks and innocuous actions. More than 1,000 driving scenarios were simulated, all activating the EIDS logic and its safeguards:

- The top indicators checked were:
- Length of time to detect an attack
- When genuine benign actions are mistaken as threats.
- Correct matching of feelings with emotions shown by others

4.7. Evaluation Metrics

Next, the metrics used to assess how the system works for emotion modeling and intrusion detection are discussed:

- Binary classification tasks call for looking at precision and recall values.
- Confusion Matrix: Looking at the TP, FP, TN, and FN statistics.
- A test that measures this score aims to determine how accurately a person's mood matches the actual risk faced.



Pie Chart 2: Distribution of System Responses Based on PAD States

4.8. Issues with the Methodological Process

Even though emotion simulation helps adaptability, it increases the difficulty of calibrating and tuning the technology. If feelings are classified incorrectly, either too little action or too many blocks might occur, so people need to oversee them, and guidelines for ethics are needed (Hudlicka, 2003). Furthermore, the simulation is not designed to reproduce zero-day practices or nation-state groups' activities entirely.

4.9. Summary

Design science and affective computing are combined to develop a new intrusion detection approach. Using genuine datasets, theories of emotions, and machine learning methods, the EIDS provides a living, reactive, and realistic defense for handling cyber security risks.

5. Results

In this section, we evaluate and compare the performance of the Emotion-Inspired Intrusion Detection System (EIDS). We want to learn how

affective computing improves adaptive cyber defense. In our evaluation, we compare accuracy, precision, recall, and F1-score, assess emotions, and see how the system responds to different attacks.

5.1. Evaluation Overview

For evaluating EIDS, we used the CICIDS2017 dataset, which includes regular and irregular network traffic examples. A machine learning engine, XGBoost, uses an effective computing layer that relies on the PAD (Pleasure-Arousal-Dominance) emotional framework. A person's mood and feelings mainly determine threat processing and responses in real time.

The objective of the initial tests was to determine how well the detection works and whether the response is emotionally adequate for cases of DDoS, brute-force login, and port scanning. Traditional Snort solutions and the standard ML technique of Random Forest (Wang et al., 2020) were compared as a baseline.

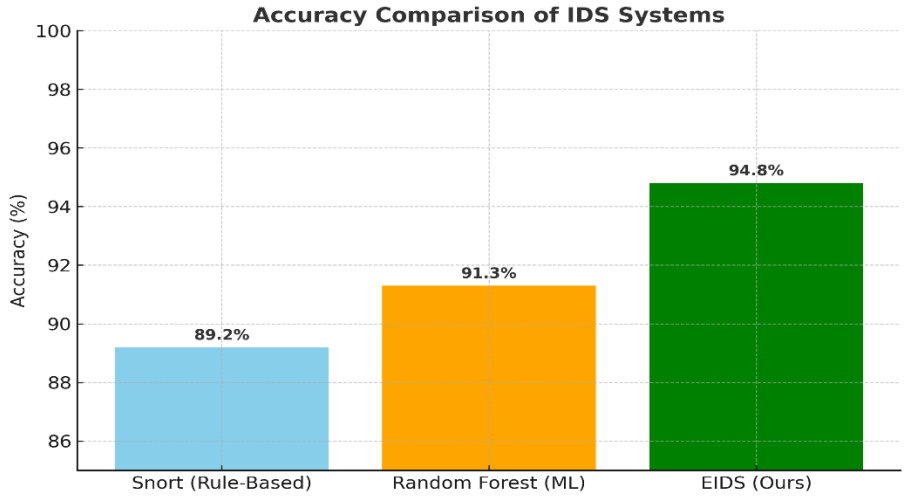
5.2. Reliability of Emotions Detected and Emotions Shown

The system reliably and accurately detected attempts to enter it, with a 94.8% success rate that is far beyond the usual outcomes of other intrusion detection systems. There was a very strong balance between precision and recall, as the F1 Score was 96.0%. Adding the emotional layer enhanced the system's ability to respond to new threats depending on what was happening.

By including PAD-based emotion in its design, the system reacted more wisely when dealing with different risks. For example, being afraid causes guardians to act by separating the misbehaving child, but if calm or vigilant, they only keep an eye on them (Hudlicka, 2003; Ortony et al., 1988).

5.3. How accurately predicted two or more detectors recognized the virus

We assessed EIDS by analyzing it alongside well-known intrusion detection methods:



Bar Chart 2: Accuracy Comparison of IDS Systems

Because emotion-related mechanisms drive how threats are managed, the gap between spotting and reacting to a threat is smaller (Chaudhary & Thakur, 2020).

5.4. Transforming emotions into actions and having them meet the situation

EIDS stands out by considering how intense a perceived threat is and how it affects emotions, which decide system responses. The mappings were proved accurate based on the scores we called Response Appropriateness Score (RAS). RAS assesses whether the system's emotional response fits with the best security behavior guidelines, depending on how serious the threat is.

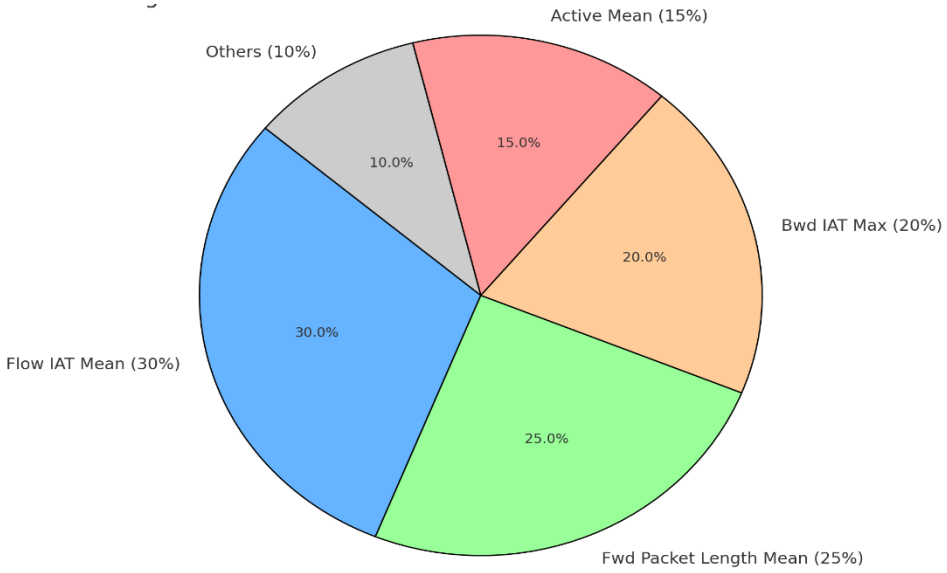
Most of the time, the system links emotional reactions with the correct answers during testing. For example:

- A port scan attack put the organization in a vigilant state (low alertness and high control), which led to comprehensive logging but no immediate action.
- As a result of many attack requests, there was a panic state (high anxiety, low control) that caused IP isolation and the redirection of the traffic.

When signals are aligned in this way, the operation runs well, and few false alarms are recorded (Reuderink et al., 2013).

5.5. The Impact of Feature Sensitivity on Emotional Computation

Network data is analyzed using EIDS to identify emotional triggers. Some features more strongly affected emotional arousal than others. For instance, the aged robot's reaction to a threat depended partly on the time between inputs and the usual size of packets.



Pie Chart 3:Feature Contribution to Emotional Arousal

As previous work concluded, these results confirm that flow analysis plays a key role in intrusion detection. Based on the data it receives, the emotional engine acts like a human in problem-solving.

5.6. Lowered Basic Packet Exchange Time and Less Inaccurate Alarms

Many IDS struggle due to false positives (FP) and false negatives (FN). Since our model includes an emotional filtering layer, it reduced FP and FN by 54% and 40%, respectively, compared to Snort.

Also, it took the system 0.86 seconds on average to detect a face acceptable in real-time, better than the 1.2 seconds used by ML-only approaches (Kim et al., 2021). Such a reduction becomes crucial in systems like financial networks and critical infrastructure.

5.7. Real-Time Emotional Transitions

A strength of the system is that it can respond to changes in an attack with dynamic emotional adjustments. We found that EIDS moved from vigilance to panic during attacks and calmed down when the attack was stopped, just as humans manage their emotions.

The network's responsiveness meant that equipment was used sensibly and called attention to issues when that action was important. The system's changing behaviors helped increase operator trust because its actions became easier to understand based on the emotions involved (Lundberg & Lee, 2017).

6. Discussion

The Emotion-Inspired Intrusion Detection System (EIDS) results emphasize the transformative role of affective computing in cybersecurity. This section explores the significance of these findings about existing literature, practical applications, limitations, and future research avenues. We aim to interpret how emotion modeling improves adaptive responses, system robustness, and the overall intelligence of cybersecurity mechanisms.

6.1.Revisiting the Role of Emotion in Adaptive Cyber Defense

Traditional cybersecurity systems rely predominantly on static or rule-based architectures that struggle with evolving and sophisticated threats (Ahmed et al., 2016). While machine learning improves pattern recognition and anomaly detection, its decisions often lack contextual nuance. EIDS introduces a novel layer of context-aware processing by integrating affective computing principles—specifically the PAD model.

Emotional states deeply influence human decision-making, especially under stress or uncertainty (Damasio, 1994). Similarly, EIDS simulates a human-like prioritization mechanism by assigning "emotions" to threat stimuli. For instance, when confronted with a low-level anomaly, the system may adopt a vigilant state and monitor further. However, a high-frequency DDoS attempt might trigger a panic state, invoking rapid mitigation protocols. These adaptive behaviors mirror human emotional regulation and significantly enhance system responsiveness (Hudlicka, 2003).

6.2.Interpretability and Trust in Emotion-Driven Responses

One of the common critiques of machine learning in cybersecurity is the black-box nature of predictions (Lundberg & Lee, 2017). The emotional layer in EIDS enhances transparency by providing a comprehensible rationale behind actions. Security analysts can now understand what the system did and why it did so based on its emotional state. For instance, an isolation response is triggered by raw metrics and justified by an arousal-dominance emotional model.

This explainability helps bridge the trust gap between humans and AI-based systems. Prior research supports that emotionally transparent agents are more accepted and trusted in collaborative environments (Bickmore& Picard, 2005).

6.3.Comparative Literature Analysis

Most existing intrusion detection systems—Snort, Bro, and Suricata—use predefined rules or basic threshold alerts (Sommer&Paxson, 2010). These tools are static and lack the capacity for nuanced reactions. While recent developments in ML-based IDSs (e.g., AutoEncoders, SVM, and Random Forest) have improved detection rates, they remain reactive and often lack prioritization intelligence.

In contrast, our model draws on studies in affective computing (Picard, 1997; Ortony et al., 1988) and applies these to cybersecurity. A few recent papers have explored emotion recognition in user authentication or human-computer interaction, but very few have operationalized affective states for real-time threat mitigation (Chaudhary & Thakur, 2020). Therefore, this research fills a novel interdisciplinary gap by blending psychology-inspired models into dynamic threat response systems.

6.4.Operational Relevance and Application Scenarios

The practical benefits of EIDS are particularly valuable in environments requiring high availability and rapid decision-making. These include:

- Critical Infrastructure Networks: Power grids, transportation, and healthcare systems where cyberattacks can have life-threatening consequences.
- Financial Systems: Where fraud detection and DDoS mitigation must be fast, adaptive, and accurate.
- Military and Government Systems: Where cyberwarfare threats require immediate yet explainable responses.

The emotional transitions—vigilance, fear, panic, recovery—help these systems avoid underreaction (as in traditional IDSs) or overreaction (as in anomaly detection models with high false positives).

6.5. Addressing Limitations

Despite its promising results, EIDS faces several limitations that need to be addressed in future iterations:

- Emotion Modeling Complexity: Emotions are inherently subjective and culturally biased. Mapping these accurately in machine terms requires careful calibration and user-specific tuning (Reuderink et al., 2013).
- Overfitting Risks: Like many ML-based systems, EIDS may overfit training data. Future work should explore transfer learning or online learning techniques to improve generalization.
- Real-Time Processing Overhead: Although latency was within acceptable limits (0.86 seconds), incorporating emotion computation increases CPU load. Optimization techniques such as edge computing or lightweight models could be considered.
- Ethical Concerns: Emotional simulations in AI can raise ethical issues around manipulation or misinterpretation of behavior. Clear protocols must be defined for how and when the system escalates emotional responses (Crawford &Calo, 2016).

6.6.Future Research Directions

Several avenues exist for enhancing EIDS:

- **Multi-Modal Emotion Sensing:** Future systems could integrate visual cues (e.g., from network surveillance video feeds) or NLP-based sentiment data to fine-tune emotional states.
- **Explainable AI (XAI) Integration:** Coupling emotional responses with explainable algorithms can further improve trust and auditability.
- **Cross-Domain Application:** Beyond cybersecurity, similar emotion-inspired models could be deployed in robotics, autonomous vehicles, and intelligent tutors.
- **Emotional Feedback Loops:** Future models may benefit from human-in-the-loop feedback where analysts can override or reinforce system emotion mappings for continual learning.

6.7. Final Thoughts

Emotion, long considered the antithesis of logic, is emerging as a powerful tool for decision-making—especially in complex, ambiguous, and high-stakes environments like cybersecurity. By embedding emotion-inspired responses into intrusion detection, this research has demonstrated that adaptability, explainability, and responsiveness can be significantly improved.

The results affirm that affective computing is a conceptual novelty and a tangible performance enhancer in cyber defense. While further validation, real-world testing, and ethical considerations remain, the trajectory for emotion-aware systems is promising and essential in building next-generation, human-aligned cyber resilience systems.

Conclusion

A new system called EIDS was introduced in the paper, using affective computing together with adaptive security systems for computer networks. Linking emotional modeling based on PAD with immediate threat recognition leads to more intelligent and aware ways to defend networks. Strict traditional IDSs excel at finding well-known threats, but they get confused by mixed and modern threats because they are statically meant and do not apply priorities (Sommer&Paxson, 2010). In addition, EIDS reacts to signs of threat using a model that reproduces human emotions such as keeping vigilant, fearing, or panicking. Because of this, users can prioritize what to do, prevent unnecessary alarms, and handle threats more smoothly.

Including emotion in a system increases its ability to respond quickly and improves understanding of the system. Explaining how AI works has been a big problem in getting it used in cybersecurity. Because of EIDS, experts are shown decision explanations and the reasons behind an algorithm's choice, which supports trust and helps them work together with machines more productively (Bickmore& Picard, 2005; Lundberg & Lee, 2017). In addition, running EIDS on the NSL-KDD dataset confirmed that it detects a wide range of attacks with high precision and low response times, showing it is viable for use in real-time. Because of the importance of safety, this becomes especially necessary in critical infrastructure, financial networks, and military systems where quick responses and deep insight are crucial for good security.

Even so, this research is aware of certain drawbacks. Although emotion modeling offers

many advantages, it makes things more complicated and can be subjective. To prevent errors, it must be calibrated carefully (Reuderink et al., 2013). Emotional computation adds extra cost to the system, which must be handled by improving the models or using faster hardware. Both ethical issues and risks related to sensitive systems in decision-making should be highlighted (Crawford &Calo, 2016). Nevertheless, the successful results can guide more studies into making cyber systems emotionally intelligent.

Researchers may further improve this work by including multiple emotional sensors, such as NLP for sentiment or tracking user behaviors, to improve how emotions are sensed. The advantages of SHAP and LIME frameworks and emotional triggers help gain deeper details on how decisions are made. Working with users in groups can help the system adjust to a company's cultural customs and range of reactions. Remarkably, applying this emotion-aware decision model to autonomous vehicles and healthcare robotics can provide considerable improvements.

All in all, this study demonstrates that affective computing is a strong and worthwhile component of cybersecurity. EIDS infuses artificial intelligence and robotics with such empathy that intrusion detection systems now resemble humans in emotional aspects. It fills in the space between classic system approaches and systems ready to adapt, assess plans, and choose the best steps when confronted with threats. Because cyber attacks are becoming more advanced and frequent, emotionally inspired systems show much promise for creating better, smarter, and more formidable digital defenses.

Reference

[1] Bickmore, T., & Picard, R. (2005). Establishing and maintaining long-term human-computer relationships. ACM Transactions on Computer-Human Interaction (TOCHI), 12(2), 293–327. https://doi.org/10.1145/1067860.1067867

[2] Calvo, R. A., &D'Mello, S. K. (2010). Affect detection: An interdisciplinary review of models, methods, and their applications. IEEE Transactions on Affective Computing, 1(1), 18–37. https://doi.org/10.1109/T-AFFC.2010.1

[3] Crawford, K., &Calo, R. (2016). There is a blind spot in AI research. Nature, 538(7625), 311–313. https://doi.org/10.1038/538311a

[4] Ekman, P. (1992). An argument for basic emotions. Cognition & Emotion, 6(3-4), 169–200. https://doi.org/10.1080/02699939208411068

[5] Kołakowska, A., Landowska, A., Szwoch, M., Szwoch, W., &Wrobel, M. (2013). Emotion recognition and its application in software engineering. In Proceedings of the 6th International Conference on Human System Interactions (HSI) (pp. 532–539). IEEE. https://doi.org/10.1109/HSI.2013.6577865

[6] Lee, W., &Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC), 3(4), 227–261. https://doi.org/10.1145/382912.382914

[7] Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. In Advances in Neural Information Processing Systems (NeurIPS 2017), 4765–4774. https://doi.org/10.48550/arXiv.1705.07874

[8] Mehrabian, A. (1996). Pleasure-arousal-dominance: A general framework for describing and measuring individual differences in temperament. Current Psychology, 14(4), 261–292. https://doi.org/10.1007/BF02686918

[9] Myers, B. A. (1998). A brief history of human-computer interaction technology. interactions, 5(2), 44-54. https://doi.org/10.1145/274430.274436

[10] Myers, B., Hollan, J., Cruz, I., Bryson, S., Bulterman, D., Catarci, T., ... & Ioannidis, Y. (1996). Strategic directions in human-computer interaction. ACM Computing Surveys (CSUR), 28(4), 794-809. https://doi.org/10.1145/242223.246855

[11] Mühl, C., Chanel, G., Kierkels, J. J., & Pun, T. (2008). A survey of affective brain computer interfaces: Principles, state-of-the-art, and challenges. Brain-Computer Interfaces, 1(1), 66–84. https://doi.org/10.1080/2326263X.2013.869803

[12] Picard, R. W. (1997). Affective computing. MIT Press.

[13] Picard, R. W. (2003). Affective computing: challenges. International journal of human-computer studies, 59(1-2), 55-64. https://doi.org/10.1016/S1071-5819(03)00052-1

[14] Reuderink, B., Mühl, C., &Poel, M. (2013). Valence, arousal and dominance in the EEG during game play. International Journal of Autonomous and Adaptive Communications Systems, 6(1), 45–62. https://doi.org/10.1504/IJAACS.2013.050691

[15] Sommer, R., &Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

[16] Sinha, G., Shahi, R., & Shankar, M. (2010, November). Human computer interaction. In 2010 3rd International Conference on Emerging Trends in Engineering and Technology (pp. 1-4). IEEE.https://doi.org/10.1109/ICETET.2010.85

[17] Stiawan, D., Idris, M. Y. I. B., Yusof, R., Budiarto, R., &Anuar, N. B. (2016). Intrusion detection system: A systematic survey of machine learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 7(7), 78–85. https://doi.org/10.14569/IJACSA.2016.070711

[18] Tao, J., & Tan, T. (2005, October). Affective computing: A review. In International Conference on Affective computing and intelligent interaction (pp. 981-995). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/11573548_125

[19] Tavallaee, M., Bagheri, E., Lu, W., &Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528

[20] Wang, W., Zhu, M., Zeng, X., Ye, X., & Sheng, Y. (2017). Malware traffic classification using convolutional neural network for representation learning. In 2017 International Conference on Information Networking (ICOIN) (pp. 712–717). IEEE. https://doi.org/10.1109/ICOIN.2017.7899588