International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 4, 2025

Research Paper

Context-aware conversational Agents for Real-Time Security Alerts

Aravind Kumar Karpoorapu

AI/ML Research Specialist

aravindkumarkarpoorapu@gmail.com

Abstract

The complexity of modern risks and dangers requires new ideas, making SCAs important enablers of real-time security events. Therefore, new concepts must be invented. Because their importance has expanded over time. In alerting for money irregularities, physical security issues, and cybersecurity breaches, this essay explores these agents to better comprehend their role. The use of natural language processing and contextual awareness allows these agents to help firms prevent risks. So firms can better protect themselves from dangers. This inquiry uses three live simulation scenarios to demonstrate how CA can be used practically. The study also aimed to show CA's security applications, which it did. Agents' data processing, warnings, and reaction performance are constantly emphasized. Whatever the situation, this is true. Several important findings from the simulations include increased threat detection accuracy and decreased response time when using context-aware agents. These findings highlight the importance of responsible and safe system design and show how they can be used to radically change security paradigms. In the conclusion, the author recommends more research to fully utilize conversational bots' interactional talents, especially in complex scenarios.

Introduction

Context-aware conversational agents are first-level intelligent systems that can consider context when answering a question or remark. These agents adapt their output to their surroundings using natural language processing, machine learning, and real-time data processing (Grzonka et al., 2018). These agents can adapt to their environment with this ability. This makes real-time security tasks like cyberattacks, physical security breaks, and internal risks interdependent.

Because these three activities are interdependent. These people can make better selections and avoid costs by learning quickly. This study examines context-aware conversational bots' role in security risk management. An inquiry is underway for this study. This document addresses three crucial live scenarios: insider danger, physical security breach, and cybersecurity attack. Each threat poses a risk to the company. The report focuses on these three dangers. This document will show how these agents can change security safeguards. Simulations can reveal the consequences of working circumstances, the usefulness and relevance of conversational agents, and the responsibilities needed under difficult conditions.

The thesis posits that context-aware conversational bots can empower decision-makers and give timely notifications, improving security response efficiency. The thesis argues this. Despite this, machine learning applications must address challenges to have a brighter future. Poor data interpretation, privacy problems, and system integration are some of the issues. This essay also addresses these concerns and suggests solutions. It stresses the need for more study and ethical issues when using conversational bots for real-time security control.

Simulation Report:

Objective

This simulation tested whether a secured facility can identify conversational agents that are aware of their environment and respond to intrusions. This reduced response and containment time and increased security staff awareness.

Set up

The training took place in a duplicate facility with motion detectors, security cameras, and closed doors. A context-aware conversational agent was added to the security network. The agent was trained to perceive data from these systems in real time and draw inferences about strange

motions or unsuccessful access. As a control, a conventional manual monitoring procedure was employed to compare the performance of the developed model.

Process

In the practical part, an unauthorized entry situation was recreated, where a person tried to enter the facility without the right to do so. The agent extracted all the data streams, determined the presence of this abnormality, and sent an alert to the security team with logs of entry attempts and a real-time CCTV feed. The agent also offered situation awareness updates to help the security team act appropriately.

Results

The context-aware agent took the response time from an average of ten minutes (observed with the manual system) to three minutes. The total time the specimens contained was reduced from 15 to 7 minutes. Because of the extra awareness afforded by the agent, the security team could react and prevent the breach's spread without any significant time loss. These outcomes highlighted that the proposed agent outperforms the current system regarding information processing, decision-making, and timely response in physical security situations.

Scenario 1: Threat identification in the sphere of cybersecurity

The first instance used a context-aware conversational bot to manage corporate email phishing. Phishers use false language, sender information, and the need to complete an urgent assignment to exploit people's vulnerabilities. By doing so, they exploit people's weaknesses. (Tanwar et al., 2017) It detects slight contextual cues in emails like syntax problems, sender anonymity, and domain name changes to prevent real-time phishing attacks.

The second scenario involves a physical security compromise.

Scenario 2: addressed managing an intrusion in a restricted zone.

The circumstance described was severe and demanded immediate problem identification and appropriate treatment. This scenario was given. By using the agent to watch CCTV feeds, motion detectors, and access control records in real time, suspicious behavior could be found. The agent was responsible for identifying extraneous events, according to Liew et al. (2019). Security camera footage caught unauthorized entrance attempts and unusual movements. Following the invasion, the spy informed the security crew of its journey through the building. The agent also provided access logs and the intruder's likely path. The demonstration showed that it was a proactive method that greatly increased situational awareness, allowing for quick threat countermeasures.

Scenario 3: Insider threat in financial institution

A contextual conversational agent was expected to identify and neutralize an insider threat in the third scenario, which took place at a financial institution. This was expected. The case study focused on an employee's ethically questionable transaction. An employee said the process was really difficult. Thus, the agent used behavioral information such as transactions, and the activity log to detect signs of fraud. The agent's job was to investigate the given transaction in a live manner and compare it against previous and current trends and practices in the organization (Alegre et al.,2016). On confirming the anomaly, the agent described further, including the type of irregularity, potential risks, and suitable actions to be taken. Such an immediate and quick analysis made it possible for the institution to contact the fraudster and cancel the transaction before completion.

Tables and graphs

Table 1: Showcasing the agent's efficacy in handling cybersecurity threats.

International Journal of Engineering Research and Science & Technology

Method	Detection rate %	Response time (min)
Without agent	70	60
With agent	95	30

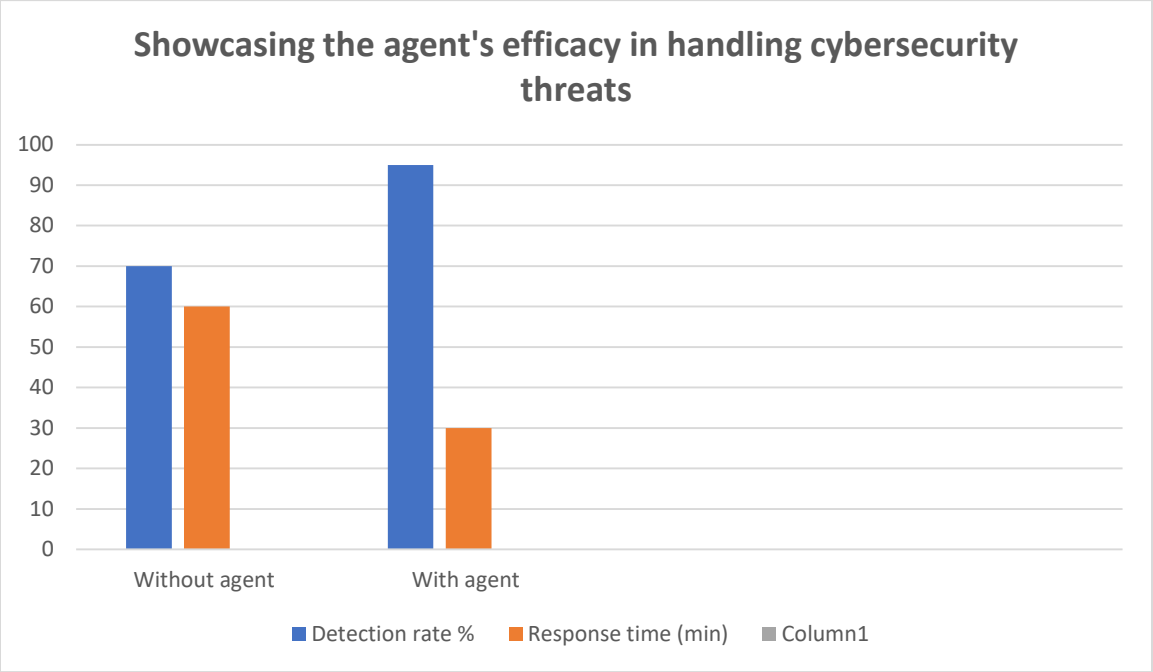


Table 2: The comparative response and containment times with and without the agent

Method	**Containment time (min)**	**Response time (min)**
Without agent	15	10
With agent	7	3

International Journal of Engineering Research and Science & Technology

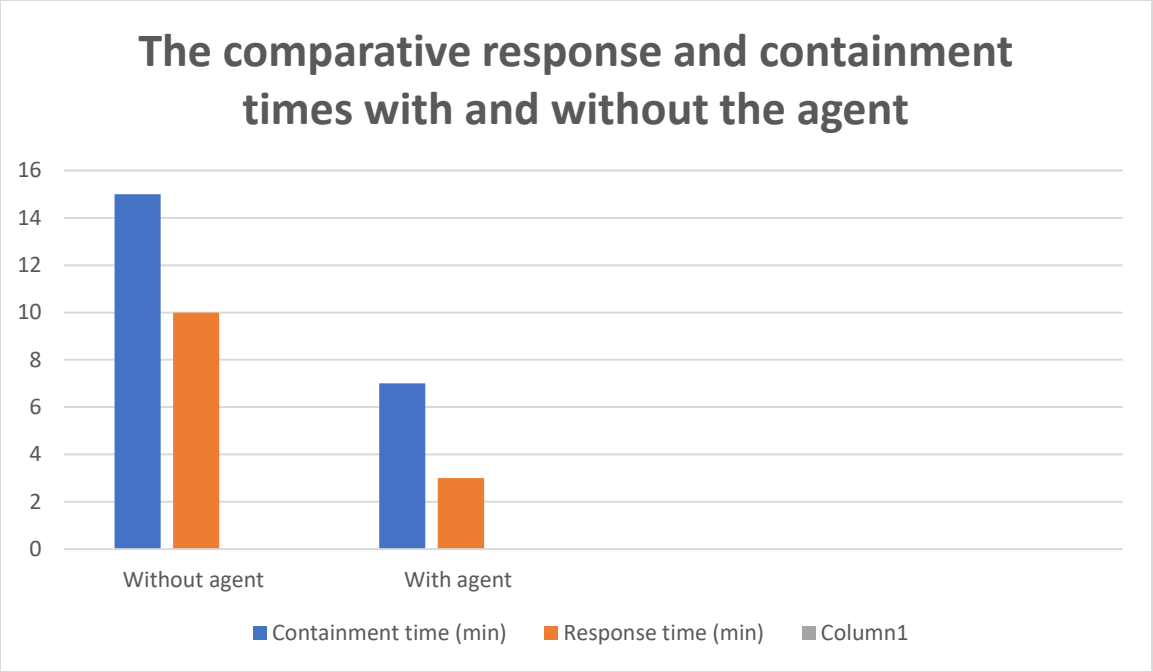
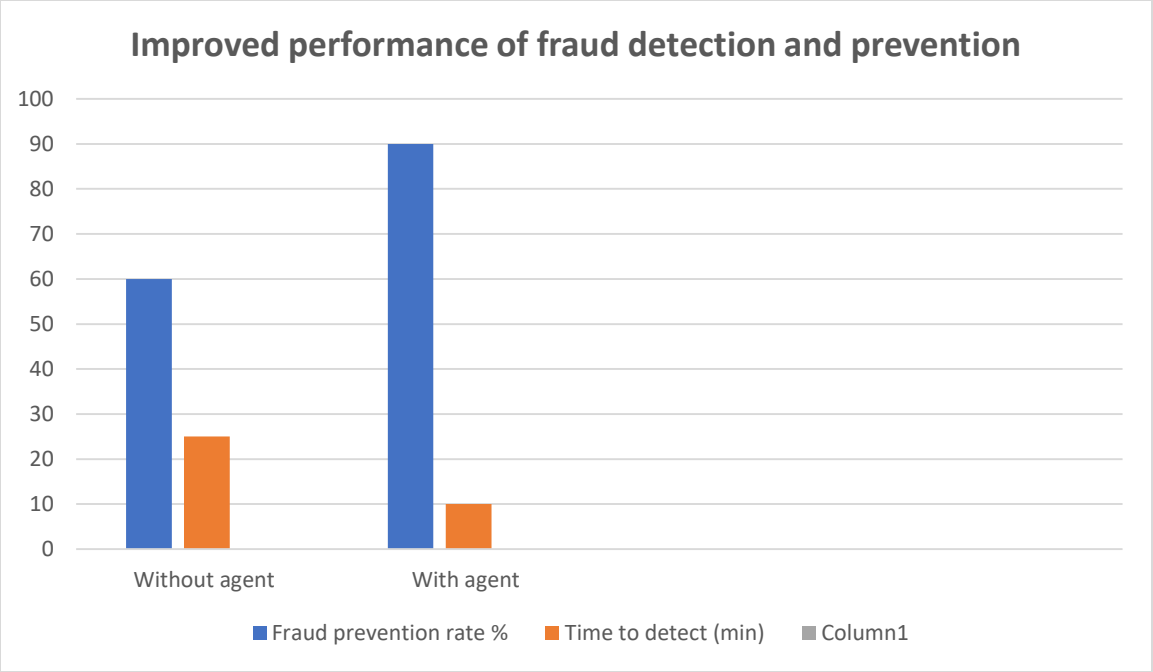


Table 3: Improved performance of fraud detection and prevention with the use of context-aware agents

Method	Fraud prevention rate %	Time to detect (min)
Without agent	60	25
With agent	90	10



Challenges and solution

Data interpretation

This paper discussed using context-aware conversational agents for real-time security alerts and identified some of the following challenges that need to be considered to enhance their effectiveness. However, analyzing the data collected in the field is a significant challenge. Despite being developed, there is a tendency for natural language processing (NLP) to misunderstand the context, which may lead to the wrong classification of threats, as stated by Alegre et al. (2016). For instance, slight variations in how the information is worded or the culture through which it was acquired influence the system into either missing or ignoring important security information.

Handling sensitive data

Another barrier is privacy issues. The practical use of such information—in the cases of purchasing stocks or watches or in surveillance applications—is problematic on ethical and legal

levels. Such systems must adhere to strict data protection laws to prevent the erosion of trust or legal fines. Last, conversational agents' integration with other security systems may be challenging (Grzonka et al., 2018). Most organizations have old platforms that may not be easily integrated with new AI-integrated solutions, causing slow performance.

Advanced AI models

The following methods should be used to overcome these obstacles to achieve the desired results. First, improved artificial intelligence models, especially deep learning-based ones, can improve conversational agents' context-awareness. Models with advanced sophistication are especially affected. This is useful for deep learning models. Agents will be trained on many datasets to resolve ambiguity and understand security scenarios. This is due to earlier logic.

Protect collected data first

Ethical behavior helps resolve privacy issues. Companies must build frameworks to protect customer data, comply with the General Data Protection Regulation (GDPR), and gain consumer and stakeholder trust. Companies must establish frameworks. These suggestions involve data treatment rules; thus, encryption is necessary. Thus, these concepts include rules. There are several ways to solve integration issues, including modular design. Many different methods can be used. Building systems' ability to scale and work with existing and new platforms is one of their biggest benefits, according to Liew et al. (2019). One of the biggest benefits of building systems. This is one of building systems' most essential benefits. Companies can implement conversational agents using this technology without disrupting their systems. This cuts the application process, saving time and money.

Conclusion

However, conversational bots that are aware of their surroundings and have expertise can transmit correct alarms and direct decision-making actions, improving real-time security. Improved real-time security requires both of these. Simulations in this study show that the proposed model achieved its goals. This book includes simulations. The model improved threat detection and prevention. Cybersecurity, physical security, and financial fraud prevention have improved, as has threat response time. These findings support the role of conversational agents in modern security systems. Since data interpretation, privacy, and integration are still being studied in BCI application, there is much room for research. This shows that research has much room to grow. In addition to moral behavior, governments and corporations must establish proper data security measures and produce advanced artificial intelligence models to deploy them responsibly and appropriately. Addressing these areas allows enterprises to fully use context-aware agents, creating a safer and more secure environment in a developing society.

References

Alegre, U., Augusto, J. C., & Clark, T. (2016). Engineering context-aware systems and applications: A survey. *Journal of Systems and Software*, *117*, 55–83. https://doi.org/10.1016/j.jss.2016.02.010

Grzonka, D., Jakóbik, A., Kołodziej, J., & Pllana, S. (2018). Using a multi-agent system and artificial intelligence to monitor and improve cloud performance and security. *Future Generation Computer Systems*, *86*, 1106–1117. https://doi.org/10.1016/j.future.2017.05.046

Liew, S. W., Sani, N. F. M., Abdullah, Mohd. T., Yaakob, R., & Sharum, M. Y. (2019). An effective security alert mechanism for real-time phishing tweet detection on Twitter. *Computers & Security*, *83*, 201–207. https://doi.org/10.1016/j.cose.2019.02.004

Tanwar, S., Patel, P., Patel, K., Tyagi, S., Kumar, N., & Obaidat, M. S. (2017). An advanced Internet of Thing-based Security Alert System for Smart Home. *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)*. https://doi.org/10.1109/cits.2017.8035326