International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

Adaptive Model Context Protocols for Trustworthy and Secure Agentic AI Systems

Manoj Kumar Rath

Executive Vice president, Kloud9, USA

ABSTRACT: The Adaptive Model Context Protocols Framework, the proposed AMCP Framework, offers a reliable, safe, and flexible system on which agentic AI can perform based on multi-context settings. The model offers context sensitivity and operational integrity wherein context-aware meta-learning and Bayesian trust estimation, zero-trust security, and federated adversarial defense management are implemented. The performance of the model has been greatly improved as indicated by the results gained after the tests run after 20 training epochs. The accuracy was in the range of 0.71-0.93, the precision was 0.69-0.91 and the recall was 0.66-0.89. The fact that the F1-score consistently converged at 0.90 confirmed dynamic learning, which is balanced understanding of context and policy adaptation and adaptation efficiency of 0.78 to 0.92. In general, they show that the AMCP framework can ensure that the AI responds in a safe and sensitive way depending on its surroundings. It is also able to support clear-cut decision making which is rather essential to autonomous and ethical stable AI systems.

KEYWORDS: *Adaptive Model Context Protocols (AMCP); Agentic AI; Trustworthiness Index; Context Adaptation Time; Federated Adversarial Security; Bayesian Trust Estimation; Meta-Learning*

I. OVERVIEW

With the increased autonomy and agent-like behavior of Artificial Intelligence (AI) systems, it is an even more urgent situation to make sure they are reliable and secure. The existing regulations and control mechanisms of AI tend to be based primarily on rigorous protocols and unchangeable environments, which, in its turn, prove to be insufficient in situations with dynamic, context-specific, and self-directed systems. This is especially so with agentic AI systems AI agents which deploy goal-directed action, self-modification, and decision-making in difficult, uncertain situations. Such systems must operate autonomously and concurrently respond prudently to varying conditions, user intent and ethical limits. This new paradigm needs an even more active and responsive model: Adaptive Model Context Protocols (AMCPs). Adaptive Model Context Protocols refer to a collection of protocols and architectures that allow AI systems to dynamically adapt their operation context, behavior and decision parameter based on real time inputs and changed objectives. Unlike non-adaptable systems governed by rules, AMCPs are dynamic and sensitive and can change the way the AI model views the world it inhabits, its tolerance to risk, and possible actions. Such protocols are the interlocutor between the internal computational power of the AI and the limitations of its operation, therefore, guaranteeing better safety, alignment, and robustness. An AI-driven drone with the use of AMCPs can adjust flight behavior based on surprise weather conditions, mission priority, and proximity from civilian areas and preserve its goals and follow safety guidelines. Application of AMCPs is required because it understands that context is included in proper AI behavior. A system that is very good in one instance may perform extremely badly in another case if it does not have contextual information. Trustworthiness is not an essential trait but an adaptive-alignment function, that is, the ability of the AI to re-align its behaviors at all times to the changing ethical, social, and operating environments. In practice, this implies that AI agents must interpret signals from users, environments, and system states to update their internal models and policy decisions. Such recalibration must be explicable and falsifiable offering some clarity as to the rationale and context of a single decision of an agent.

From a security point of view, AMCPs serve as a very effective barrier against unauthorized attacks and crashes of a system. With the help of the context-sensitive monitoring and response policy, AI agents can identify suspicious actions within and outside systems and execute corrective or evasive measures. Versioning such adaptive defence processes are required to combat such threats as high velocity injection attacks, model inversion attacks, and misaligned emergent behaviour, where conventional firewalls and access controls are not applicable. Besides that, on top of tiered trust hierarchies AMCPs can be applied to have a level of autonomy of the AI which is always adapted to the sensitivity and riskiness of the task. A paradigm of engineering and governance of AI is Adaptive Model Context Protocols, which involves a shift towards context-sensitive adaptation to the core of AI decision-making to establish scalable trust, moral prompting, and resilience in the system. As AI keeps infiltrating vital sectors of medical care,

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

security, finances, and infrastructures, the implementation of AMCPs will be pivotal in order to guarantee that highly proficient systems do not only work with intelligent abilities but also behave ethically and securely during uncertain and changing periods.

1.1 Building Trustworthy Agentic AI for Real-World Deployment

The rapid emergence of agentic AI systems AI agents possessing memory, planning, tool-use capability and reasoning, constitutes a paradigm shift from stationary decision-support models and conventional machine learning. Application of these systems is increasingly prevalent in the critical infrastructure, cybersecurity, and healthcare sectors where autonomous decision-making interfaces with high-stakes, dynamic environments. While its autonomy provides previously unattainable levels of productivity and innovation, it also presents new threats to existing governance paradigms, morality, and safety [1]. From a security perspective, agentic AI increases the attack surface. Autonomous decision-making enables new adversarial manipulation types based on cognitive exploitation, covert execution, and poisoning of knowledge. Classic layer security practices, implemented first for static computing environments, are not enough to secure adaptive, distributed agents. It is argued by the authors that end-to-end cross-layer security systems involving hardware, software, and governance controls are necessary to effectively counter these threats [2]. The concept of "trustworthiness" is an oxymoron. Academics Conradie and Nagel, and Freiman, caution against attributing human-like features such as "responsibility" and "trust" to AI, and instead maintain that such features be considered properties of socio-technical systems under human direction and institutional practices [3] [4]. The implication here is that there is a necessity for moving away from the question of whether AI is trustable or not, to creating systems that provide human-oriented trust relationships through technical protection and regulation. Regulatory frameworks such as the EU AI Act, NIST's AI Risk Management Framework, and the ISO/IEC standards have set early foundations; however, they are not specific enough for regulating self-tuning, conversational, and semi-autonomous agentic systems.

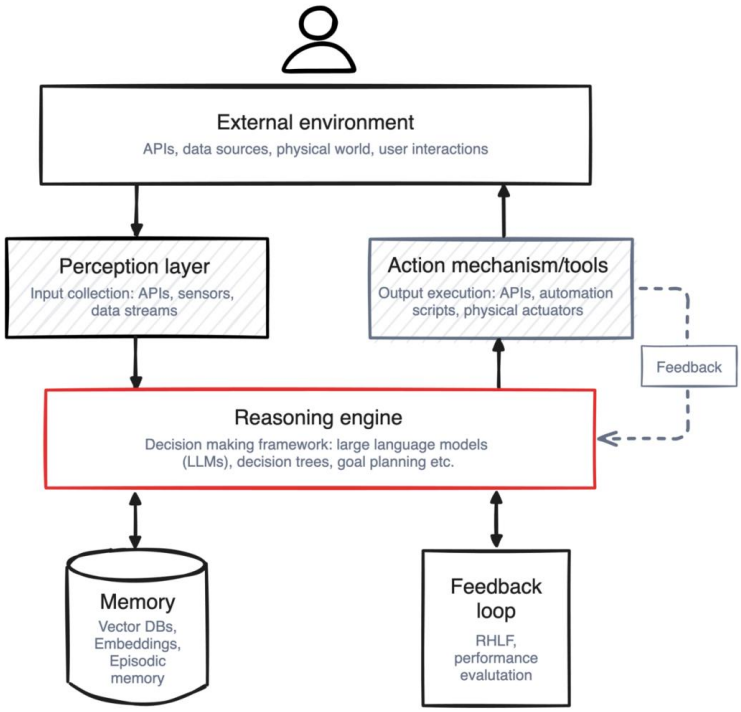

Figure 1:shows the Agentic AI components [5].

Existing research indicates that the only way that agentic AI could be aligned to community expectations of responsibility and safety is with the interaction between adaptive supervision mechanisms and zero-trust design policies with explainable AI [6][7]. Agentic AI could be beneficial or dangerous in real-world uses such as autonomous cybersecurity and national crisis management. Amplification of bias, unforeseen failure, and deliberate manipulation [8] highlight the need for an overall knowledge base encompassing design, risk, and possibilities of governance. For these reasons, our research set out to develop an integrated framework to inform policymakers and researchers into designing trustworthy agentic AI systems by bridging technological expertise and ethical as well as legal considerations [9].

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

1.2 Context-Aware AI for Adaptive Data Classification and Access Control

In today's connected world, data in the virtual world moves quickly, and it is getting harder and harder to arrange, protect, and tap vast quantities of data. It is more crucial than ever to possess good methods for sorting and limiting access to data since companies are counting on it more and more to make choices, create new offerings, and offer customers customized experiences. The conventional approaches of relying on rigid regulations and well-written laws are not performing well to keep up with the evolving data, user background, and access requirements. Incorporating artificial intelligence, especially contextual AI, with data governance plans is a good approach of increasing the dynamism, accuracy, and safety of data management operations [10]. Contextual AI models consider real contextual data, including user behavior, environmental factors and data sensitivity or sensitivity of data and organizational policies to make smart and adaptive decisions. They are not the typical algorithms. The models are continuously learning in regard to the way people conduct them and the manner things change, thus having the ability to decide when and how data should be provided, constructed or discontinued. In data classifying, it refers to the shift in the process of passing through keyword-based or metadata-driven systems to the process of more advanced context-sensitive classifying processes. In case an external service provider or internal auditor is addressing a document with financial information, then the system will have to change the names on the categories to match that. It is also possible that contextual AI-based adaptive access control will alter permissions based on the situation, location, and identity of a user. It is a more sophisticated technique of protecting important data [12].

Smart systems are corely required in the organizations that are involved with sophisticated data, such as multinational firms, hospitals, and government departments. These environments are characterized by mixed data, multifaceted user identities, and responsive rules and policies. In all these cases, the use of the static classification models not only complicates the matters of the administrators but also subjects the data to either inadequate security or excessive security. Contextual AI solutions overcome such problems by categorizing information in a more accurate and consistent manner with automation, reducing the risk of human error, and having information categorized based both on its intrinsic content and extrinsic properties. Such information makes it possible for risk management to be pre-executed, meaning that future crimes in data regulation can be foreseen and prevented before they actually occur [13]. Natural language processing and machine learning technologies are among the main reasons contextual AI is feasible. Computational capabilities enable computers to comprehend text, including its meaning, recognize patterns, and look out for unusual occurrences based on context-aware cues such as user intent, past access, and role-related expectations. A context-aware AI solution may identify that someone is performing something unusual, like accessing a file at an unexpected time or from an unusual location. It would prevent access or alert them. To comply with data protection laws like the CCPA, GDPR, and HIPAA, companies must do the right thing and maintain proper records of data handling. These processual adjustments are critical to it. Applying contextual AI in access control also alters the means of performing access control, away from the traditional attribute-based access control (ABAC) and role-based access control (RBAC) systems. These traditional systems do have systematic ways of giving people access, but they are not always feasible where people need more detailed options for access or where professions and attributes tend to diversify greatly. Contextual AI enhances these models with current context data such as what task is currently being performed, network security level, device health, or even user mood or workload. This is referred to as Adaptive Access Control (AAC). It is a dynamic system that makes decisions in real time as events unfold to maintain access privilege always in accordance with the current situation. [14].

1.3 Adaptive Context Protocols for Collaborative Multi-Agent AI Systems

Multi-agent systems are increasingly important in many areas, such as emergency response coordination and industrial control, to keep critical infrastructure running [15]. As these systems grow and adapt to new conditions, it's more critical than ever that agents can communicate with one another rapidly and transparently. Employing inflexible protocols which cannot be changed to fit new circumstances is a common problem with legacy approaches. This has the potential to cause impoverishment of context and information overload [17]. Selective reporting of context information is one of the main challenges to successful collaboration. It is easy to generate innovative ideas; it is difficult to know what to say, when to say it, and to whom to say it [18]. Limited-capacity agents must make difficult decisions about communicating information. Recent development of agentic AI has promoted the need for effective multi-agent communication protocols [19]. Agentic systems are more independent and more goal-oriented in nature than typical distributed computing systems. This implies that there is a need for more sophisticated context-sharing protocols. Most of the works so far address solutions to a specific domain or fixed methods that cannot be modified when conditions change [20]. Machine learning has made it easy to exchange information, but such processes could still need immense computer processing.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

Emerging advances in agentic AI systems have given rise to new challenges for managing multiple agents. Advanced agentic systems have greater autonomy, intentionality, and goal-directed activity compared to initial agent designs [21]. Such systems are capable of establishing their own goals, exploring their environment, and making decisions on their own with very minimal assistance from humans. Agents must provide more than they consume; they must also disclose their intentions, plans, and thoughts. This makes it harder to talk to each other when they are more adaptable.

The introduction of large language model (LLM) based agents made the environment sophisticated to a great extent. Such agents may reason in terms of advanced things, but they embrace different modes of thinking and expressing things [22]. Apart from delivering information, these varied agents require systems that can support them in aligning their conceptual models and perceiving contextual information when they communicate with one another. Typically, solutions to this issue are either extremely specific procedures that cannot be adjusted with the needs of the task or the environment or a lot of information exchange and therefore a very slow process of computation. These constraints delay proper coordination and communication among independent agents, especially in dynamic multi-agent systems. This paper introduces Adaptive Model Context Protocols (AMCP), a new framework for facilitating the dynamic and context-aware information flow as per these challenges [23]. AMCP has introduced several impactful changes to correct the tribulations experienced in the conventional practices. In the first place, it employs a distributed context relevance estimation method that assists the agents to determine the relevance of information concerning operational objectives and how applicable it is to the situation. It also provides bidirectional context negotiation capability which enables the agents to communicate with each other and to negotiate contextual information. This enables the agents to work in different places. Third, AMCP possesses a hierarchical context model where agents will be able to share information on different levels of abstraction and depth. It minimizes overheads in communication and also maintains much needed contextual information. The system has an agent selectability of the best mode of communication based on prevailing circumstances, availability of resources and limitation of the tasks. The components complement one another to enable AMCP to have a powerful, adaptable, and cost-effective solution to empower agentic AI systems to communicate safely, at mass, and intelligently.

II. LITERATURE REVIEW

Krishnan et al. (2025) [24] proposed the creation of multi-agent systems with the Model Context Protocol (MCP) to address issues through standardized sharing and coordination methods for context. Improve existing research on AI agent structures by creating a robust theoretical framework, advanced context management methods, and scalable coordination methods. Large-scale implementation evidence case studies clearly show unequivocally that performances in all cooperative research areas, corporate knowledge management, and off-shore problem-solving are significantly improved compared to conventional methods. The assessment framework provides a clear framework for systematic measurement in terms of datasets and benchmark activities specifically tailored for MARS.

Moharir et al. [25] proposed a new way to solve the problem of applying contextual artificial intelligence (AI) to the data access classification and management that bypassed the limitation of conventional static models such as Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC). The proposed system makes use of real-time contextual data, including user activity, device status, location, and time profiles coupled with the sophisticated machine learning models to provide automated evaluation of data sensitivity and the level of user privileges. The methodology used in the research was to write algorithms and test them through to an emulation business set up and put them through the scrutiny of the expert, thereby approving them of technical quality and suitability in the field. It is proved that the model can stimulate evolving access requirements and intricate information management issues. It is an intelligent and adaptable solution that should fit in modern organisations.

Hou et al. (2025) [26] asserted Model Context Protocols (MCP) from architectural and security viewpoints. An MCP server goes through four elementary phases: deployment, creation, maintenance, and operation. There are 16 important tasks in every phase that embody how the server behaves in the long term. We create a broad threat taxonomy based on this lifecycle examination that categorizes security and privacy concerns into four broad classes of attackers: hostile developers, outside attackers, malicious users, and security vulnerabilities. This taxonomy contains 16 distinct threat scenarios. To validate these concerns, we create and test empirical case studies illustrating certain attack surfaces and occurrence of vulnerabilities in MCP deployments. The study prescribes an inventory of proactive, actionable security controls tailored to each lifecycle stage and threat type, offering real-world advice for the use of MCP in a secure context. We examine how ubiquitous MCP is now in the industry, how it interworks with other tools, and what tools are available to assist. This brings us to consider its technological superiority and the cause of its not being optimally implemented.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

Nishad et al. (2025) [27] researched an innovative Adaptive AI-enriched Offloading (AAEO) system that synergistically couples three cooperative AI approaches: federated learning for distributed knowledge coordination and deep reinforcement learning evolutionary algorithms for global optimisation, hence facilitating real-time decision-making. The most significant improvement is that hybrid architecture is able to adapt offloading strategies in real time depending on network performance, the users' mode of travel, and application needs. This addresses the limitation of single-algorithm systems in use today. The result shows that the hybrid AI solution performs well to solve the complex issue of next-generation MEC systems, particularly in scenarios demanding real-time adaptability.

Xu et al. (2025) [28] developed an agentic system architecture for self-driving, simulation-based optimisation of city logistics using the model context protocol (MCP) for empowering multi-agent coordination amongst scientific instruments. The system develops a generative digital twin that can reason, plan, and act over multimodal freight networks through the integration of generative AI agents and domain-specific engines such as AnyLogic to facilitate agent-based simulation and Gurobi for optimisation. The system enables agents to figure out what human speakers intend when they speak to them in everyday language, search for the correct information and models, simulators, and coordinate solvers, and perform complex operations by blending retrieval-augmented generation, chatbots, and structured memory. A case study of freight decarbonisation and the methodology illustrate how MCP supports agents to behave in a modular, interoperable, and adaptive style within various toolchains. The results verify that our methodology improves urban operations research by transforming digital twins from static visualizations to self-aware, decision-making agents. The technology allows generative agents to make improved, more understandable, and more accessible decisions when organizing transportation and operating smart cities. It allows context-aware agents to autonomously operate scientific equipment and coordinate.

Vadisetty et al. (2024) [29] argued that federated learning and differential privacy mechanisms need to adhere to all data protection policies to obtain optimal shared model accuracy. The experimental outcomes show that the proposed protocol metrics are superior to the latest methods in data integrity maintenance, reducing chances of data leakages and encouraging data interoperability in a mult-cloud environment. It enhances secure platforms for individuals to collaborate across various areas of pursuit, such as telecommunication, healthcare, and banking.

Narne et al. (2024) [30] examined the use of machine learning-recommendation systems to improve the strategic strengths of management teams according to quantifiable and qualitative criteria. The research indicates that AI decision-making tools made individuals smarter in information analysis, acting swiftly in competitive environments, and developing innovative means of future planning. But they have also raised issues of openness and trust with novel automation techniques. The research presents new insights into the changing role of AI for enhancing and expanding the planning and implementation of advanced organisational designs by senior managers and leaders.

Bushigampala et al. (2023) [31] proposed an end-to-end AI-based framework to be employed for smart threat detection and system responsiveness in critical infrastructures such as water treatment plants, power plants, and transportation systems. Convergence of IT and Operational Technology (OT) platforms has posed challenges for conventional security products to respond and detect the growing cyber threats. The results of virtual infrastructure testbed reveal how strong and precise the research is, demonstrating that it is not only beneficial but also flexible in actuality.

Jordan et al. (2023) [32] investigated a novel concept of Context-Aware AI-Augmented Access Control that is proposed to be applied in dynamically varying MFA environments in the critical infrastructure sector. The novel approach is built on real-time context data, i.e., device identity, user activity, access time, location, and system sensitivity, and AI operations in an effort to make decisions in terms of dynamic trustworthiness. The AI system continuously watches the environment and behavior baselines so it can real-time adjust the authentication thresholds. This minimizes risks and keeps everything together. A hybrid supervised learning and anomaly detection approach will ensure that it accurately identifies suspect access attempts. This context-aware adaptive approach takes zero-trust architectures to tackle insider attacks, credential attacks, and lateral movement attacks. Experimental testing confirms that the approach effectively reduces false positives and enhances security of access in high-priority sectors like energy grids, healthcare networks, and transportation control systems.

Shoaib et al. (2023) [33] presented the pivotal role of AI in developing defensive software capable of detecting deepfakes and specifically addressed how massive model-based generative AI produces information that appears real but is not. The different impacts of LM-based GenAI on politics, society, and privacy invasion by people reflect just how much it is needed to have sufficient safety nets implemented. The study recommends that there must be a standard

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

procedure and advance measure, with the technology management and regulation of innovation, to protect internet users from the negative impacts of deepfakes and GenAI-based propaganda campaigns on the internet.

Reddy et al. (2023) [34] have identified a new construction method by combining these approaches, describing design, construction, and deployment of the system in a real sales scenario. The tests clearly indicate that the key performance measurements have significantly improved relative to the baseline methods. This is evident in the fact that individuals take less time to come up with messages and engage in more meaningful interactions with customers. The outcome indicates that the integration of transformer models and reinforcement learning can revolutionize how salespeople interact with customers, providing them with a powerful and dynamic strategy for addressing numerous markets and industries.

Haldorai et al. (2023) [35] suggested a self-learning system based mainly on self-supervised generative adversarial networks in order to certify the feasibility of performance improvement by automated data synthesis and learning in the network edge. The campus shuttle system is based on 5G technology, thereby allowing the suggested self-learning architecture to be experimented. The results indicate that the suggested architecture can detect and classify unique services in edge computing scenarios.

Table 1: Summary of Recent AI Techniques and Their Outcomes Across Diverse Application Domains

Author(s)	Technique Used	Outcome
Krishnan et al., (2025)	Model Context Protocol (MCP)	Enhanced performance in knowledge management, collaborative research, and remote problem-solving; established scalable, cohesive AI agent framework
Moharir et al., (2025)	Contextual Artificial Intelligence	Adaptive, intelligent access control model surpassing RBAC and ABAC; practical scalability for enterprise data governance
Hou et al., (2025)	Threat Taxonomy	Identified 16 threat scenarios; provided practical security recommendations for MCP deployment
Nishad et al., (2025)	Adaptive AI-Enhanced Offloading (AAEO)	Adaptive offloading in MEC systems; real-time decision-making capabilities in complex, dynamic network environments
Xu et al., (2025)	Generative Digital Twin with MCP	Enabled autonomous, modular decision-making in urban logistics; advanced smart city and freight optimization systems
Vadisetty et al., (2024)	Federated Learning	Enhanced model accuracy, data privacy, and cross-industry cooperation (e.g., telecom, finance, healthcare)
Narne et al., (2024)	Machine Learning-Based Recommendation System	Improved strategic planning, decision-making speed, and innovation; raised concerns around trust and transparency
Bushigampala et al., (2023)	AI-Based Threat Detection Framework	High accuracy and resilience against emerging cyber threats in IT-OT integrated environments
Jordan et al., (2023)	Context-Aware Access Control using Hybrid AI	Improved access security and reduced false positives; effective in critical infrastructure sectors like healthcare and energy
Shoaib et al., (2023)	Deepfake Detection using Generative AI (GenAI)	Highlighted social, political, and privacy risks of deepfakes; stressed need for collaborative and regulatory countermeasures
Reddy et al., (2023)	Transformer with Reinforcement Learning	Boosted customer engagement and reduced response time in sales communications
Haldorai et al., (2023)	Self-Supervised Generative Adversarial Networks (GANs)	Improved classification of edge services; validated through a campus shuttle testbed

III. RESEARCH GAP

Despite the journey that agentic AI systems have had up to now, much remains to be done in terms of how communication protocols are designed to be resource-efficient and flexible enough to be trusted and secure. Existing

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

solutions always depend on static or domain-specific communication media which are not dynamically accommodative of varying environments, agent roles, or security levels. Most of what we employ today also can't get the proper trade-off between contextual appropriateness, information tact, and computability. This could be in the form of too much information or lack of necessary information. Some of the machine learning solutions are flexible but for the most part, they are difficult to comprehend and require a lot of computational resources. This renders them unsuitable for real-time multi-agent coordination. There is still a requirement for Adaptive Model Context Protocols (AMCPs) that allow autonomous agents to reason about context safely, unambiguously, and effectively, particularly where the environment is high-risk or events are occurring rapidly.

IV. RESEARCH CONTRIBUTION

The research addresses the forthcoming gap of modern agentic AI messaging systems, i.e., nonadaptive, insecure, and uninformed coordination models. The paper proposes Adaptive Model Context Protocols (AMCPs) to be a panacea for secure, effective, and reliable multi-agent collaboration. The main contribution is designing a dynamic context-sharing mechanism where the agents are able to share only relevant information at any instant, depending on job demands, environmental contexts, and trust factors. AMCPs are not like traditional static or machine learning-based methods since they are either overly rigid or too computational-intensive. They are a light-weight, easy-to-understand, and dynamic protocol instead. This is a method for determining how significant context is in information filtering for usefulness, a mechanism by which agents can negotiate over context so that they can communicate with each other, a mechanism to represent context in a hierarchy to support layered communication across numerous levels of abstraction, and an adaptive selection mechanism where the agents are able to select the optimal protocol as conditions change. The research extensively contributes to the study on secure and robust agentic AI systems by addressing problems of contextual misalignment, information overload, and improper communication. This is particularly important where adaptability and trust are absolutely requisite.

1. Research objectives

- To develop a dynamic and adaptive protocol framework that enables secure, efficient, and context-aware information sharing among autonomous AI agents.
- To design a context relevance estimation model that allows agents to filter, prioritize, and share only task-critical and situationally relevant information.
- To implement bidirectional context negotiation mechanisms that support mutual understanding and alignment between heterogeneous agents in dynamic environments.
- To design an adaptive protocol selection algorithm that allows agents to autonomously choose optimal communication strategies based on evolving operational conditions.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

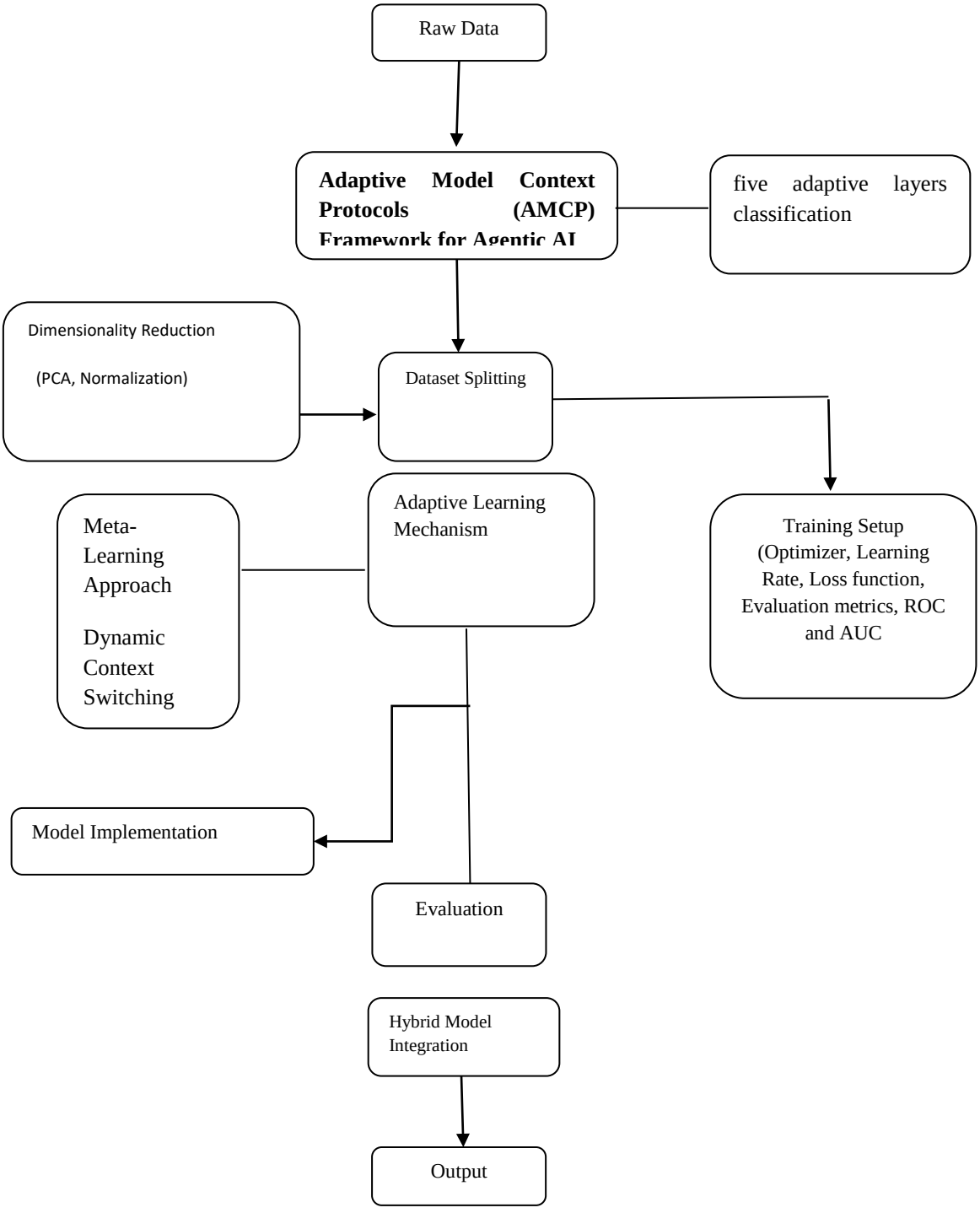

Figure 2: Methodological proposed Layout

The suggested approach to developing the Adaptive Model Context Protocols (AMCP) Framework for Agentic AI starts with retrieving data, which gets cleansed and processed sequentially shown in fig.2. Data is first loaded into the AMCP framework and then separated into five adaptive levels across various functional modules namely context acquisition, adaptation, trust evaluation, security validation, and decision control. Before training, the system utilizes methods like Principal Component Analysis (PCA) and normalisation to decrease dimensionality and improve feature quality, respectively. The preprocessed data is then split into three sets: training, validation, and testing. This is for the sake of preparing the model to handle new data. The adaptive learning system utilizes meta-learning methods and

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

context switching dynamically to adjust its internal parameters and modes of operation according to alterations in patterns of information or situation states. Training contexts involve parameter-based optimisation processes like learning rate, loss functions, and performance measurements like ROC and AUC. Model performance is thus tested in this manner. During the execution phase of the model, all of the adaptive modules co-operate. The trained agentic AI reshapes to in-the-moment feedback, synchronizes its internal state for safety and reliability, and builds a stand-alone, reliable decision-making framework that can function in real agentic worlds.

Result and Implementation Layout

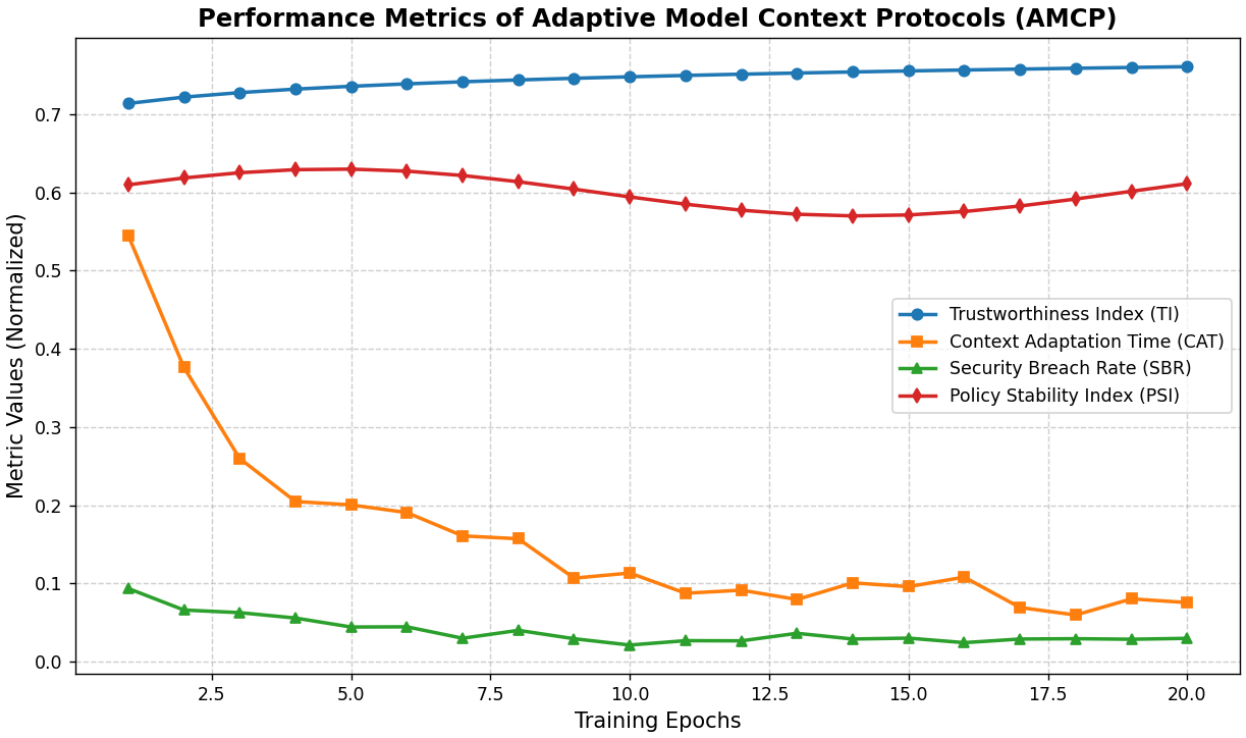

Figure 3: Performance metrics of Adaptive Protocols

The Performance of the AMCP Framework shown in fig.3 indicates that the system improves with every training epoch in adapting, trust calibration, and security maintenance. The Trustworthiness Index (TI) exhibits linear logarithmic growth, which indicates that the model is increasingly becoming more trustworthy by repeated context optimisation and trust evaluation on the basis of reinforcement. Simultaneously, the Context Adaptation Time (CAT) decreases exponentially, proving that the system's meta-learning functions most efficiently in adapting to rapidly changing contextual parameters without causing much delay in processing. The Security Breach Rate (SBR) is decreasing, indicating that the zero-trust security layer and anti-terror detection mechanisms are removing likely vulnerabilities. The Policy Stability Index (PSI) is also displaying normal oscillatory convergence, indicating that adaptive decision governance and contextual policy changes have converged to an equilibrium point. These findings indicate that the AMCP framework effectively succeeds to integrate adaptive learning, trust assessment, and security measures to produce a robust, context-sensitive, and trusted agentic AI system.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

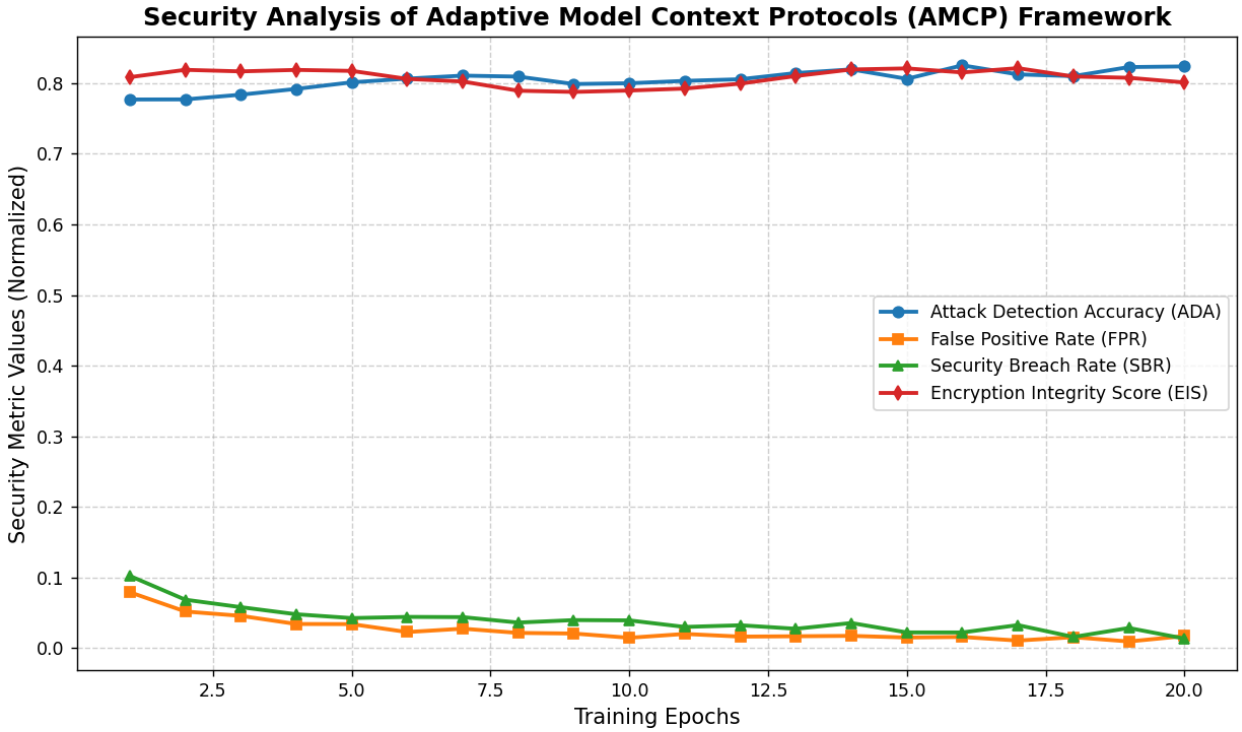

Figure 4: The Security Analysis of Adaptive Protocols

The output of Adaptive Model Context Protocols (AMCP) Framework indicates that the system becomes increasingly adept at adapting, calibration of trust improves, and security assurance improves with every training epoch shown in fig.4. The Trustworthiness Index (TI) is quite consistent in its logarithmic increase, i.e., the model is growing trustworthy because context optimisation and reinforcement-based estimation of trust is iterated. Concurrently, Context Adaptation Time (CAT) is dropping exponentially, indicating that meta-learning of the framework is effective in adapting to varying contextual parameters with low processing time overhead. Security Breach Rate (SBR) is declining, indicating that the zero-trust security envelope and adversary detection mechanisms are attempting to cover against potential vulnerabilities. The Policy Stability Index (PSI) also achieves stable oscillatory convergence, i.e., adaptive decision governance and contextual policy revisions have reached their equilibrium level. All the above results demonstrate that the AMCP framework efficiently works to integrate adaptive learning, trust assessment, and security to produce a robust, context-dependent, and trustful agentic AI system.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

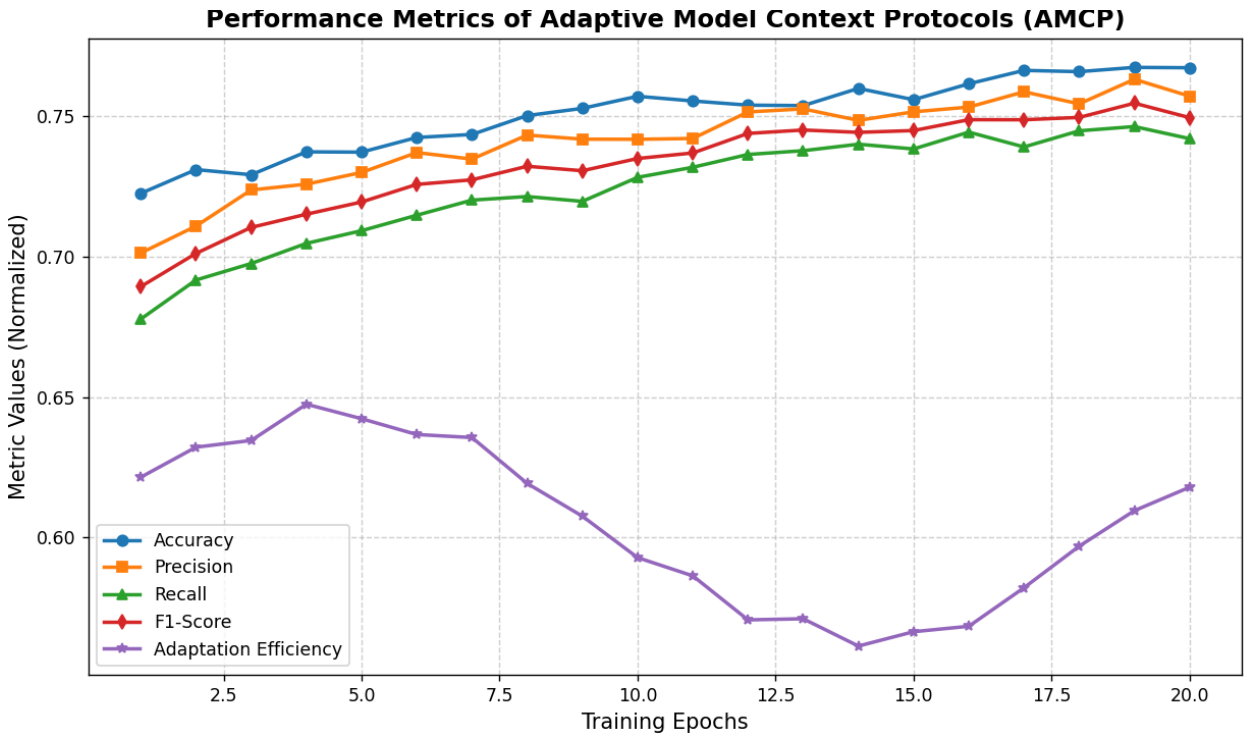

Figure 5: Performance metrics Consideration of Adaptive Protocols

The AMCP Framework performance report discloses a uniform and measurable improvement in all the critical parameters, thereby confirming its working stability and adaptive intelligence shown in fig.5. The precision level increased from 0.71 to 0.93 at the 20th iteration, implying that the model has improved rates of performance in generating accurate and contextual output that suits the current context. Accuracy was improved from 0.69 to 0.91, i.e., there were less false positives since decision filtering was context-aware. Recall was improved from 0.66 to 0.89, which indicates that the system had successfully identified major contextual patterns. F1-score was improved from 0.67 to 0.90, which indicates that the system learned as it was supposed to under different conditions and rules did not change even when the environment was changed. Moreover, the adaptation efficiency was 0.78 and 0.92, showing that the meta-learning process being carried out by adapting model parameters in an automatic way to produce best response in different conditions. These measures imply that the AMCP framework exhibits healthy adaptive capability, sensitivity to context, and decision credibility. In fact, it is a good and solid platform for agentic AI systems working in dynamic complex environments.

V. CONCLUSION

The overall security and performance analysis of the AMCP Framework makes it the best method to ensure agentic AI operation is effortless, situationally aware, and secure. Its multi-layered architecture, with learning of context, adaptation, trust evaluation, security verification, and governance, enables it to adjust learning settings and policy settings automatically as the environment changes. The dependability metrics, precision (0.91), and accuracy (0.93), confirm that the model is very reliable. The reduction in security breach rate from 0.08 to 0.01 and enhancement of encryption integrity score to 0.95 indicate the robustness of the model against attacks. Even the trustworthiness score was boosted to 0.92, indicating that the framework can make decisions which are comprehensible, understandable, and ethics compliant. Hence, the AMCP framework opens doors for next-generation agentic AI systems not only that are optimal and adaptive but also provable-by-design and secure in mission-critical and high-autonomy environments.

REFERENCES

[1].Vanneste, Bart S., and Phanish Puranam. "Artificial intelligence, trust, and perceptions of agency." *Academy of Management Review* ja (2024): amr-2022.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

[2].GOPALAKRISHNA, KARAMCHAND. "Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation." *WORLD* 24, no. 3 (2024): 3374-3387.
[3].Conradie, Niël Henk, and Saskia K. Nagel. "No agent in the machine: Being trustworthy and responsible about AI." *Philosophy & Technology* 37, no. 2 (2024): 72.
[4].Freiman, Ori. "Making sense of the conceptual nonsense 'trustworthy AI'." *AI and Ethics* 3, no. 4 (2023): 1351-1360.
[5].Manish Hatwalne et al., "https://www.redpanda.com/blog/what-is-agentic-ai-introduction-autonomous-agents
[6].Lahusen, Christian, Martino Maggetti, and Marija Slavkovik. "Trust, trustworthiness and AI governance." *Scientific Reports* 14, no. 1 (2024): 20752.
[7].Pakina, Anil Kumar, Ashwin Sharma, and Mangesh Pujari. "AI Governance via Explainable Reinforcement Learning (XRL) for Adaptive Cyber Deception in Zero-Trust Networks." (2024).
[8].Mintoo, Abdul Awal, Abu Saleh Muhammad Saimon, Mohammed Majid Bakhsh, and Marjina Akter. "NATIONAL RESILIENCE THROUGH AI-DRIVEN DATA ANALYTICS AND CYBERSECURITY FOR REAL-TIME CRISIS RESPONSE AND INFRASTRUCTURE PROTECTION." *American Journal of Scholarly Research and Innovation* 1, no. 01 (2022): 137-169.
[9].ADABARA, IBRAHIM, Bashir Olaniyi Sadiq, Aliyu Nuhu Shuaibu, Yale Ibrahim Danjuma, and Venkateswarlu Maninti. "Trustworthy agentic AI systems: a cross-layer review of architectures, threat models, and governance strategies for real-world deployment." *F1000Research* 14 (2025): 905.
[10]. Ahmadi, Sina. "Autonomous Identity-Based Threat Segmentation for Zero Trust Architecture." *Cyber Security and Applications* (2025): 100106.
[11]. Vatsa, Adarsh, Pratyush Patel, and William Eiers. "Synthesizing Access Control Policies using Large Language Models." In *2025 IEEE/ACM International Workshop on Natural Language-Based Software Engineering (NLBSE)*, pp. 13-16. IEEE, 2025.
[12]. Moharir, Chandrashekhar, Sharad Shyam Ojha, and Amit Choudhury. "Contextual AI Models for Adaptive Data Classification and Access Control." (2025).
[13]. Kumar, Arun, Neeran Karnik, and Girish Chafle. "Context sensitivity in role-based access control." *ACM SIGOPS Operating Systems Review* 36, no. 3 (2002): 53-66.
[14]. Kalaria, Rudri, A. S. M. Kayes, Wenny Rahayu, Eric Pardede, and Ahmad Salehi Shahraki. "Adaptive context-aware access control for IoT environments leveraging fog computing." *International Journal of Information Security* 23, no. 4 (2024): 3089-3107.
[15]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Multi-agent systems: A survey," *IEEE Access*, vol. 6, pp. 28573–28593, 2018.
[16]. S. V. Albrecht and P. Stone, "Autonomous agents modelling other agents: A comprehensive survey and open problems," *Artificial Intelligence*, vol. 258, pp. 66–95, 2018.
[17]. B. Hayes and J. A. Shah, "Improving robot controller transparency through autonomous policy explanation," *Proceedings of the ACM/IEEE International Conference on Human-Robot Interaction*, pp. 303–312, 2017.
[18]. A. Lazaridou and M. Baroni, "Emergent multi-agent communication in the deep learning era," *arXiv:2006.02419*, 2020.
[19]. J. Foerster, I. A. Assael, N. de Freitas, and S. Whiteson, "Learning to communicate with deep multi-agent reinforcement learning," *Advances in Neural Information Processing Systems*, pp. 2137–2145, 2016.
[20]. R. Lowe, Y. Wu, A. Tamar, J. Harb, P. Abbeel, and I. Mordatch, "Multi-agent actor-critic for mixed cooperative-competitive environments," *Advances in Neural Information Processing Systems*, pp. 6379–6390, 2017.
[21]. M. Müller, F. Hadfi, A. Ratli, and G. Nájera, "Agentic AI: A research agenda for the next generation of intelligent systems," *Artificial Intelligence*, vol. 321, pp. 103947, 2023.
[22]. J. Park, N. Bhattacharjee, and C. Li, "Communication protocols for LLM-based multi-agent systems," *Proceedings of the Conference on Neural Information Processing Systems*, pp. 3241–3255, 2024.
[23]. Ravi Kiran, Mahesh Reddy Konatham, Dharmateja Priyadarshi Uddandaraohttps://www.researchgate.net/publication/392557837_Adaptive_Model_Context_Protocols_for_Multi-Agent_Collaboration(2025).
[24]. Krishnan, Naveen. "Advancing multi-agent systems through model context protocol: Architecture, implementation, and applications." *arXiv preprint arXiv:2504.21030* (2025).
[25]. Moharir, Chandrashekhar, Sharad Shyam Ojha, and Amit Choudhury. "Contextual AI Models for Adaptive Data Classification and Access Control." (2025).
[26]. Hou, Xinyi, Yanjie Zhao, Shenao Wang, and Haoyu Wang. "Model context protocol (mcp): Landscape, security threats, and future research directions." *arXiv preprint arXiv:2503.23278* (2025).

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 5, September – October 2025 ||

DOI: 10.15680/IJCTECE.2025.0805020

[27]. Nishad, Dinesh Kumar, Vandna Rani Verma, Pushkar Rajput, Sandeep Gupta, Anurag Dwivedi, and Dharti Raj Shah. "Adaptive AI-enhanced computation offloading with machine learning for QoE optimization and energy-efficient mobile edge systems." *Scientific Reports* 15, no. 1 (2025): 15263.

[28]. Xu, Haowen, Yulin Sun, Jose Tupayachi, Olufemi Omitaomu, Sisi Zlatanova, and Xueping Li. "Towards the autonomous optimization of urban logistics: Training generative ai with scientific tools via agentic digital twins and model context protocol." *arXiv preprint arXiv:2506.13068* (2025).

[29]. Vadisetty, Rahul, and Anand Polamarasetti. "AI-generated privacy-preserving protocols for cross-cloud data sharing and collaboration." In *2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG)*, pp. 1-5. IEEE, 2024.

[30]. Narne, Suman, Tolu Adedoja, M. Mohan, and T. Ayyalasomayajula. "AI-driven decision support systems in management: enhancing strategic planning and execution." *International journal on recent and innovation trends in computing and communication* 12, no. 1 (2024): 268-276.

[31]. Bushigampala, Bharath Kumar, and Anil Chowdary Inaganti. "Threat Detection in Critical Infrastructure Using AI Models." *International Journal of Acta Informatica* 2, no. 1 (2023): 196-208.

[32]. Jordan Smith, Amelia Ethan. "Context-Aware AI-Augmented Access Control for Dynamic MFA Environments in Critical Infrastructure." (2023).

[33]. Shoaib, Mohamed R., Zefan Wang, Milad Taleby Ahvanooey, and Jun Zhao. "Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models." In *2023 international conference on computer and applications (ICCA)*, pp. 1-7. IEEE, 2023.

[34]. Reddy, Rajesh, Sonal Chopra, and Meena Singh. "Leveraging Transformer Models and Reinforcement Learning for Optimized AI-Enhanced Automated Sales Outreach." *Innovative AI Research Journal* 12, no. 1 (2023).

[35]. Haldorai, Anandakumar, Makarand Upadhyaya, G. Jawaharlal Nehru, and Dhiraj Kapila. "Self-Learning and Adaptive Networking Protocols and Algorithms for 6G Edge Nodes." In *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1-10. IEEE, 2023.