Volume 11, Issue 6, June – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

Context Aware Trust for Collaborative Cloud Infrastructure

Wajeha Zahra[1]; Salman Ahmad[2]; Dr. Usama Ahmad[3]

[1]Department of Software Engineering, Government College University Faislabad, Bahawalpur, Pakistan.
[2]Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute of Science and Technology, Sawabi, Pakistan.
[3]Professor at Government College University Faislabad, Faisalabad, Pakistan.

Publication Date: 2026/07/15

Abstract: In the current era, collaborative cloud infrastructure has allowed organizations to share computing resources, services and data in distributed systems. Abstract shows that this has allowed organizations to share computing resources, services and data across distributed systems. This paradigm enhances scalability, flexibility, and cost-effectiveness, but it also leads to substantial trust and security challenges associated with diverse community users, dynamic resource allocation, multi-tenant designs, and interactions across organizations. Existing trust management systems are based on static trust relationships and fixed access policies, which are unsuitable to deal with the dynamic environment of collaborative cloud computing. This study introduces a novel approach to address these shortcomings by proposing a Context-Aware Trust Framework (CATF) that dynamically assesses trustworthiness based on cloud entities' behaviors and contextual data. The proposed framework relies on several trust parameters, such as user behaviors, device reputation, spatial context, temporal context, history of interactions and level of sensitivity of the resources, to derive adaptive trust scores for granting access and sharing resources. The framework includes context acquisition layer, trust evaluation engine, risk assessment module and access decision component, all of which allow real-time trust assessment. A mathematical trust computation model is designed to measure trust levels and aid in dynamic decision making in collaborative cloud. In addition, an evaluation methodology based on simulations is presented to evaluate the effectiveness of the framework for the enhancement of trust accuracy, reduction of unauthorized access attacks, and enhancement of security resilience. The results reveal that context-based trust evaluation can be an effective way to enhance the security while maintaining the operational flexibility of collaborative cloud-based systems. The suggested framework helps improve the development of intelligent trust management mechanisms and offers a scalable base for secure and adaptive collaboration across cloud computing in modern distributed computing environment.

Keywords: *Context-Aware Trust, Collaborative Cloud Infrastructure, Trust Management, Cloud Security, Access Control.*

How to Cite: Wajeha Zahra; Salman Ahmad; Dr. Usama Ahmad (2026) Context Aware Trust for Collaborative Cloud Infrastructure. *International Journal of Innovative Science and Research Technology*, 11(6), 3468-3479. https://doi.org/10.38124/ijisrt/26jun2033

I. INTRODUCTION

Cloud computing has revolutionized the modern information technology by offering scalable, flexible and cost-efficient computing resources. This model of cloud infrastructure can be extended to the collaborative cloud infrastructure where multiple organizations share resources, services, and data in distributed environments (Batchu, 2025). By leveraging the principle of collaborative cloud systems, which involves resource pooling, workload distribution, and cloud-edge integration, the overall operational efficiency and utilization of resources can be enhanced, thereby supporting various applications like joint research, disaster response, and shared business intelligence platforms (Kim et al., 2019; Bao & Guo, 2022). Cooperative cloud infrastructures have been gaining interest in the world of enterprises, governments, and academic institutions as they strive to maximize cloud investments (Chen et al., 2015; Natsos & Symeonidis, 2026). Collaborative cloud environments come with a number of security and trust issues, however. With all these heterogeneous users, different security policies and dynamic resource allocation, many traditional security mechanisms might not be sufficient to address the complex attack surfaces (Feng et al., 2011; Khalil et al., 2014). Another challenge with multi-tenant architectures is unauthorized access, data isolation, and cross tenant interference (Kumar & Goyal, 2019). One aspect of trust management is especially crucial due to the varying levels of reliability and security maturity that participating organizations may have on external entities. Thus, trust issues are still a major impediment to secure cloud collaboration and cloud adoption (Singh & Chatterjee, 2017; Natsos & Symeonidis, 2026). Traditional security methods

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

like encryption, firewalls and intrusion detection systems do provide a certain degree of security but are not enough for trust-based decision making in dynamic cloud environments. Technical security controls are not the only factors that should be taken into account in a trust assessment; they should also account for historical interactions and the behaviour of the trust. Furthermore, the collaborative cloud systems are highly dynamic, with users' roles, resources availability, and network conditions continually changing, which restricts the success of static security and trust models (Ali et al., 2026). However, if adaptive trust mechanisms are not implemented, collaborative cloud infrastructures are still open to insider threats, unauthorized access, and compromised data integrity (Lombardi et al., 2024).

A solution that takes context into account is possible and that is what context-aware trust management does—it uses environmental, behavioral, and situational data to make trust calculations. Previous studies have demonstrated that the accuracy of the trust assessment can be significantly enhanced by considering the contextual information such as user behavior, device attribute, location, time, and resource sensitivity in the distributed systems (Liu et al., 2018; Li et al., 2019). For the most part, prior work has concentrated on different domains like the Internet of Things, social networks, and vehicular systems, and has neglected to attend to collaborative cloud infrastructures (Tyagi et al., 2023; Chahal et al., 2020). Currently, many approaches involve evaluating trust statically, which cannot adjust well to evolving operational situations and new security threats (Konsta et al., 2023). This restriction exposes major challenges in the research of developing context-aware and adaptive trust frameworks for collaborative cloud environments (Gangwani et al., 2024). In order to fill this gap, this study presents a Context-Aware Trust Framework (CATF) for collaborative cloud infrastructures. A number of parameters are incorporated into the framework to enable dynamic trust computation and adaptive access control, such as user behavior, device trustworthiness, location, temporal context, historical interactions and resource sensitivity. The suggested framework is a modular architecture that includes context acquisition, context processing, trust evaluation, risk assessment and access control modules. Evaluation of the framework in terms of its effectiveness to increase the trust accuracy, detection of unauthorized access and increase of security resilience is performed by means of simulation. The results can help to further develop trust management approaches for secure and scalable collaborative cloud infrastructures.

II. LITERATURE REVIEW

- *Collaborative Cloud Infrastructure*

Collaborative cloud infrastructure is a system where two or more organizations share computing resources, data and services to accomplish shared goals. It can be used by multiple organizations to collaborate and coordinate the use of resources across administrative lines, whereas traditional cloud models are confined to a single organization. For applications that need to share processing power, resource pooling and workload distribution enhance computational efficiency, scalability and service performance, making collaborative cloud environments appropriate. (Kim et al., 2019) With the widespread adoption of cloud/edge computing, the resource utilization is further improved by enabling latency-sensitive applications and ensuring centralized management (Bao & Guo, 2022). They can be used in various areas such as scientific research, smart infrastructure management, disaster response, and business intelligence where multiple entities need to access the shared resources with security (Chen et al., 2015). However, collaborative cloud infrastructures have some important security and trust issues. Having multiple organizations operating with varying security policies and operational requirements makes handling the system more complex and there are new attack surfaces created. Defensive strategies for collaborative cloud environments must be able to meet the challenges of collaborative users, distributed ownership and evolving trust relationships, according to Natsos and Symeonidis (2026). This has made the Trust Management a basic need to ensure trustworthy collaborations and at the same time, the efficient resource sharing (Singh & Chatterjee, 2017).

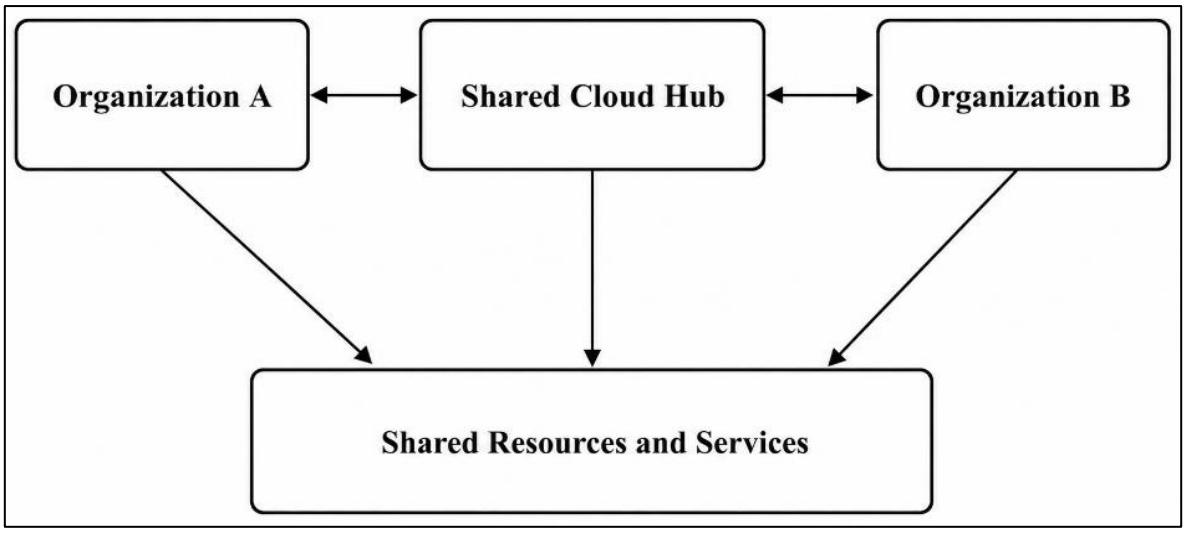

Fig 1 Collaborative Cloud Environment

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

➢ *Trust Management in Cloud Computing*

Trust management offers a way to assess the trustworthiness and reliability of cloud entities, services, and users. Earlier on, there are three types of traditional trust models; namely, reputation-based, policy-based, and hybrid. The models rely on direct interactions, recommendations, service quality indicators, and security policies to calculate trust scores to aid decision-making processes (Yan et al., 2014). Researchers have stressed the necessity for adapting trust mechanisms as cloud environments are getting more dynamic. Chahal et al. (2020) highlighted certain difficulties such as scalability, trust evolution and resistance to malicious behavior. The potential application of blockchain technology in creating decentralized and tamper-proof trust records has been examined in recent studies, offering a glimpse into how blockchain can enhance transparency and mitigate reliance on central entities (Liu et al., 2023). Also, other studies have emphasized the need for privacy preservation, interoperability and integration of machine learning in contemporary trust framework (Konsta et al., 2023; Arshad et al., 2023; Ud Din et al., 2019). The developments prove that the trust management is moving from the reputation-based, statically designed ones to the intelligent and adaptive ones that can be used in large-scale distributed environments. But many current approaches are still challenged to adapt quickly to the dynamic nature of clouds and advanced attack techniques.

➢ *Context-Aware Trust Management*

Context-aware computing is the ability of systems to react to information about the environment, situation and user. In trust management, contextual information of trust is used to improve the decisions that are made beyond mere static trust scores. The study by Liu et al. (2018) showed that using a context-aware trust mechanism gives more accurate trust inferences than traditional methods by taking into account other parameters like location, time, condition of the device, relationship history, and environment. A few studies have used context-aware trust management to various fields. Karthik and Ananthanarayana (2019) added contextual information to the medical decision on trust in healthcare systems and Rehman et al. (2022) came up with a context-aware trust framework in the vehicular network. Similar approaches have been conducted in fog computing systems, service-oriented systems, and IoT systems (Wang et al., 2018; Li et al., 2019; Hussain et al., 2020; Jang et al., 2022). In recent years, machine learning, reinforcement learning, probabilistic reasoning and trust evaluation based on blockchain have been used to enhance trust prediction and adaptation capabilities (Ahmed et al., 2023; Aldini et al., 2024; Hasan et al., 2025; He et al., 2025). While these advances bring context-aware systems closer to their ideal, they can still be subject to context manipulation attacks where adversaries can input misleading contextual data to bias trust decisions (Lewis et al., 2023). The results of this study reveal the need for more resilient context-aware trust frameworks which are able to validate contextual information and adapt to emerging threats.

➢ *Trust Evaluation Models*

Trust evaluation models are the basis for computing the trustworthiness of distributed systems. Current models use mathematical, statistical, and machine learning approaches to produce trust scores based on direct observation, recommendations, and context (Gangwani et al., 2024). Since trust is a multifaceted concept, it has been proved to be more accurate than traditional reputation-based methods when combined with service quality, security compliance, behavioral history and contextual attributes (Alhanahn et al., 2018). The results of Wang et al. (2018), Hussain et al. (2020) and Rehman et al. (2022) indicated that the use of multiple trust parameters will increase the accuracy of the decision and will be adaptive. Most existing models have, however, static trust parameters and only use a context-based adaptation, which makes them less effective in a highly dynamic cloud environment. However, researchers still go on recommending adaptive trust calculation methods capable of adapting to the changing behaviors and emerging threats (Tyagi et al., 2023; Chahal et al., 2020).

➢ *Security Threats in Collaborative Cloud Systems*

However, the distributed and multi-organizational nature of collaborative cloud infrastructures exposes them to a large number of potential security dangers. Lewis et al. (2023) discovered attacks that take advantage of the inadequacies of trust evaluation mechanisms to gain access to unauthorized resources. The other notable risks are insider attacks, data leakage, resource hijacking, account compromise, insecure interfaces, and vulnerabilities due to shared technology (Kumar & Goyal, 2019; Natsos & Symeonidis, 2026). To overcome these threats, researchers have suggested several strategies, such as continuous risk assessment, adaptive access control, automated threat detection, and defense-in-depth security strategies (Ali et al., 2026; Pitkar, 2025). With the use of a machine learning approach, security solutions are becoming more sophisticated to enhance anomaly detection and threat response (Lombardi et al., 2024; Alzoubi et al., 2024). Although these methods improve cloud security, they rely on the quality and adaptiveness of trust evaluation mechanisms.

Table 1 Summary of Existing Trust Framework

Approach	Strengths	Limitations
Reputation-Based	Simple implementation	Limited adaptability
Policy-Based	Strong rule enforcement	Poor contextual awareness
Hybrid Models	Improved reliability	Increased complexity
Context-Aware Models	Dynamic trust evaluation	Vulnerable to context attacks
Blockchain-Based Models	Transparency and immutability	Computational overhead
AI-Driven Models	Adaptive learning capability	High resource requirements

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

➢ *Research Gap*

The following are some important research gaps identified from the literature. First, even though collaborative cloud infrastructures are unique multi-organizational infrastructures, they are not quite as explored as other trust frameworks such as IoT, social networking, and vehicular systems in the literature (Tyagi et al., 2023; Konsta et al., 2023). Second, most of the current models are based on static trust values, which are unable to adapt to user behavior changes, resource allocation patterns and new threats (Chahal et al., 2020). Third, existing frameworks tend to only look at a narrow list of contextual factors, which means that their assessments of trust are partial (Alhanahnah et al., 2018; Wang et al., 2018). Fourth, lack of integration of risk assessment mechanisms diminishes resilience to the advanced attacks that can be executed in context (Lewis et al., 2023). Practical issues, such as scalability, computational cost, deployment complexity and unified trust computation, are still not well tackled (Natsos & Symeonidis, 2026; Hasan et al., 2025). These restrictions encourage the creation of a powerful Context-Aware Trust Framework (CATF) that can incorporate various contextual parameters, adaptive computation of trust, and risk-aware decisions for ensuring safe cooperative cloud infrastructures.

III. METHODOLOGY

➢ *Research Design*

This research is a quantitative simulation-based study to test the proposed Context-Aware Trust Framework (CATF) in collaborative cloud environments. Simulations allow the safe testing of trust management mechanisms in different operational settings and security attack scenarios that are not feasible in the actual cloud deployment context (Kim et al., 2019; Gangwani et al., 2024). It takes into account collaborative cloud use cases like access to shared multi-tenant resources, cross-organizational access, and dynamically allocated resources. These scenarios are performed in normal and hostile conditions, including the possibility of insider threats, attempts to access unauthorized systems, and attempts to manipulate the context (Lewis et al., 2023). Improvements in trust assessment and access control are measured against the success of the framework. Existing trust management approaches are compared with the success of the framework to determine improvements in trust assessment and access control. The research involves four steps: setting up the simulation environment, generating the scenarios, implementing the framework, and evaluating the performance of the framework, providing a comprehensive and repeatable evaluation of the proposed framework.

➢ *Framework Implementation*

The CATF is applied in a systematic manner with components development, parameter configuration, integration, test and deployment. The framework consists of six interrelated modules which all contribute to context-aware trust management. The Context Acquisition Layer collects information like user behavior, device characteristics, location and access time. The Context Processing Layer processes the collected data, filters and classifies it to create meaningful contextual information. The Trust Evaluation Engine generates trust scores based on weighted trust parameters, and the Risk Assessment Module assesses the risks of access requests to the security system. The Access Control Module makes a decision on access based on the trust and risk evaluations. The Module Monitoring and Feedback constantly refreshes the information about trust based on user activities and interactions with the system. In implementation, trust parameters and weighting factors are set based on the collaborative cloud security requirements, along with the decision threshold. Environmental factors (including context-adjustment factors) are integrated to reflect conditions of the environment (e.g. location, time, resource sensitivity). The modules are connected to each other via standardized interfaces, which allows them to work together seamlessly and to exchange data efficiently. To validate functionality and confirm end-to-end trust evaluation processes, unit and integration testing are conducted. The framework is then applied in the simulation environment with pre-defined simulation parameters such as the duration of the simulation, the number of users, the categories of resources and the trust scenarios.

➢ *Data Collection and Context Generation*

As this study is not deployed in the real-world, synthetic datasets were created to simulate realistic collaborative cloud activities. The users generated data consists of user profiles, device features, location, temporal access pattern, interaction history, and the classification of the resources (Jang et al., 2022). Baselines (user profiles) are used to establish behavioral baselines and device attributes are used to evaluate the trustworthiness of the device. Location data can be used to evaluate access legitimacy while temporal patterns can be used for analyzing time-based behavioural variations. The interaction histories are used for historical trust calculations while the resource catalogs categorizes the resources by sensitivity. These datasets produce realistic access requests and access patterns of users and allow for the continuous evaluation of trust and adaptation of trust during the simulation process.

➢ *Simulation Environment*

The simulation environment is a controlled environment to test CATF under different threat and operation environments. It represents multiple organizations, users, administrative domains, and common cloud resources to reflect the real collaborative cloud infrastructures. The simulator can be used to simulate dynamic resource allocation, interactions between different organizations, and network parameters, including latency and bandwidth fluctuations (Kim et al., 2019; Bao & Guo, 2022). A trust scenario engine is used to create the pre-defined operational and attack scenarios, such as normal user activities, insider attacks, unauthorized access attempts, and context-based attacks (Lewis et al., 2023). Such scenarios can be automatically executed, resulting in uniformity between experiments and making it easier to compare them. By using a standardized integration interface, CATF and the existing trust management methodologies will be able to run in the same simulation environment and therefore can be fairly compared. Additionally, a system for performance monitoring captures trust scores, access decisions, threat detection results, response

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

times and resource usage metrics. These records give quantitative data to assess the effectiveness of the framework, and also for comparative performance analysis (Gangwani et al., 2024).

➢ *Evaluation Metrics*

The effectiveness of Context-Aware Trust Framework (CATF) is measured by means of Trust Accuracy, Detection Rate, False Positive Rate, Response Time and Scalability. Trust Accuracy is the accuracy of trust judgments based on comparing the outcomes of the predictions made with the actual outcomes.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Where:

TP = True Positives
TN = True Negatives
FP = False Positives
FN = False Negatives

The higher accuracy value the more reliable the trust evaluation. Detection Rate, or True Positive Rate, is the framework's ability to accurately determine if malicious entities or security threats exist.

$$\text{Detection Rate} = \frac{TP}{TP+FN} \quad (2)$$

Higher detection rates indicate stronger threat-identification capability.

False Positive Rate (FPR) quantifies the proportion of legitimate entities incorrectly classified.

$$\text{False Positive Rate} = \frac{FP}{FP+TN} \quad (3)$$

Lower FPR values are desirable because excessive false alarms can negatively affect legitimate user activities.

Response Time measures the duration required for trust evaluation and access-decision generation. Lower response times indicate better real-time performance.

$$\text{Response Time} = t_{decision} - t_{request} \quad (4)$$

Where:

- $T_{request}$ = time at which the access request is submitted
- $T_{decision}$ = time at which the trust decision is generated

Evaluation of scalability is performed by gradually adding number of users, number of cloud resources, and number of concurrent requests and duration of the simulation. Scalability of CATF depends on its stability with respect to its values of Accuracy, Detection Rate, False Positive Rate, and Response Time with growth in workloads. A scalable trust management framework should be able to meet the performance requirements even as the number of users and resources increases and the number of requests increases, showing it to be suitable for large-scale collaborative cloud infrastructures.

IV. RESULTS AND DISCUSSION

➢ *Trust Accuracy Performance*

The first experiment investigated whether or not the trust assessment was accurate across various operational scenarios. CATF was compared with a Static Trust Model (STM) and a Reputation-Based Trust Model (RTM). Normal activities, insider threats, unauthorized access attempts and context manipulation attacks were simulated.

Table 2 Trust Accuracy Comparison

Framework	Normal (%)	Insider Attack (%)	Unauthorized Access (%)	Context Attack (%)	Average (%)
STM	89.4	81.6	79.3	74.8	81.3
RTM	92.1	87.5	85.8	82.4	86.9
Proposed CATF	97.2	95.4	94.8	92.6	95.0

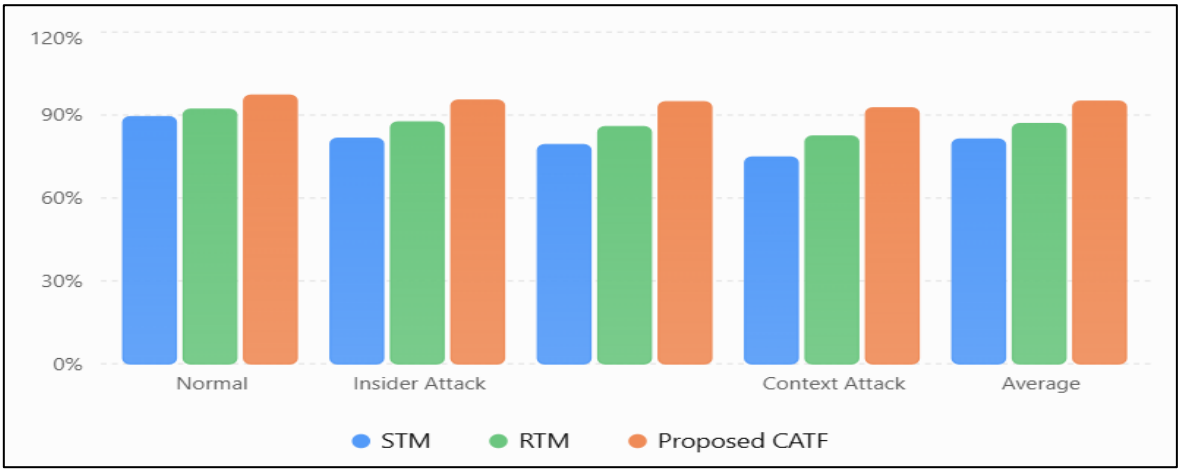

Fig 2 Comparison of STM, RTM, and the Proposed CATF Under Different Operational Scenarios

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

The results show that the accuracy of trust obtained by CATF was always better than other algorithms in all scenarios. The framework showed an average accuracy of 95.0% which was better than RTM and STM by 8.1% and 13.7%, respectively. This improvement comes from the embedding of several contextual parameters, such as user's behavior, device trustworthiness, location and temporal. CATF dynamically updated trust scores as the context changed to reflect the accuracy of the trust assessment, unlike the static approaches.

➢ *Unauthorized Access Detection*.

The second experiment was to test the capacity of each framework to detect malicious activity and unauthorized access attempts.

Table 3 Detection Rate Performance

Framework	Detection Rate (%)
STM	78.5
RTM	86.9
Proposed CATF	95.8

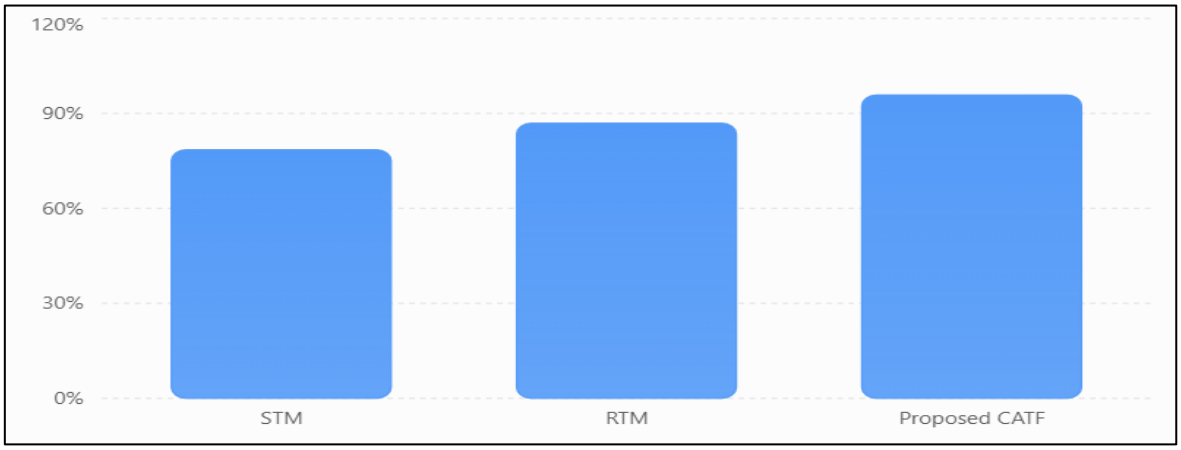

Fig 3 Detection Rate Comparison Among STM, RTM, and the Proposed CATF.

The proposed framework had the highest detection rate of 95.8%. The results show that contextual awareness has a significant impact regarding the capability to identify threats. CATF was able to successfully identify malicious activity, which was not detected by traditional trust mechanisms, by leveraging behavioral analysis and contextual validation. The results are in line with the past research indicating that context-aware trust systems offer greater security resilience in dynamic environments.

➢ *False Positive Analysis*

A false positive is when a legitimate user is misidentified as a malicious user. Too many false-positives decreases usability and impact on user experience.

Table 4 False Positive Rate Comparison

Framework	False Positive Rate (%)
STM	9.8
RTM	6.3
Proposed CATF	3.1

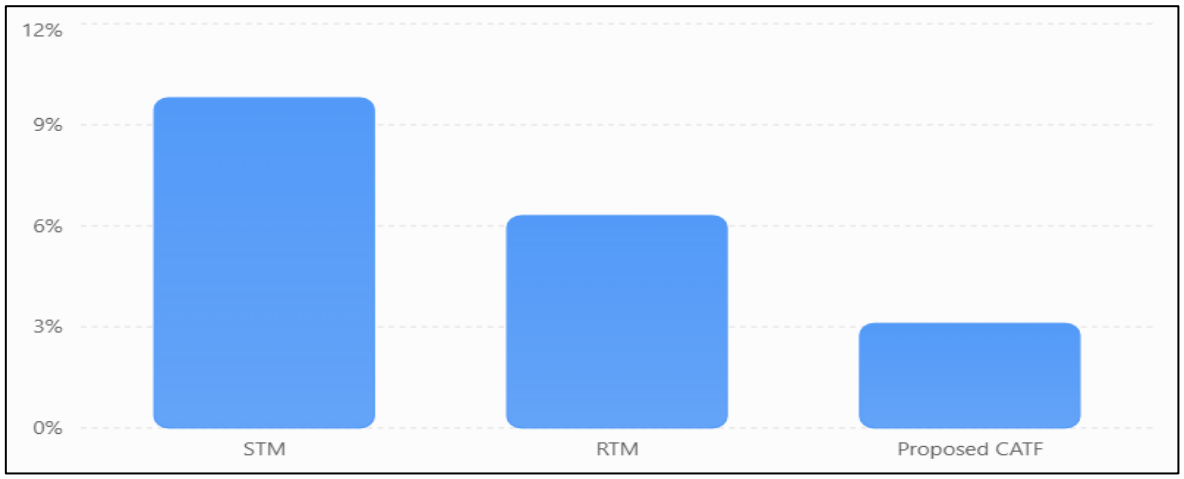

Fig 4 False Positive Rate Comparison Among STM, RTM, and the Proposed CATF.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

The false positive rate was lowest for CATF, at 3.1%, which is a significant improvement over the benchmark frameworks. Multiple trust indicators helped to reduce the dependency on single trust parameters and to minimize incorrect classification. This outcome showcases the framework's capability to achieve security requirements while maintaining operational efficiency.

➢ *Response Time Evaluation*

Trust is pivotal in collaborative cloud settings, and real-time trust estimation is essential. The response time experiment used the average time to process access requests and develop trust-based decisions.

Table 5 Average Response Time

Framework	Response Time (ms)
STM	28
RTM	39
Proposed CATF	46

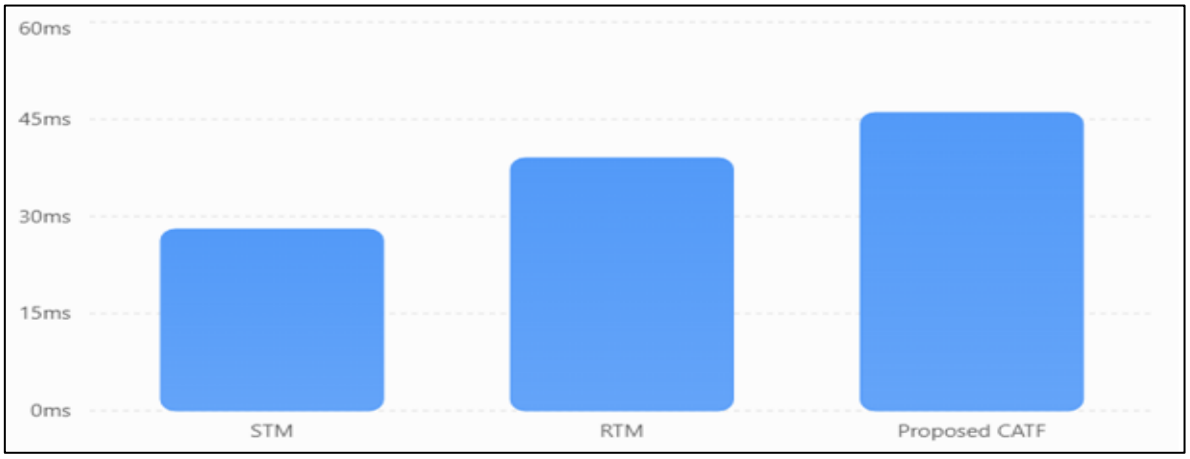

Fig 5 Response Time Comparison Among STM, RTM, and the Proposed CATF

The proposed framework showed a slightly longer response time compared to STM and RTM because of a few more contextual processing and risk assessment operations. But the average response time was 46ms, which is still within a good time range for real-time cloud access control. The additional complexity of calculating the computation is outweighed by the significant improvement in the accuracy of the trust and threat detection.

➢ *Scalability Assessment*

In the scalability experiment we investigated the performance of the framework with different workloads.

Table 6 Scalability Results

Workload Level	Accuracy (%)	Detection Rate (%)	False Positive Rate (%)	Response Time (ms)
Low	97.2	96.1	2.8	39
Medium	96.4	95.7	3.0	46
High	95.0	94.9	3.4	58

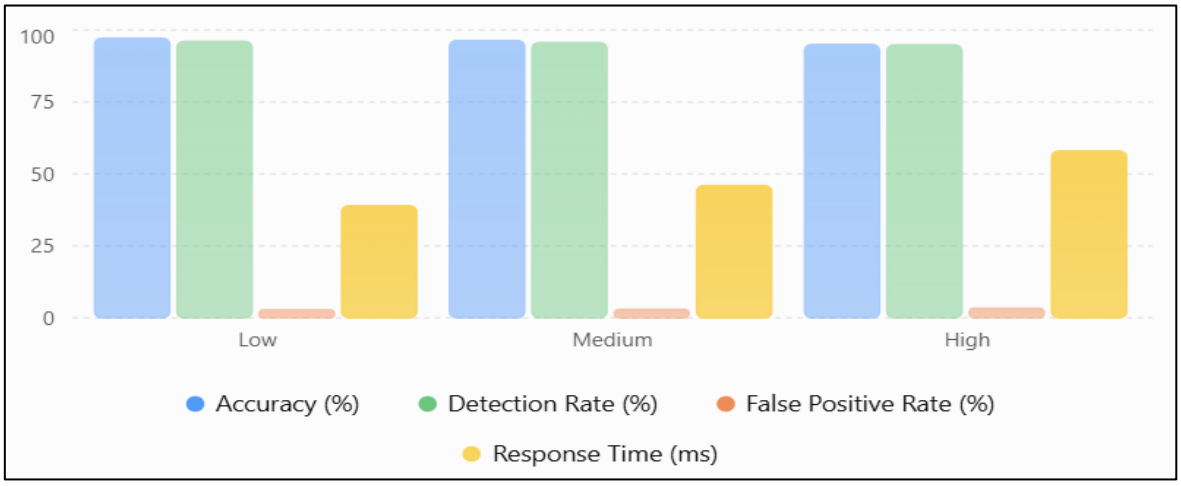

Fig 6 Performance Variation of CATF Under Different Workload Levels.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

The results show that the number of users, resources and concurrent requests had no effect on the performance of CATF. However, accuracy and detection performance stayed above 94% for high workloads, showing that it is very scalable. The framework proved to be robust and robust with regard to security performance in the large scale collaborative cloud settings.

➢ *Impact of Contextual Parameters*

In an ablation experiment the influence of each contextual parameter on the overall accuracy of trust was examined.

Table 7 Contribution of Contextual Parameters

	Accuracy (%)
Full CATF	95.0
Without User Behavior	91.6
Without Device Trust	92.3
Without Location Context	93.1
Without Temporal Context	93.6
Without Historical Interaction	90.8

The results indicate that the most significant factors in the accuracy of the evaluation of trust are the historical interactions and user behavior. Both parameters were found to have a significant effect when removed. The trustworthiness of the devices, their location, and temporal context also were important factors for improving trust assessment, further indicating the need to merge multiple dimensions of context into the trust computation process.

➢ *Discussion*

The experimental results confirm the success of the proposed Context-Aware Trust Framework in solving trust management problems in collaborative cloud infrastructures. Finally, in all measures, CATF performed significantly better than traditional trust models, demonstrating higher trust accuracy, better ability to detect threats and lower false positive rates. The reason for these improvements is that the framework is able to assess the trust dynamically by considering contextual information and not only static trust relationships or reputation scores. The results also show that context-awareness is an important component in detecting malicious behavior in dynamic cloud environments. CATF's integration of user behavior, device trustworthiness, location, temporal patterns and historical interactions led to more accurate trust ratings and better access-control decisions. The results of the ablation study validated the need for multidimensional trust evaluation, as no single contextual parameter was sufficient to achieve the best performance. CATF added a certain amount of computational overhead, but the added response time was not significant and had no impact on real-time operation. The framework's scalability characteristics were demonstrated by running the experiments with different workloads and showing stable performance even as the workload increased, making the framework ideal for large-scale collaborative cloud deployments. Overall, the results corroborate the research hypothesis that contextual information is useful in computing trust and can greatly improve the security, trustworthiness, and resistance to new threats in collaborative cloud environments.

V. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

➢ *Limitations of the Framework*

The proposed Context-Aware Trust Framework (CATF) exhibited overall good performance, however a few limitations should be noted. The first is that the framework relies critically on the availability, accuracy and timeliness of the contextual data. As the evaluations of trust depend upon contextual information like user behavior, device features, location, and previous interactions, incomplete or unreliable information could impact the precision of the trust evaluation (Tyagi et al., 2023; Chahal et al., 2020). A major difficulty in collaborative cloud environments with several administrative domains is keeping the data quality consistent. Second, the real-time context processing and dynamic computation of trust adds to the computational overhead. Although the simulation results demonstrated good response times, deployments involving thousands of users and many access requests could result in higher processing delays (Hussain et al., 2020; Gangwani et al., 2024). Additional testing is needed to establish the performance of the framework under extreme operating conditions. Another constraint is the evaluation approach that is based on simulations. While trusting a cloud environment is a powerful way to test the trust mechanisms, synthetic datasets and attack scenarios may not capture the complexity of real-world collaborative cloud infrastructures (Kim et al., 2019). Therefore, the framework must be tested in actual field, practical deployment and real operational environment. It also uses pre-defined parameters and weights to trust and may not be equally representative in any organization. The variations of security policies, operational goals, and risk tolerance might need customized trust configurations to optimize performance (Alhanahn et al., 2018; Wang et al., 2018). Furthermore, while the framework includes a section on attacks involving the manipulation of context, the robustness against newly emerging attack techniques and advanced adversarial strategies need further investigation (Lewis et al., 2023). Finally, the framework makes the assumption of a reasonable level of cooperation between the participating organisations. The implementation of information sharing and trust verification can be more challenging in settings where the interests of the parties are not aligned or there is limited trust between them (Ahmed et al., 2023; Arshad et al., 2023).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

➢ *Future Research Directions*

Advanced AI techniques can be incorporated into the proposed framework in the future to further strengthen it. For these complex behavioral patterns and prediction of trustworthiness, machine learning and deep learning models have proven to be effective, particularly in dynamic settings (Wang et al., 2023; Hasan et al., 2025). The application of AI to trust prediction might allow for the development of adaptive trust management systems, which would learn from past success and failures and dynamically modify their trust levels and parameter weights, as well as access-control decisions. Reinforcement learning models can also enhance the evaluation of the level of trust, leveraging on the observed performance of the system and changes in threat situations (He et al., 2025). In addition, future research would require further consideration of explainability and transparency, so that trust decisions from the AI systems are easily understood and accountable (Um et al., 2022). There are new improvements to consider such as the blockchain technology. Blockchain can enable decentralized trust management, immutability of trust records, and transparent trust-related activities verification (Liu et al., 2023). Smart contracts might automate access control policies and trust enforcement, and decrease the need for centralized authorities. This is especially useful in multi-organizational collaborative cloud solutions. However, blockchain acceptance poses difficulties in terms of scalability, latency, and processing costs, demanding attention via lightweight, hybrid, and hybrid blockchain constructions (Punia et al., 2024). Federated learning also has many potential applications to the future of trust management. Federated learning can help preserve privacy while harnessing knowledge across multiple organizations, without sharing all the data centrally (Bao & Guo, 2022). The method would enable trust prediction models to gain from the multitude of operational experiences but not reveal sensitive data. Research is needed on personalized federated learning approaches that can be used with organizational variations and still benefit the collective learning. One potentially exciting path to explore is the synergistic marriage of AI, blockchain, and federated learning into a single trust paradigm. This could involve leveraging intelligent trust prediction, decentralized trust verification, and privacy-preserving collaborative learning to develop highly adaptive and resilient trust management systems. Further studies are needed to investigate the transfer learning, interoperability standards, and cross-platform trust management for the deployment in different collaborative cloud infrastructures. Such advances would further improve the precision, extensibility, transparency and security in the evaluation of trust, and continue to develop secure collaborative cloud environments.

VI. CONCLUSION

In recent years, collaborative cloud infrastructures have proven to be an effective means of resource sharing, service integration and cross-organizational collaboration. Yet these are environments that are both dynamic and heterogeneous, posing many trust and security challenges that cannot be solved with the traditional monostatic trust models. Current solutions can't keep pace with users' behavior, context, and new security challenges, reducing the benefits they provide in collaborative cloud environments. The study suggested a Context-Aware Trust Framework (CATF) that was tailored for collaborative cloud infrastructures. The framework incorporates several contextual factors such as user behaviour, device trustworthiness, location, time, history of interactions and the sensitivity of the resource in order to build a dynamic trust computation and adaptive access-control decision. To support full-fledged trust management in distributed cloud environments, a modular structure of context acquisition, context processing, trust evaluation, risk assessment, monitoring, and access-control was built. The framework was tested using metrics like the accuracy of trust, detection rate, false positive rate, response time and scalability by simulating experiments. The experimental results showed that CATF outperformed the conventional trust management strategies in all the evaluation criteria. This framework had high accuracy of trust, high detection accuracy of unauthorized access attempts, a small number of false positive and stable performance with load increasing. The computation time was acceptable for real-time cloud operation despite the computational overhead of contextual processing. The scalability analysis also confirmed the suitability of the framework to deploy large-scale collaborative cloud. The results suggest that contextual information is crucial in trust evaluation processes. The proposed framework uses multi-dimensional contextual information to achieve better and adaptive trust evaluation compared to the traditional static or reputation-based models. As a result, CATF increases the security resiliency, access-control decisions and trust relationships between collaborating security organizations. The study presents an extensive context-aware framework and proves the efficacy of the framework using quantitative evaluation, thereby making a significant contribution to the development of trust management in collaborative cloud computing. The proposed approach provides a practical basis to create secure, scalable and adaptive trust management solutions to meet the increasing demands of modern cloud collaborative environment.

REFERENCES

[1]. Liu, G., Liu, Y., Liu, A., Li, Z., Zheng, K., Wang, Y., & Zhou, X. (2018). Context-aware trust network extraction in large-scale trust-oriented social networks. *World Wide Web*, *21*(3), 713–738. https://doi.org/10.1007/s11280-017-0485-6

[2]. Karthik, N., & Ananthanarayana, V. S. (2019). Context Aware Trust Management Scheme for Pervasive Healthcare. *Wireless Personal Communications*, *105*(3), 725–763. https://doi.org/10.1007/s11277-018-6091-9

[3]. Alhanahnah, M., Bertok, P., Tari, Z., & Alouneh, S. (2018). Context-Aware Multifaceted Trust Framework For Evaluating Trustworthiness of Cloud Providers. *Future Generation Computer Systems*, *79*, 488–499. https://doi.org/10.1016/j.future.2017.09.071

[4]. Rehman, A., Hassan, M. F., Hooi, Y. K., Qureshi, M. A., Shukla, S., Susanto, E., … Abdel-Aty, A. H. (2022). CTMF: Context-Aware Trust Management Framework for Internet of Vehicles. *IEEE Access*, *10*, 73685–

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

73701. https://doi.org/10.1109/ACCESS.2022.3189349

[5]. Wang, Y., Chen, I. R., Cho, J. H., Swami, A., Lu, Y. C., Lu, C. T., & Tsai, J. J. P. (2018). CATrust: Context-aware trust management for service-oriented Ad Hoc networks. *IEEE Transactions on Services Computing*, *11*(6), 908–921. https://doi.org/10.1109/TSC.2016.2587259

[6]. Li, N., Varadharajan, V., & Nepal, S. (2019). Context-aware trust management system for IoT applications with multiple domains. In *Proceedings - International Conference on Distributed Computing Systems* (Vol. 2019-July, pp. 1138–1148). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICDCS.2019.00116

[7]. Jang, S. Y., Park, S. K., Cho, J. H., & Lee, D. (2022). CARES: Context-Aware Trust Estimation for Realtime Crowdsensing Services in Vehicular Edge Networks. *ACM Transactions on Internet Technology*, *22*(4). https://doi.org/10.1145/3514243

[8]. Lewis, C., Li, N., & Varadharajan, V. (2023). Targeted Context-Based Attacks on Trust Management Systems in IoT. *IEEE Internet of Things Journal*, *10*(14), 12186–12203. https://doi.org/10.1109/JIOT.2023.3245605

[9]. Aldini, A., Curzi, G., Graziani, P., & Tagliaferri, M. (2024). A probabilistic modal logic for context-aware trust based on evidence. *International Journal of Approximate Reasoning*, *169*. https://doi.org/10.1016/j.ijar.2024.109167

[10]. Hasan, A. A., Fang, X., Latif, S., & Iqbal, A. (2025). Context-Aware Trust Prediction for Optimal Routing in Opportunistic IoT Systems. *Sensors*, *25*(12). https://doi.org/10.3390/s25123672

[11]. He, Y., Han, G., Jiang, J., Cheng, X., & Xu, P. (2025). CADTR: Context-Aware Trust Routing Algorithm Based on Priority Sampling DDPG for UASNs. *IEEE Transactions on Mobile Computing*, *24*(11), 11688–11702. https://doi.org/10.1109/TMC.2025.3581512

[12]. Siddiqui, S. A., Mahmood, A., Sheng, Q. Z., Suzuki, H., & Ni, W. (2023). Trust in Vehicles: Toward Context-Aware Trust and Attack Resistance for the Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *24*(9), 9546–9560. https://doi.org/10.1109/TITS.2023.3268301

[13]. Wang, Y., Li, L., & Liu, G. (2015). Social context-aware trust inference for trust enhancement in social network based recommendations on service providers. *World Wide Web*, *18*(1), 159–184. https://doi.org/10.1007/s11280-013-0241-5

[14]. Singh, J., Dhurandher, S. K., Woungang, I., & Chao, H. C. (2024). Context-Aware Trust and Reputation Routing Protocol for Opportunistic IoT Networks. *Sensors*, *24*(23). https://doi.org/10.3390/s24237650

[15]. Ahmed, W., Di, W., & Mukathe, D. (2023). Blockchain-Assisted Privacy-Preserving and Context-Aware Trust Management Framework for Secure Communications in VANETs. *Sensors*, *23*(12). https://doi.org/10.3390/s23125766

[16]. Hussain, Y., Zhiqiu, H., Akbar, M. A., Alsanad, A., Alsanad, A. A. A., Nawaz, A., … Khan, Z. U. (2020). Context-Aware Trust and Reputation Model for Fog-Based IoT. *IEEE Access*, *8*, 31622–31632. https://doi.org/10.1109/ACCESS.2020.2972968

[17]. Wang, Q., Zhao, W., Yang, J., Wu, J., Xue, S., Xing, Q., & Yu, P. S. (2023). C-DeepTrust: A Context-Aware Deep Trust Prediction Model in Online Social Networks. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(6), 2767–2780. https://doi.org/10.1109/TNNLS.2021.3107948

[18]. Gupta, S., Modgil, S., Kumar, A., Sivarajah, U., & Irani, Z. (2022). Artificial intelligence and cloud-based Collaborative Platforms for Managing Disaster, extreme weather and emergency operations. *International Journal of Production Economics*, *254*. https://doi.org/10.1016/j.ijpe.2022.108642

[19]. Batchu, S. (2025). BEYOND AUTOMATION: AI-HUMAN COLLABORATIVE FRAMEWORK FOR OPTIMIZING CLOUD INFRASTRUCTURE MANAGEMENT. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY*, *16*(1), 1893–1908. https://doi.org/10.34218/ijcet_16_01_137

[20]. Kim, H. W., Kang, J., & Jeong, Y. S. (2019, August 1). Simulator considering modeling and performance evaluation for high-performance computing of collaborative-based mobile cloud infrastructure. *Journal of Supercomputing*. Springer Science and Business Media, LLC. https://doi.org/10.1007/s11227-019-02882-x

[21]. Bao, G., & Guo, P. (2022, December 1). Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. *Journal of Cloud Computing*. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s13677-022-00377-4

[22]. Chen, Z., Chen, J., Shen, F., & Lee, Y. (2015). Collaborative Mobile-Cloud Computing for Civil Infrastructure Condition Inspection. *Journal of Computing in Civil Engineering*, *29*(5). https://doi.org/10.1061/(asce)cp.1943-5487.0000377

[23]. Natsos, D., & L. Symeonidis, A. (2026). Towards a Defense-in-Depth Approach for Securing Collaborative Cloud Infrastructures. In *Lecture Notes in Computer Science* (Vol. 16083 LNCS, pp. 409–418). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-032-04207-1_27

[24]. Tyagi, H., Kumar, R., & Pandey, S. K. (2023). A detailed study on trust management techniques for security and privacy in IoT: challenges, trends, and research directions. *High-Confidence Computing*, *3*(2). https://doi.org/10.1016/j.hcc.2023.100127

[25]. Chahal, R. K., Kumar, N., & Batra, S. (2020, January 15). Trust management in social Internet of Things: A taxonomy, open issues, and challenges. *Computer Communications*. Elsevier B.V. https://doi.org/10.1016/j.comcom.2019.10.034

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

[26]. Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jantti, R. (2023). A Survey on Blockchain-Based Trust Management for Internet of Things. *IEEE Internet of Things Journal*, *10*(7), 5898–5922. https://doi.org/10.1109/JIOT.2023.3237893

[27]. Gangwani, P., Perez-Pons, A., & Upadhyay, H. (2024). Evaluating Trust Management Frameworks for Wireless Sensor Networks. *Sensors*, *24*(9). https://doi.org/10.3390/s24092852

[28]. Ud Din, I., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2019). Trust management techniques for the internet of things: A survey. *IEEE Access*, *7*, 29763–29787. https://doi.org/10.1109/ACCESS.2018.2880838

[29]. Arshad, Q. ul A., Khan, W. Z., Azam, F., Khan, M. K., Yu, H., & Zikria, Y. B. (2023). Blockchain-based decentralized trust management in IoT: systems, requirements and challenges. *Complex and Intelligent Systems*, *9*(6), 6155–6176. https://doi.org/10.1007/s40747-023-01058-8

[30]. Um, T. W., Kim, J., Lim, S., & Lee, G. M. (2022). Trust Management for Artificial Intelligence: A Standardization Perspective. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12126022

[31]. Hou, M., Banbury, S., Cain, B., Fang, S., Willoughby, H., Foley, L., … Rudas, I. J. (2025). IMPACTS Homeostasis Trust Management System: Optimizing Trust in Human-AI Teams. *ACM Computing Surveys*, *57*(6). https://doi.org/10.1145/3649446

[32]. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, *42*, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014

[33]. Konsta, A. M., Lafuente, A. L., & Dragoni, N. (2023). A Survey of Trust Management for Internet of Things. *IEEE Access*, *11*, 122175–122204. https://doi.org/10.1109/ACCESS.2023.3327335

[34]. Feng, D. G., Zhang, M., Zhang, Y., & Xu, Z. (2011). Study on Cloud Computing security. *Ruan Jian Xue Bao/Journal of Software*, *22*(1), 71–83. https://doi.org/10.3724/SP.J.1001.2011.03958

[35]. Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1). https://doi.org/10.3390/computers3010001

[36]. Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*. Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2019.05.002

[37]. Lombardi, F., Di Pietro, R., & Signorini, M. (2024). Cloud Security. In *Computer and Information Security Handbook, Fourth Edition: Volumes 1-2* (Vol. 2, pp. 1081–1092). Elsevier. https://doi.org/10.1016/B978-0-443-13223-0.00065-5

[38]. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2026). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*. Taylor and Francis Ltd. https://doi.org/10.1080/08874417.2024.2329985

[39]. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. *Artificial Intelligence Review*, *57*(5). https://doi.org/10.1007/s10462-024-10776-5

[40]. Singh, A., & Chatterjee, K. (2017, February 1). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*. Academic Press. https://doi.org/10.1016/j.jnca.2016.11.027

[41]. Pitkar, H. (2025). Cloud Security Automation Through Symmetry: Threat Detection and Response. *Symmetry*, *17*(6). https://doi.org/10.3390/sym17060859

[42]. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine Learning for Cloud Security: A Systematic Review. *IEEE Access*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3054129

[43]. Chauhan, M., & Shiaeles, S. (2023, September 1). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*. Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/network3030018

[44]. Singh, I., & Singh, B. (2023). Access management of IoT devices using access control mechanism and decentralized authentication: A review. *Measurement: Sensors*, *25*. https://doi.org/10.1016/j.measen.2022.100591

[45]. Uddin, M., Islam, S., & Al-Nemrat, A. (2019). A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control. *IEEE Access*, *7*, 166676–166689. https://doi.org/10.1109/ACCESS.2019.2947377

[46]. Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022, October 25). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*. Emerald Publishing. https://doi.org/10.1108/IJWIS-04-2022-0077

[47]. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024, December 1). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s13677-024-00697-7

[48]. Collins, L. (2024). Access Controls. In *Computer and Information Security Handbook, Fourth Edition: Volumes 1-2* (Vol. 2, pp. 1267–1273). Elsevier. https://doi.org/10.1016/B978-0-443-13223-0.00079-5

[49]. Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, *8*(1). https://doi.org/10.1186/s42400-024-00320-x

[50]. Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025). A Systematic Review of Access Control Models: Background, Existing Research, and Challenges. *IEEE Access*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2025.3533145

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun2033

[51]. Penelova, M. (2021). Access Control Models. *Cybernetics and Information Technologies*, *21*(4), 77–104. https://doi.org/10.2478/cait-2021-0044

[52]. Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies. *ACM Transactions on Information and System Security*, *3*(2), 85–106. https://doi.org/10.1145/354876.354878

[53]. Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023, December 1). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*. KeAi Communications Co. https://doi.org/10.1016/j.csa.2023.100015

[54]. Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023, February 1). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors*. MDPI. https://doi.org/10.3390/s23041805

[55]. Kalaria, R., Kayes, A. S. M., Rahayu, W., Pardede, E., & Salehi Shahraki, A. (2024). Adaptive context-aware access control for IoT environments leveraging fog computing. *International Journal of Information Security*, *23*(4), 3089–3107. https://doi.org/10.1007/s10207-024-00866-4