Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Building Digital Trust in the AI Age: A Review of Privacy, Cybersecurity, and Emerging Threats

Keerthana.V
5th Sem BCA
Vijaya College Jayanagar

Jahnavi.K
5th Sem BCA
Vijaya College Jayanagar

Abstract - Artificial intelligence (AI), cloud computing, the Internet of Things (IoT), and other connected services have changed how people and organizations create, store, share, and use information. These technologies make many activities faster and easier, but they also create greater concerns about privacy, cybersecurity, and the safe handling of data. This paper reviews digital trust by focusing on the connection between privacy, cybersecurity, user awareness, and confidence in digital services that use AI and other emerging technologies. It discusses common threats such as phishing, malware, ransomware, unauthorized access, fraud, and data breaches, along with protection measures such as encryption, authentication, access control, firewalls, monitoring, and risk management. The paper also considers how AI, cloud computing, and IoT create new trust-related challenges. From the reviewed material, it is clear that digital trust is not based on one factor. Security, privacy, transparency, reliability, credibility, accountability, and user awareness all contribute to it. Therefore, protecting digital services requires a combination of technical controls, organizational practices, and responsible user behaviour.

Keywords: Artificial Intelligence (AI); Cloud Computing; Internet of Things (IoT); Cybersecurity; Data Privacy; Digital Trust; Literature Review; Protection Mechanisms; User Awareness.

1. INTRODUCTION

Digital trust means the confidence people have when they use digital technologies, online services, organizations, and systems that collect or process their information. For example, when a person uses online banking, a digital payment application, social media, an e-commerce website, an educational portal, or a cloud service, the person expects the service to protect both the information and the transaction. Concerns such as whether personal data is safe, whether it will be used properly, and whether an online transaction can be trusted are all part of digital trust.

Digital interactions are different from many face-to-face interactions because users usually cannot see what is happening inside the technology. They may not know which software, servers, people, or data-processing activities are involved. Because of this, users depend on signals such as login and authentication procedures, privacy information, service availability, security measures, the reputation of the organization, and their own previous experience. Trust generally increases when a service works as expected, explains its practices clearly, protects information, and takes responsibility when something goes wrong.

The importance of digital trust has grown along with AI applications, cloud platforms, IoT devices, mobile apps, social networks, and digital financial services. These technologies provide useful features and automation, but they also involve collecting and processing more information. AI systems can depend on large datasets, cloud services can move information between several platforms, and IoT devices can continuously collect data from homes, workplaces, or other physical environments. Each of these situations can create privacy or security concerns that may affect how much users trust a service.

For this reason, digital trust cannot be viewed as a single technical feature. It develops from several connected factors, including security, privacy, transparency, reliability, accountability, credibility, and user awareness. A system may have strong security controls but still make users uncomfortable if they do not understand how their information is being used. In

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

the same way, a service may provide clear information but lose user confidence if it repeatedly has security problems. The interaction among these factors is the main focus of this review.

Figure 1. Conceptual framework of digital trust

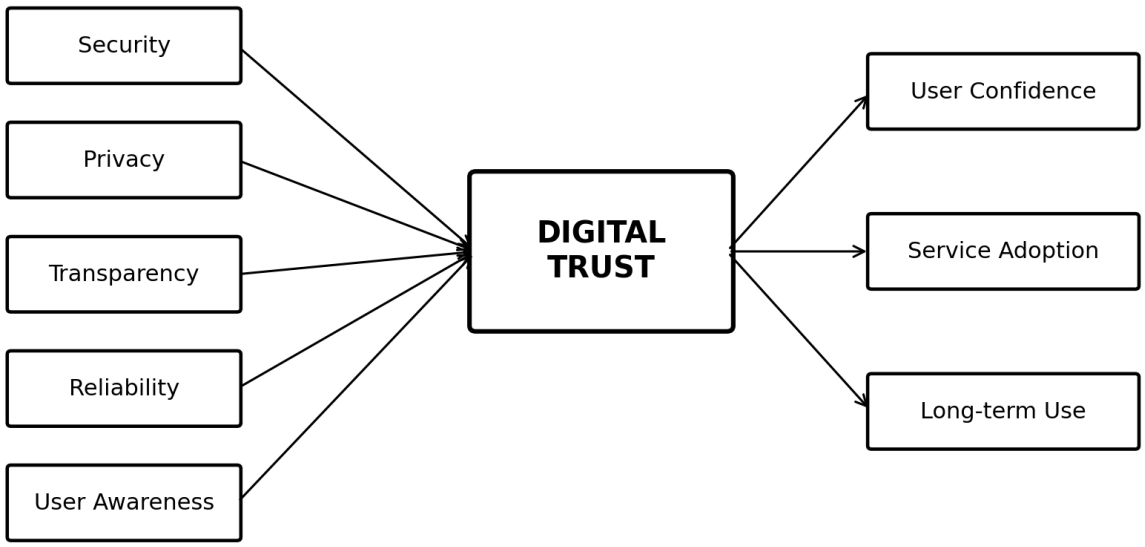


Figure 1. Conceptual framework of digital trust. Security, privacy, transparency, reliability, and user awareness interact to influence digital trust and, in turn, user confidence and continued adoption.

2. BACKGROUND OF DIGITAL TRUST

Digital services are now used for many routine activities, including banking, shopping, communication, education, healthcare, entertainment, and government services. Many of these services ask users to provide personal information, login details, contact information, location data, or payment details. People are more willing to provide such information when they believe that the service is secure and that the organization will handle their data responsibly.

Security is one of the main foundations of digital trust because users expect protection from unauthorized access, malware, data breaches, account attacks, and similar threats. Privacy is closely related, but it mainly deals with how personal information is collected, used, shared, stored, and protected. Transparency helps users understand what information is being collected and the reason for collecting it. Reliability is concerned with whether the service works consistently and gives accurate results. Accountability is also important because users need to know who is responsible when a problem occurs.

Trust is also affected by an organization's reputation and by the user's earlier experiences. People often form expectations from previous interactions, recommendations from others, and what they hear about a service or company. A good experience can increase confidence, while repeated failures, unclear data practices, or security incidents can have the opposite effect. Therefore, digital trust can change over time instead of remaining fixed once it has been established.

3. LITERATURE REVIEW

Pietrzak and Takala (2021) carried out a systematic literature review on digital trust and examined how the concept has developed in previous research. They found that there was no single definition of digital trust that was accepted by all researchers. Their review traced research on the topic back to 1996 and noted a strong increase in interest after 2016. The review identified reliability, credibility, security, data protection, and privacy as important ideas connected with digital trust.

Saveljeva and Volkova (2025) reviewed earlier research to examine the meaning and factors associated with digital trust. Their study considered 86 sources and found 42 different definitions of the concept. They described digital trust in relation to confidence in people, processes, and technology operating in a safe digital environment. Their work also pointed to transparency, ability, benevolence, and integrity as important parts of trust.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Recent cybersecurity guidance also supports the need for approaches that consider risk and trust together. The NIST Cybersecurity Framework 2.0 provides organizations with a general structure for managing cybersecurity risk, while the NIST AI Risk Management Framework addresses trustworthiness during the design, development, use, and evaluation of AI systems. These frameworks show that trust needs to be considered throughout the life of a digital system instead of being added only after a security problem appears.

Overall, the literature shows that digital trust has several dimensions. Security and privacy form an important base, while reliability, transparency, accountability, credibility, and user awareness affect how users judge a service. This review brings these factors together with common cyber threats and with newer technologies such as AI, cloud computing, and IoT to give a broader view of digital trust.

4. METHODOLOGY

This paper follows a narrative literature-review approach to study digital trust, privacy, cybersecurity, and the responsible use of digital technologies. The source material included research papers, journal articles, books, magazines, and online sources found through Google Search. The material was considered for its relevance to the topic, and information related to privacy, cybersecurity threats, protection methods, user awareness, and digital trust was selected for discussion.

The review brings together ideas from different researchers and guidance organizations to understand how digital trust is developed and how it can be affected by security and privacy problems. The discussion is arranged around four main questions: what digital trust means, what factors can increase or reduce it, which threats can damage it, and what technical, organizational, and human measures can help improve confidence in digital services.

This paper is not a statistical meta-analysis. The available source material does not provide a reproducible database-search procedure, detailed inclusion and exclusion rules, or a formal PRISMA screening process. Therefore, the work is described as a literature review rather than as a fully systematic review.

5. CYBERSECURITY THREAT LANDSCAPE AND DIGITAL TRUST

Cybersecurity incidents can affect digital trust directly because users may see an attack as evidence that a service has not protected their information properly. Phishing uses deceptive messages or websites to trick people into giving away passwords, credentials, or other sensitive information. Malware can affect a device and allow unauthorized activities. Ransomware can prevent access to files or systems. Unauthorized access and data breaches can expose accounts or confidential information, while fraud can result in financial loss and misuse of personal details.

The damage caused by these threats is not limited to the technical problem itself. An attack may lead to financial loss, service interruptions, exposure of personal information, damage to an organization's reputation, and reduced user confidence. Even after the technical issue has been fixed, users may continue to wonder whether their information is safe. In this way, the loss of trust can remain long after the original cybersecurity incident.

User awareness is especially important when attacks depend on social engineering. Security software may protect many parts of a system, but a user can still be persuaded to open a harmful link, reveal a password or OTP, install unsafe software, or send payment information to a fraudster. Security awareness should therefore be treated as one part of building digital trust. Users need practical guidance that helps them recognize suspicious situations and make safer decisions.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Figure 2. Common cyber threats and their effect on digital trust

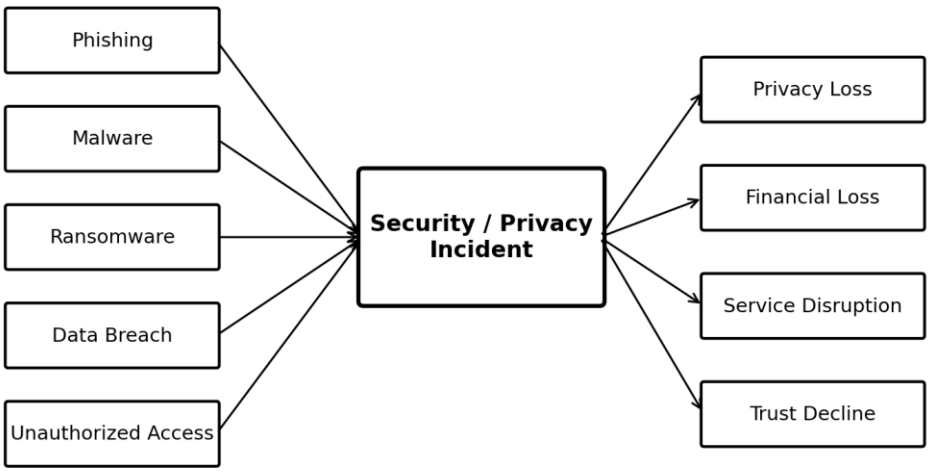


Figure 2. Common cyber threats and their potential effects on privacy, finances, service continuity, and digital trust.

6. PROTECTION MECHANISMS FOR STRENGTHENING DIGITAL TRUST

Encryption changes readable information into a protected form so that unauthorized people cannot easily understand it. It can be used when information is being transmitted and, depending on the implementation, when it is stored. Authentication checks whether a user or device is really the one claiming access. Strong authentication is useful because a stolen password alone should not automatically give an attacker access to protected information.

Access control decides which users, devices, applications, or services are allowed to use particular resources. Firewalls help control network traffic according to security rules. Logging and monitoring make it possible to observe activity and investigate unusual events. Backups and recovery procedures are also important because they help an organization restore services after an incident and reduce the effect of a disruption.

These security measures are more effective when they are used together rather than separately. NIST's Zero Trust Architecture emphasizes that a user or device should not automatically be trusted just because it is inside a particular network. Identity and authorization should be checked before access to resources is provided. This approach is useful in cloud and distributed environments where the old idea of a clear internal network boundary is less practical.

Technical controls also need support from organizational policies and clear responsibilities. Organizations should have incident-response procedures, privacy practices, defined roles, and user-awareness programmes. Users are more likely to trust a service when they can see both technical protection and evidence that the organization has clear procedures for handling information and responding to problems.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Figure 3. Layered protection approach for building digital trust

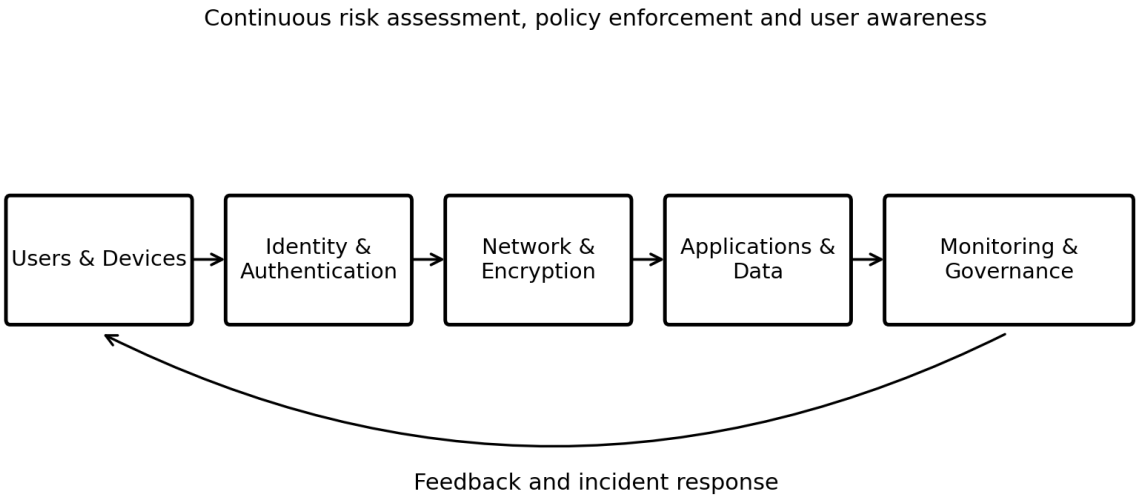


Figure 3. Layered protection approach for building digital trust across users, identity, networks, applications, data, monitoring, and governance.

7. EMERGING TECHNOLOGIES AND NEW TRUST CHALLENGES

7.1. Artificial Intelligence and Digital Trust

AI is changing the way people interact with digital systems because users increasingly depend on applications that recommend content, generate text or images, classify information, or support decisions. Trust in an AI system is therefore not only a cybersecurity issue. Users may also want the system to behave consistently, provide understandable information, protect the data used by the system, and operate under suitable organizational controls. The NIST AI Risk Management Framework provides guidance for considering these trustworthiness issues during the AI lifecycle.

AI can also introduce additional privacy and security concerns. The data used to train or operate an AI system may contain sensitive information, and AI-enabled applications can themselves be attacked, manipulated, or misused. This means that trust needs to be considered from data collection and model development through deployment, monitoring, and eventual retirement. Organizations also need processes for reviewing risks when an AI system, its data, or its intended use changes.

7.2. Cloud Computing

Cloud computing changes the location of data and applications and also changes how users reach them. An organization may depend on several cloud services, APIs, storage systems, and identity providers at the same time. This can make security responsibilities harder to understand. Users may not know where their information is processed or which provider is responsible for a particular security function.

In cloud environments, digital trust depends on identity management, access control, encryption, monitoring, service reliability, privacy practices, and clear responsibilities between customers and providers. Least-privilege access and zero-trust principles are useful because access should be based on verified identity and actual need rather than on an assumption that a user or device is trustworthy.

7.3. Internet of Things

IoT devices connect physical objects to networks and often collect information continuously. Examples include smart-home products, sensors, wearable devices, and connected equipment. These devices may be spread across many locations and can have limited processing or security capabilities, which makes long-term protection difficult. Weak passwords, old software, poor configurations, and missing updates can create vulnerabilities that affect both the device and the information it collects.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

NIST's IoT cybersecurity guidance describes device capabilities and supporting activities that can help organizations address security needs in IoT products. The guidance shows why security should be considered from the time a device is designed or purchased through deployment, maintenance, and retirement. For users, regular security updates and clear information about product support can make connected devices easier to trust.

8. DISCUSSION AND ANALYSIS

The reviewed material indicates that digital trust develops through a combination of technology, organizational behaviour, and user experience. Security controls are necessary because users need protection from attacks, but technical security alone does not create trust. Users also need understandable information about data handling, dependable service, accessible support, and confidence that the organization will act responsibly when a problem occurs.

Digital trust can be understood as an ongoing cycle. A user begins with certain expectations about a service. The service then provides signals through its security, privacy practices, transparency, and reliability. The user compares those expectations with the actual experience. Good experiences can strengthen confidence and encourage continued use, while security incidents or unclear practices can reduce it. Organizations can influence this cycle by investing in security, communicating clearly, and responding properly to user concerns.

The review also suggests that trust should be considered throughout the life of a digital service. Problems can arise during design, deployment, normal operation, maintenance, or later changes. For example, a service may initially have clear privacy practices but introduce a new feature that collects additional information. Similarly, an AI system may work well when first launched but require regular monitoring as its data, users, and operating environment change. Continuous governance is therefore important.

Table 1. Relationship between trust dimensions, risks, and strengthening measures

Trust dimension	Typical risk	Strengthening measure
Security	Unauthorized access, malware, data breaches	Authentication, encryption, monitoring
Privacy	Too much or unclear use of data	Collect less data, privacy controls, clear information
Reliability	Repeated failures or service outages	Testing, resilience, backups and recovery
Transparency	Unclear data collection or processing	Clear notices, explanations and communication
Accountability	Weak response when incidents occur	Clear responsibility, governance and incident response
User awareness	Phishing and social-engineering attacks	User education, warnings and practical guidance

9. CHALLENGES AND ISSUES

Several issues still make digital trust difficult to maintain. First, cybersecurity awareness is not the same for all users. Someone who is unfamiliar with phishing, fake websites, fraudulent calls, or suspicious attachments may be more easily targeted by social engineering. Second, digital services can be complicated, and users may not clearly understand what information is collected, where it is stored, or how it may be shared.

Third, technology can change faster than users can understand its risks. AI applications, cloud services, and IoT products can introduce new dependencies and new points of attack. Organizations therefore need to update their security controls, policies, and user guidance as technology and threats change.

Fourth, measuring trust is not simple. One user may trust a service because it is convenient while still being worried about privacy. Another user may place greater importance on security than convenience. Because trust depends on several factors and can differ between users and situations, a single numerical value may not describe it accurately without considering the context.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

Finally, rebuilding trust after an incident can be more difficult than preventing the incident in the first place. Organizations need to explain what happened, communicate honestly, support affected users, fix the weaknesses, and show that corrective steps have actually been taken. A clear response can help restore confidence, although the result will depend on the seriousness of the incident and the user's previous experience with the service.

10. FUTURE SCOPE

There are several useful directions for future research on digital trust. One possibility is to develop practical models that measure security, privacy, transparency, reliability, accountability, and user awareness together. Such models could be adapted for different sectors because the expectations of users are not the same in banking, education, healthcare, e-commerce, and social media.

Future studies could also look at how trust develops when a person first starts using a digital service and how earlier experiences influence later decisions. Long-term studies may help researchers understand whether trust changes after a security incident, a major feature update, a change in privacy policy, or a noticeable change in service quality.

Another important area is the connection between digital trust and AI. Researchers can study how explanations, transparency, data practices, human oversight, and system reliability affect people's willingness to depend on AI-based services. Similar work can be carried out for IoT environments, where trust may depend on device security, software updates, manufacturer support, and the way collected data is handled.

Research can also focus on practical methods for restoring trust after a cybersecurity incident. Comparing communication methods, user-support arrangements, remediation activities, and user responses could help organizations identify which actions are most useful when trying to rebuild confidence.

11. CONCLUSION

Digital trust has become an important part of modern digital technologies and services. The literature reviewed in this paper shows that users' confidence is connected with security, privacy, reliability, transparency, credibility, accountability, and responsible handling of personal information. The fact that researchers use different definitions of digital trust also shows that it is a multidimensional concept.

Privacy and cybersecurity provide an important foundation, but technical protection by itself is not enough. Users also need clear communication, reliable services, responsible data practices, useful customer support, and suitable security policies. Organizations therefore need to combine preventive security measures with continuous monitoring and an effective response when incidents occur.

The increasing use of AI, cloud computing, and IoT makes this combined approach more important. These technologies offer clear benefits, but they also create new dependencies, data flows, and security risks. Building digital trust therefore requires attention not only to technology but also to the organizations, processes, and people involved in using it.

Overall, digital trust should be treated as something that needs to be maintained over time rather than achieved once and then forgotten. Security incidents, new features, changes in technology, and changing user expectations can all affect confidence. Continued research and practical risk-management measures are needed to measure, strengthen, and restore trust in different digital environments.

REFERENCES

[1] Pietrzak, P., & Takala, J. (2021). Digital trust – a systematic literature review. Forum Scientiae Oeconomia, 9(3), 59–71. https://doi.org/10.23762/FSO_VOL9_NO3_4

[2] Saveljeva, J., & Volkova, T. (2025). A survey on digital trust: Towards a validated definition. Digital, 5(2), 14. https://doi.org/10.3390/digital5020014

[3] Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[4] Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1

[5] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology, NIST SP 800-207. https://doi.org/10.6028/NIST.SP.800-207

[6] Fagan, M., Megas, K. N., Scarfone, K., & Smith, M. (2020). IoT Device Cybersecurity Capability Core Baseline. National Institute of Standards and Technology, NISTIR 8259A. https://doi.org/10.6028/NIST.IR.8259A

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 11, CONFLUENCE - 2026

[7] Fagan, M., Megas, K. N., Marron, J., Brady, K. G., Cuthill, B. B., & Herold, R. (2021). IoT Non-Technical Supporting Capability Core Baseline. National Institute of Standards and Technology, NISTIR 8259B. https://doi.org/10.6028/NIST.IR.8259B

[8] Megas, K. N., Fagan, M., Marron, J., Watrobski, P., & Cuthill, B. B. (2022). Profile of the IoT Core Baseline for Consumer IoT Products. National Institute of Standards and Technology, NISTIR 8425. https://doi.org/10.6028/NIST.IR.8425

(This work is licensed under a Creative Commons Attribution 4.0 International License.)