Application of Trustworthy IoT Technology in Fast Communities:
Smart Access Control

Fauzia Yasmin
School of Computer and Artificial Intelligence, Wuhan University of Technology, China

Md Sobuj Ali
School of Computer and Artificial Intelligence, Wuhan University of Technology, China

Saida Sultana
School of Business, National University, Bangladesh

Abstract:
As a response to the current development status and existing problems in the ubiquitous and trustworthy aspect of the Internet of Things (IoT) in the construction of smart community systems in Bangladesh, this paper presents the trustworthy technology strategy of the ubiquitous and trustworthy IoT intelligent system. Additionally, it provides a list of the demonstration application practice of trustworthy IoT technology at the level of smart communities through three different application scenario project construction cases. These cases include smart access control, smart buildings' construction, and smart parks' construction.

Keywords: Internet of Things, Universal trustworthiness, Cloud computing, AI Plus.

Introduction
The integration and innovation of the IoT and other new generation information technologies, such as data science, digital twin, robotics, represented by 5G requires the IoT to be more secure, open, intelligent and efficient (Shoukat, et al., 2021; 2022a; 2022b; 2023a; 2023b; Jabeen, et al., 2022). From the perspective of key technologies, compared with traditional communities, the technical elements of smart communities are more complex. They must also cover modern surveying, mapping, geographical information, video information, precise positioning, semantic modeling, simulation, intelligent control, AI, Edge computing has new needs, making multi-technology innovation integration increasingly critical (Nawaz, et al., 2022). Smart infrastructure, edge sensing. The most basic smart community support platform, management service platform, connects edge terminal devices and smart apps (Niaz, et al., 2022). It focuses on construction, operation, and maintenance using pervasive IoT sensing and edge intelligent facility access. It supplies equipment, application, property, community, government, and business staff. Providing services to associated users empowers openness, sharing, and business distribution. It provides access device services, supports a wide range of interface protocols, aggregates and accesses ubiquitous perception data, and supports multi-level and flattening.

Distributed edge deployment facilitates the centralized planning, construction, and
maintenance of a reliable information infrastructure that is accessible everywhere. It enables comprehensive management and collaborative interaction of equipment. It focuses on the application layer, allowing open and shared data to empower various types of IoT applications and foster the development of innovative IoT data applications (Zeng, Pang, & Tang, 2024). The IoT sensing platform serves as the interface connecting the smart community (Monios, et al., 2024) to the physical world. The level of sensing granularity present across a community has a direct impact on the overall quality of the community's smart infrastructure.

The Trusted IoT (Shao, et al., 2023) intelligent system is a widely used and reliable application platform system for the IoT, developed by A. K. Khan Telecom company. The core function of this technology is to facilitate the gathering, transmission, and analysis of real-time data in the IoT. The objective of the Internet data service center is to achieve widespread presence, reliability, and advanced cognitive capabilities. This article presents a range of solutions, derived from smart buildings to smart community development, that are built around the "A. K. Khan Telecom Trusted IoT Intelligent System".

**Background**

**System Structure**

The IoT incorporates a perception layer, which distinguishes it from regular information networks (Moustafa, et al., 2023). The IoT operates independently of fixed infrastructure, power supply, resources, geographical location limits, and other limiting factors. It can be utilized at any time and in any location, with convenience and effectiveness. Nevertheless, the IoT is very vulnerable to a range of security attacks, such as eavesdropping, identity forgery, signal interference, data tampering, retransmission, and denial of service. Based on the traditional hierarchical framework of the IoT, it encounters various levels of security vulnerabilities and dangers (Zhang, & Allebach, 2008), as seen in Figure 1.

The perception layer (Khattak, et al., 2019) is a crucial element of the IoT. In contrast to previous information networks, the necessity of the perception layer amplifies the security vulnerabilities of the IoT. The security system for the IoT must address and handle all security concerns, including the potential invasion and attack of IoT sensing nodes, the possibility of high-level encryption and decryption methods being compromised, and the risk of hackers counterfeiting user identities. Security concerns at the transport layer primarily encompass interception of communication channels, exploitation of routing protocol flaws, network

![Figure 1. Security threats at various layers of the IoT](image)

The perception layer (Khattak, et al., 2019) is a crucial element of the IoT. In contrast to previous information networks, the necessity of the perception layer amplifies the security vulnerabilities of the IoT. The security system for the IoT must address and handle all security concerns, including the potential invasion and attack of IoT sensing nodes, the possibility of high-level encryption and decryption methods being compromised, and the risk of hackers counterfeiting user identities. Security concerns at the transport layer primarily encompass interception of communication channels, exploitation of routing protocol flaws, network
congestion resulting from extensive simultaneous access, and manipulation of original material. The primary security vulnerabilities at the application layer include inadequate encryption leading to information leakage, insufficient protection of user privacy, unauthorized tampering of application business data by hackers, unreasonable role permissions resulting in unauthorized access, and the potential for information alteration and loss. The term "stability" is mentioned in reference. The data security trust protection of the IoT encompasses the utilization of information homogeneity technology, information concealment technology, and multi-dimensional security computing to address the issue of location confidentiality in wireless networks (Dai, et al., 2014), as seen in Figure 2.

Prior to conducting any evaluations, it is imperative to verify the security and integrity of the fundamental software and hardware components in the trust control layer (Pasquier, Singh, & Bacon, 2015). Access to the network is restricted to information equipment that complies with security standards. Furthermore, the trust chain transmission mechanism is employed to regulate the behavior of sensors, smart terminals, and other edge computing devices, ensuring their compliance. The trust data layer consists of two sorts of data: trust ubiquitous sensing data and trust processing data.

Trust-sensing data means that edge sensing devices in the IoT perception layer can obtain real data according to the system's intentions; trust-processing data means that trust-sensing data can be trusted to reach the trust processing layer through trust transmission, and then sent to the application layer after preprocessing and processing. The data obtained by the application layer reflects the real situation of the sensing layer.

**Trust Terminal**

Trusted terminals include trusted software systems, trusted hardware devices and trusted effective access. Trusted software and trusted hardware are trust components carried by hardware to perform platform security and integrity testing. Key authentication and negotiation steps are very critical when performing trusted access.
Trust Transfer

The network layer of the IoT is a data transmission channel that transmits data obtained by the perception layer to the data processing center or client application APP of the application layer service platform through various network infrastructure and communication protocols. It is not a new network transmission facility. It is mainly supported by existing networks such as telecommunications operator networks, the Internet, cable TV networks and satellite communication networks. With the further advancement and implementation of the intensive integration of radio and television networks, telecommunications networks and the Internet, and the widespread application demonstration and rapid popularization of IPv6 and 5G application scenarios, the network layer is gradually developing towards full-area IP speech. The security threats of the IoT at the network layer are greater than the various security risks and attacks faced by IP before, including data packet loss during transmission, data counterfeiting, data interception, data storms, etc. The location, concurrency, acquisition address, delivery time and communication protocol of data in the IoT are relatively fixed, so the security risks it faces (Al-Masri, et al., 2020) are more complex than ordinary networks.

Trusted Users

The trust measurement of the IoT application layer mainly includes trust in the authenticity of user identity and trust in operational compliance. True trust in user identity is that the user's identity can ensure that access control is authorized, the access process is recorded, identity verification and other means are tracked, and malicious behavior can be verified through authentication and other identity confirmations. The trust of user operation compliance is mainly measured through node trust, which is an organic combination of operational information and physical information. The IoT environment has the characteristics of multiple sources of equipment, different structures, high-dimensional complexity, and dynamic changes. Establishing an IoT security trust architecture that meets the requirements of different structures, reliable performance, data security and stable services (Islam, & Sandip, 2020) is a goal that domestic and foreign scholars have been pursuing.

In order to achieve this goal, designing a secure and trusted architecture for the IoT with clear layers and rigorous structure is the prerequisite for the dynamic and trusted operation of the IoT. It is necessary to model different structural nodes in the IoT from multiple dimensions to provide a dynamic trust group. Network and trusted feedback control provide basic support. The A. K. Khan Telecom Trusted IoT Intelligent system is designed based on such an architecture.

System Features

The technical route of A. K. Khan Telecom Trusted IoT Intelligent system can be summarized as follows: dynamic trust networking is the core of trust operation, dynamic trust feedback control is the key to dynamic trust operation of the IoT, facing different nodes of the IoT The research and application demonstration of dynamic trusted operation mechanism promote the independent innovation ability of trust information technology (Huang, et al., 2020).

Dynamic

According to actual application scenarios, the IoT can be simply divided into general IoT networks and dedicated IoT networks. The security trust architecture of these two IoTs is different. The field of exclusive IoT mainly focuses on the interaction of trust between things in a closed environment, trustful information perception and trustful computing processing.

The types of security attacks faced by this type of IoT are relatively simple, and most of them are control system-oriented interventions, mainly including intervention changes in sensing data (Chander, et al., 2022), intervention changes in control commands, etc.
Therefore, its structure has poor adaptability to ordinary scenarios, and its attack behavior is relatively simple. The exclusive IoT security system architecture combines the middleware layer and the application layer into the control layer, which reduces the complexity of the overall security architecture of the IoT and places control security in the most important position. However, the characteristics of this architecture are customized based on the involution of the IoT system. It only focuses on the exposed security risks of the application layer and middleware layer, without considering the exclusive services brought by these exposed edge-aware networks. security risks response methods. At the same time, this architecture cannot solve the problems of terminal privacy protection and node collaboration.

The architecture of the conventional IoT is similar to that of the Internet. The entire architecture is a non-closed system and is open. This design leads to unclear security boundaries of the IoT and a more complex perception environment, resulting in the inability to clarify its security boundaries.

Existing considerations for the security trust architecture of the IoT are limited and research is lacking. Functionally speaking, the existing security architecture is imperfect. The security architecture of the exclusive IoT focuses on ensuring the security of business processes from attacks and security control; the security architecture of the open IoT focuses on protecting the information, user identities and user behaviors of organizations, users and terminal devices from attacks, and ensure data security.

From a structural perspective, the complete form of the security system architecture has not yet been formed. The entire security trust architecture is based on the traditional hierarchical architecture of the IoT, which blocks the security policies between layers and the security trust system within the layers. Security trust information flow cannot be reused, and the security of the system cannot be guaranteed with high quality.

During the implementation process, although many solutions have proposed different ubiquitous trustworthy technical means such as identity authentication, privacy protection, data encryption and access control, even if these technical means achieve their respective so-called security goals, they still have The complete safety of the system during operation cannot be completely guaranteed. First, security assurance requires huge computing resource overhead, and limited edge terminals cannot achieve the required intensity within a complete interaction cycle. Second, the security mechanism cannot effectively resist common network attacks in sensing networks.

The IoT can be divided into perception layer, network layer and application layer based on functions. However, in actual application scenarios, IoT nodes are difficult to classify according to logical layers. For example, some nodes not only collect data, but also serve as network relay nodes to forward data, and at the same time provide services for other nodes. This makes it difficult for nodes in the IoT to be networked according to logical layer divisions. Based on the abstract description of structural nodes, studying node dynamic trust networking to make it the basis for secure trust operation of the IoT requires the use of various theories such as social community construction and spatio-temporal dynamic balance. The establishment of the real-time trusted network model of the IoT is undoubtedly the core of the real-time trust operation of the IoT.

**Feedback Control**

Research on the trust measurement of nodes in the perception layer of the IoT can not only improve the security of the IoT, but also simplify monitoring, control and prevention of other expenses. However, the current trust measurement research on perception layer nodes is not satisfactory. First of all, the current trust measurement research focuses on a certain application field and is not universal; at the same time, there is a lack of trust measurement model for perception layer nodes. The trust measurement mechanism plays a very important role in the security of the IoT. Therefore,
staying the trust measurement model is very critical and time is urgent. At the perception layer, there are many difficulties in implementing trust measurement: 1) Lack of facility support; 2) Limited node resources; 3) Fragile wireless channels; 4) multi-source heterogeneous nodes.

IoT nodes face many difficulties in establishing a trust mechanism through trust measurement. The main reason is that a wide range of use scenarios lead to unpredictable patterns in node association; decentralized scenarios make the original unified and intensive security trust strategy for objects and terminals failure; different structural scenarios make it impossible to use an integrated trust measurement method.

First, the existing trust measurement methods for perception layer nodes are all proposed based on the node's historical behavior data and different practical application scenarios. They do not consider the trust evaluation strategy that combines objective evaluation and subjective judgment, nor do they consider dynamic measurement. Combined with static metrics.

Second, the trust measurement method cannot adapt to the complex and heterogeneous networks with different structures in the IoT in real time, and faces the overall research and design deficiencies of different structures, situations, ubiquity, and mobility of the underlying environment of the IoT.

Third, existing trust measurement methods consume very high energy and are actually not suitable for sensing layer nodes with relatively limited edge computing resources.

At present, there are not many studies and analyzes in the industry on the unique characteristics of nodes in the IoT perception layer at the smart community level, and the existing security strategies are not enough to ensure safe and trustworthy computing of perception layer nodes.

Therefore, in order to ensure the trustworthy operation of the sensing layer nodes of the IoT, it is first necessary to study the separable load mechanism of the sensing layer nodes. Secondly, in order to ensure the trusted computing of perception layer nodes, it is necessary to study the trust access strategy of perception layer nodes. Finally, in order to protect the real-time status of sensing nodes and improve the reliability of sensing nodes, it is necessary to study trust measurement methods for IoT sensing layer nodes suitable for smart community scenarios.

The distribution of nodes in the IoT is fragmented in time and space. Different node groups in the same area belong to different institutions, and different institutions are even in competitive and hostile relationships. Therefore, how to ensure the dynamic credibility balance of the IoT requires research on the integration of nodes. Trusted feedback control mechanism for point groups and nodes within the group. The Spurui Trusted IoT intelligent system is built on a trusted group, introduces the idea of group collaboration, realizes feedback control of groups and individuals, ensures the dynamic trustworthy balance of the IoT, and proposes a new research idea for IoT security research.

Independent Innovation Capabilities

The security protection mechanism of the IoT is highly consistent with the application scenarios. Although it can deal with security threats related to the application scenarios, it lacks a systematic, universal and global security solution for the IoT. The security mechanism Research needs to make breakthroughs in order to build a trusted IoT. With the advancement of economy, society and science and technology, the IoT has penetrated into every corner of human society. The normal operation of important information systems related to the national economy and people's livelihood cannot be separated from the security and trustworthiness of the IoT. The A. K. Khan Telecom Trusted IoT Intelligent System Relevant research breakthroughs lay a key technical foundation for the dynamic and trustworthy operation of the IoT, and have important theoretical and practical significance for improving information technology innovation capabilities.
Key Technologies

The smart community system mainly includes research on the IoT load splitting (Shoukat, et al., 2024) algorithm, the trusted network connection mechanism of the IoT perception layer, the trust measurement mechanism of the IoT perception layer, and standardized trusted services. Figure 3 shows the key technical research tasks.

Data Encryption Algorithm

In order to ensure the confidentiality of data during the communication process, communication encryption mechanisms, encryption algorithms, and key exchange technologies are involved in IoT communications.

1) Communication encryption mechanism.

End-to-end encryption (also known as off-line encryption or packet encryption) is used in the data communication process. End-to-end encryption allows data to always exist in ciphertext during the transmission process from the source point to the end point. When end-to-end encryption is used, Messages are transmitted without being decrypted until they reach the end point, and because the message is protected throughout the transmission, even if a node is compromised, the message will not be leaked.

End-to-end data encryption technology is used in the communication encryption mechanism of the IoT, which is mainly suitable for data encryption in communication networks. The algorithm of this encryption technology is relatively simple and its application cost is low, so it has wide applicability. For end-to-end data encryption algorithms that encrypt messages independently, the advantage is that this method has good application effects and is easy to maintain and operate in the future.

2) Data encryption algorithm.

The encryption algorithm uses the advanced encryption standard AES. AES uses a symmetric block cipher system. The minimum supported key lengths are 128, 192, and 256, and the block length is 128 bits. The algorithm should be easy to implement on various hardware and software. In IoT communication, the key length is 128 bits.
3) Key exchange algorithm.

Since the AES algorithm selected is a symmetric block encryption algorithm, that is, the sender and receiver use the same key for encryption and decryption, a secure dedicated channel must be used to transmit the key. However, dedicated channels are expensive and difficult to implement, so the key exchange algorithm is used in IoT communications to realize key exchange between the sender and the receiver.

Among them, Diffie-Hellman is an asymmetric key encryption method that ensures the security of shared keys through insecure networks. It is an algorithm specially used for key exchange and is suitable for communicating parties to securely negotiate the session key for a communication. This algorithm is based on the difficulty of discrete logarithm calculation and has high security.

After the communicating parties determine the AES key to be used, the Diffie-Hellman algorithm is used for key exchange, and then the entire communication process is encrypted through the end-to-end encryption mechanism.

Ubiquitous Trust Networks

Based on the trust network connection architecture and the security access requirements of the perception layer nodes of the IoT, research the ubiquitous universal trust network connectivity architecture suitable for perception networks with different structures, refine the security architecture, and study the perception network. The two-way trusted authentication technique of layer nodes is used to study the trust networking strategy of IoT perception layer edge nodes. Identity authentication of IoT sensing layer nodes that prioritizes efficiency and security, mutual trust authentication for entry and exit, and trust-building network strategies for nodes are covered.

Ubiquitous Trust Measurement

In view of the limitations that the existing trust measurement mechanism cannot adapt to the different structural sensing environments of the IoT, the trust measurement of the perception layer nodes is studied using the trust-trust network connection model and state and behavioral trust measurements. Strategy; Study edge sensing node trust measurement-based feedback control.

When the wireless sensor network is turned on, measure the trust status of each sensor node and check whether the edge wireless sensing network's software and hardware comply with the security policy to ensure that sensor nodes' software and hardware have not been tampered with. The group aggregation node starts and finishes the measuring procedure since it has more energy than ordinary nodes. The information and upper nodes measure the group and information aggregation nodes, respectively. The entire IoT Measurements at every stage ensure operational safety.

Wireless sensor network snapshots help measure real-time node status. The wireless sensor network is made up of groups, so members can be untrustworthy, crucial trustworthy, or trustworthy. Each credible evaluation vector maps to its evaluation level.

Any group record includes trusted, borderline trusting, and untrusted members. Sociologically, the environment matters more, and a member Trust level will range greatly between those with trusting peers and those with untrusting peers. To determine a node's immediate trustworthiness, one must also consider its linked nodes' trust ratings.

A second is standardized trust services. In a trust-based IoT ecosystem, ubiquitous security services can be offered singly or in groups using multiple trust service techniques. To supply trust services in various situations. In any event, 5G IoT security is moving towards standardized trust services. The ISO7498-2 standard is suited for implementing trust service actions in a wide range of pan-IoT application scenarios under information security rules. This standard specifies the relationship between trust services and trust policies and their OSI reference model location. Table 1 compares trust service properties, and method.
Table 1. Relationship Between Trust Service Properties and Trust Service Mechanisms

<table>
<thead>
<tr>
<th>Trust service mechanism/properties</th>
<th>Encryption</th>
<th>Digital signature</th>
<th>Access control</th>
<th>Complete data</th>
<th>Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer entity authentication</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Data source identification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Access Control Services</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Connection confidentiality</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>No connection confidentiality</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Business flow confidentiality</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Connection integrity</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

From Smart Buildings to Smart Communities

The application of A. K. Khan Telecom Trusted IoT Intelligent system starts from buildings (Komninos, 2011), extends to building groups, and even parks (communities) and communities outside the buildings to monitor and manage all man-made and natural environments, thus forming a ubiquitous trusted digital space for life and production. The core concept is to use the layered idea of the IoT and rely on ubiquitous trusted IoT intelligent technology to collect all front-end edge facility information of various professional subsystems in the community intelligent system in a trustworthy and perceptual manner. The layer data adapter trustless transmits the sensed data to the trusted application layer through the trusted transport layer self-organizing network or communication network, and the relevant subsystems in the A. K. Khan Telecom Trusted IoT Intelligent system perform unified analysis and processing of the data to achieve sub-trustworthy intelligent linkage of the system realizes a trustworthy smart park (community) with trustworthy smart buildings as units. The trustworthy smart community group constitutes a trustworthy smart community, as shown in Figure 4, including the relationship between smart buildings and smart parks.

Figure 4. Inclusive Relationship Between Smart Buildings and Smart Parks
Application Examples

Smart Building

Due to the needs of pneumonia prevention and control work, the office building to strengthen the management and control of people entering and exiting, play a role in preventing the epidemic of pneumonia, and ensure the safety of office personnel in the building (Ma, et al., 2020). The entire building is equipped with a trusted networked online access control and visitor system. In order to ensure the quality of signal access, the access control controller preferentially uses wired access to the office intranet of the BD Smart Zoon. The card reader is selected to support card swiping, NFC, and With the QR code authentication method, users can activate multiple authentication methods at the same time or choose any one according to their own preferences, and two-way authentication is used for entry and exit. The computer room is equipped with an access control system server, and all front-end access control controllers are uniformly managed by the access control system server. Set up a card management computer in the management department, and also equip it with a card issuer and a card printer, so that managers can set access permissions for corresponding personnel according to users and departments, thereby achieving personnel access control. The access control controller is linked with the fire protection zone of the building. When a fire alarm signal is received, the trusted access control system of the corresponding zone automatically fails.

Intelligent Park

Incorporate the six components of "people, vehicles, objects, rooms, networks, and places" into the BD Smart Zoon in order to implement a comprehensive perimeter alarm system, personnel access control system, parking management system, fire sensing system, non-motor vehicle management system, video surveillance system, park smart security network monitoring platform, and more by maximizing the use of ubiquitous trusted IoT technology.

Smart Community

BD Smart Zoon Smart Community adopts the same implementation architecture as the Smart Park, based on ubiquitous trusted IoT technology, ensuring the safe and effective operation of various smart application services in the community.

Conclusion

A smart community is a community that incorporates several elements such as community infrastructure, specialist industries, neighborhood social interaction, life services, smart housing, property services, security, ecological environment, and operation management. Currently, the primary goal of IoT intelligent systems is to develop pervasive and reliable IoT technology in order to establish smart communities. In the future, it will be focused on a diverse array of cutting-edge information technologies, including cloud computing, big data, artificial intelligence, and 5G. Create a comprehensive and reliable digital replica park that will facilitate enhanced innovation and optimization of intelligent park structures, infrastructure, and management services.

Acknowledgement

The authors appreciate the reviewers for their helpful comments and suggestions in this study.

References


things systems, 3-45. https://doi.org/10.1007/978-3-030-87059-1_1


Shoukat, K., Jian, M., Umar, M., Kalsoom, H., Sijjad, W., Atta, S. H., & Ullah, A. (2023a). Use of digital transformation and artificial intelligence strategies for pharmaceutical industry in Pakistan: Applications and


