IOT DEVICES AND CONTROL SYSTEMS WORKING TOGETHER TO IMPROVE SECURITY

Rupinder Singh
Chitkara University Institute of Engineering and Technology
Chitkara University,
Punjab, India
rupinder.1153@chitkara.edu.in

Jaspreet Singh Bajaj
Chitkara University Institute of Engineering and Technology
Chitkara University,
Punjab, India
Jaspreet.bajaj@chitkara.edu.in

Simerjeet Singh Bawa
Chitkara Business School, Chitkara University, Punjab, India
Simerjeetsingh.bawa@chitkara.edu.in

***Abstract*— The Internet of Things (IoT) facilitates seamless integration and interoperability among various networks, devices, technologies, and products by placing emphasis on control schemas. End-users require uninterrupted and precise connectivity, irrespective of the integration node (e.g., tablet, laptop, television, smartphone, or other internet-connected device). Intelligent IoT devices have the capability to function as flexible connections with ever-changing configurations, enabling timely reactions and potentially worldwide reach.**

In response to the urgent requirement for secure real-time control operations, this research paper introduces a methodology that integrates intelligent Internet of Things (IoT) system functionalities with power system interfaces. The proposed methodology integrates computing, cryptography, signal/image processing, and communication networks to facilitate authentication and authorization operations via gateways and terminals. This results in a real-time performance environment that is not only more secure but also more adaptable and robust in comparison to conventional approaches. Moreover, the researchers delineate a framework for the Internet of Things that is applicable to power system inputs in administrative, industrial, transportation, and comprehensive monitoring environments.

Keywords—IOT, System Interfaces, Image Processing, authentication, Control System

I. INTRODUCTION

It should be feasible to streamline administration by organising it based on information structure. This can be achieved by utilising features like automatic measurement studying, available device testing, and efficient management approaches, such as those employed in the Internet of Things. [1,2]. Additionally, it raises the dangers related to data security. Numerous interrelated presumptions, listed below, support these results.

Coordinated readiness may help to avert or lessen the consequences of high-risk events. Plans for emergency services should be created and then put into action [7]. It is necessary to disseminate information regarding evaluation strategies and alert systems, specifically in the case of an explosive chemical discharge from a manufacturing site, to a broader segment of the general public. [8]. Possible measures include public responses such as evacuations, as well as the private option of staying indoors until the discharged material has been eliminated. Due to their ability to handle potential dangers, they are actively seeking information on disaster preparedness.

When a company operates well and creates effective emergency service organisations, people should become more interested in it and its commitment to upholding corporate responsibility to endanger the community's health and safety [9]. Once the community is informed of this obligation, they should assist businesses as they have the ability to oversee the decisions and activities related to potential risks and the consequences of behaviour. The integration of risk communication into political engagement was made possible in large part by these kinds of discoveries [10]. It would be advisable for public information specialists to expand on past discoveries that could facilitate efficient communication management within a results-driven management setting.

It has made it possible to shut down intelligent services in order to meet crucial requirements, such as flexible connectivity, onboard device data management, extremely dependable cloud computing, or privacy policy approach. By fully using the integrated processing capability of peripheral devices, onboard computing could establish device independence based on dispersed sensory input. Furthermore, data processing enables digital manufacturing enterprises to swiftly set up smart manufacturing, which ought to satisfy specific client demands and ongoing modifications to production conditions. For commercial IoT applications, location expertise and inadequate networking were necessary. Because computing on a smartphone is physically appealing, it was easier to deliver high bandwidth, reduced concern for operations near the network edge, and end-to-end latency. IoT-based production was introducing edge computing. Devices near the border at the terminal infrastructure could help extend the availability of IoT embedded gadgets with reasonable processor speed, cache memory, and storage.

Modern Internet of Things (IoT) control systems rely heavily on gateways. Multiple industrial sectors, such as transportation infrastructure, automated operations, manufacturing, including medical services, can be monitored simultaneously through these control system interfaces. In a similar vein, gateway systems now provide unified and streamlined administrative interfaces for advanced control systems[3]. Control gateways with enough computing power could also be used by contemporary IoT client devices to help with remote access security and administration issues. Cloud storage with an interface for a control system is becoming a more and more popular way to manage security. Thanks to improvements in customer device security features, memory capacity, and gateway processing power, gateways may now monitor remote access safety requirements directly through Internet of Things client computers[4].

979-8-3315-1898-1/24/$31.00 ©2024 IEEE

Because Internet of Things (IoT) devices frequently operate in settings with inadequate security infrastructure, it is imperative to secure IoT devices [12].

Security model for Internet of Things (IoT)

Researchers propose a system that allows for the direct or indirect transmission of trustworthy tasks from client devices to gateways or cloud services. The power of management gateways and the sophistication of Internet of Things client computers work together to make this a reality. Security issues with Internet-connected control systems were assessed. Systems where the internet is the primary source of safety, rely on encrypted messages sent between client devices and cloud servers to provide control instructions to the devices. Still, the situation demands a cloud platform. A direct relationship is especially useful when employing a cloud platform was intended or practicable[5]. This idea will look at the case when a gateway and an IoT customer device work together directly to implement control techniques. The user's text is empty. Furthermore, it employs the customer's characteristics and gateway systems to ensure a reliable state during the transaction. In essence, it has the capability to be expanded to a cloud-based system. The client computer gathers the identifying data required for user authentication at the start of the procedure and sends it to the gateway. A multi-factor authentication (MFA) technique validates the user's identification details through the combination of a password and username with biometric data that the client provides, like a fingerprint or photo as mentioned in fig. 1. The gateway will carry out the client's authorised control activities once authentication is successful[6].

Numerous user or environmental parameters can be captured by several smart technologies' sensors. One of these methodologies could be employed to oversee a modification in the client's surroundings. A baseline can be constructed for clients by merging well-known desirable behaviors with sensor data.

Fig. 1. multi-factor authentication

If this stipulation is not met, the participant's identification may be reevaluated or the link may be severed. On the other side, it's possible that the proximity sensor detected a device separation. Utilising solutions such as TrustZone and other trustworthy run-times is crucial to ensure the stability of the client's PC with a stable cloud infrastructure.

The flowchart in Figure 2 shows the steps, which serve as the gateways for the control systems and the Internet of Things clients. Three parts make up the model. Connecting client devices and server gateways and establishing a safe zone are the first three steps. It is assumed that changing one's identification Incorporating screening procedures in phases three and four does not pose a security risk. Cleaning up once the link was established could be the fifth stage. The steps in the procedure are as follows: At the outset, the consumer-side process starts when the customer initiates portal access. In order to finalise the identification procedure, more information will be needed after the bridge verifies the customer's identity.

The gateway verifies the user's identity and determines their authorised category when it receives client identity data, like a 3D picture or any other item. The client device must then act as a gateway for the server after authentication and verification. The Real-Time Identity Monitor needs to be activated in order to scan for any signs of a change in behaviour, such as placing a smartphone down or looking away from a keyboard.

This method makes use of all client-device detectors. When the client required to be re-authenticated, the connection was interrupted, and the bridge was alerted about any impending changes to their identify. The appliance is closed tightly on all sides after it is finished. At any stage in the procedure, the computer will immediately proceed to next step, disconnect connection, sends a negative message to current identity monitor detects any irregularity.

Prior to commencing any control activities, the system gateway must successfully undergo process of identification and verification, which may provide difficulties, particularly during the safety phase. Alternatively, it can use a provider based on cloud to complete the safety processes domestically. Both might be incorporated into the layout. Further study should be conducted in this area, particularly to determine the most effective way to use detector technology to track a customer's identity in real time. One of the best ways to identify objects in motion was using a 3-D camera, which would be a great place to start. However, there are many additional detectors available in modern intelligent technologies that can be utilised for this purpose, such as movement, lighting, or device proximity.

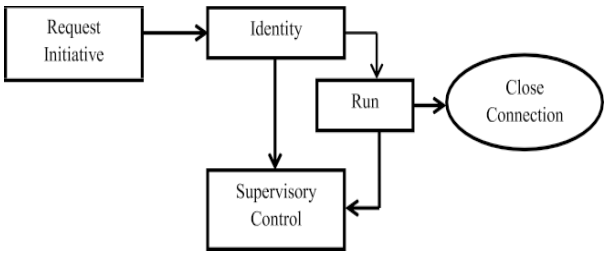

Fig. 2. Functional framework.

II. THE APPLICATION OF E2E IOT ARCHITECTURE IN THE INDUSTRY

To create comprehensive IoT solutions, two core technologies are merged. One is an IoT gateway-connected edge application platform that includes appliances and sensors. An identity monitoring platform was a cloud-based solution that could combine organised, safe, or networked

services in real-time. To guarantee their sustainability, the EAP and CSP are developed with three main goals in mind. Their primary efficacy ought to be at long ranges. They also require remote controllability and protection. They ought to be expandable in terms of storage and usability as well.

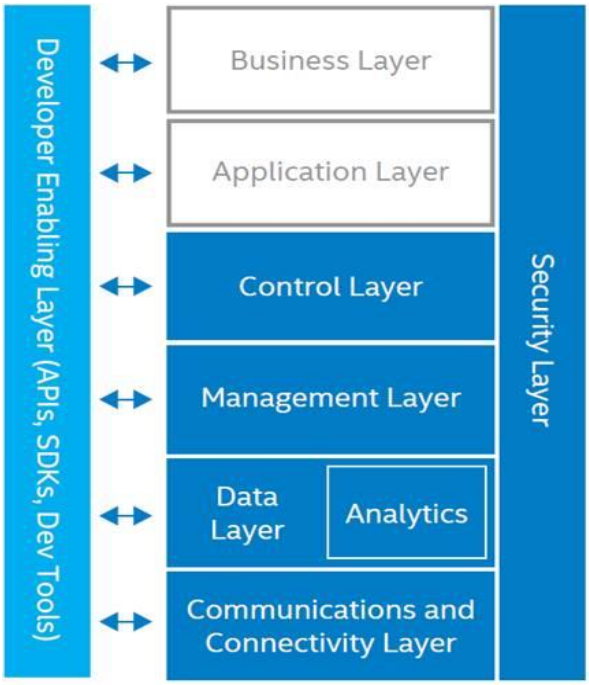

Fig 3. Architecture of IoT

The structural arrangement of the building components. IoT architecture solves the unique problems of EAP by offering a highly customisable technology stack together with a gateway-centric ARP structure. Middleware for processing data input and encapsulation, various wide area network (WAN) connection choices for failover operations, and Inexpensive hardware components for sensors and actuators are essential aspects of the software stack. Customers can utilise a variety of control gateways that make use of System-on-a-Chip (SoC) technology, including alternatives like Quark/Atom core and Xeon[11].

Durability, performance, secrecy, and dependability are just a few of the criteria that should inform the selection process for an Internet of Things application.

III. FINDINGS AND ANALYSIS

For corporate settings, these easily accessible, powerful gateways with robust cryptography and processing capabilities were ideal for protecting an Internet of Things' perimeter (IoT). For endpoint verification & identification provided via Internet to be more reliable, the control system gateway might incorporate real-time detection sensors[15].

One would use this approach to generate security tags for endpoints and edge points. The last devices divide the data they produce into several 16-byte chunks at the outset. When there are no suitable divisions of 16 for the last data block, no infills are applied. Two entries are used to generate the safety label in the S-LEA approach. The 4-byte K shared private key and multiple 16-byte blocks of input data are produced by both end and peripheral devices.

The overall working of Dynamic key generation in six steps are as follows [13]:

First-party key exchange: A safe first key exchange takes place between the Internet of Things device and the server (or another device).

Dynamic Generation of Keys: New keys are generated by the Internet of Things device based on predetermined parameters, including a predetermined time interval, a predetermined number of data transmissions, or the detection of a potential security concern.Using the KDF and the shared initial key, the server or another device synchronises with the Internet of Things device to produce identical keys[14].

Important Distribution: The devices involved safely exchange the freshly created keys. Secure channels that were set up during the first key exchange can be used for this.

.

Here is a simplified way illustrating the process:

1. **Initial Setup:**
    - IoT Device ↔ Server (Initial Key Exchange)
2. **Key Generation Process:**
    - IoT Device: Uses Initial Key + Nonce → KDF → New Key
    - Server: Uses Initial Key + Nonce → KDF → New Key
3. **Data Transmission:**
    - IoT Device → Encrypt Data with New Key → Send to Server
    - Server → Decrypt Data with New Key → Process Data
4. **Periodic or Conditional Key Regeneration:**
    - IoT Device ↔ Server (New Nonce)
    - IoT Device: Uses Previous Key + New Nonce → KDF → New Key
    - Server: Uses Previous Key + New Nonce → KDF → New Key
5. **Key Rotation and Revocation:**
    - Old Keys are Discarded Securely

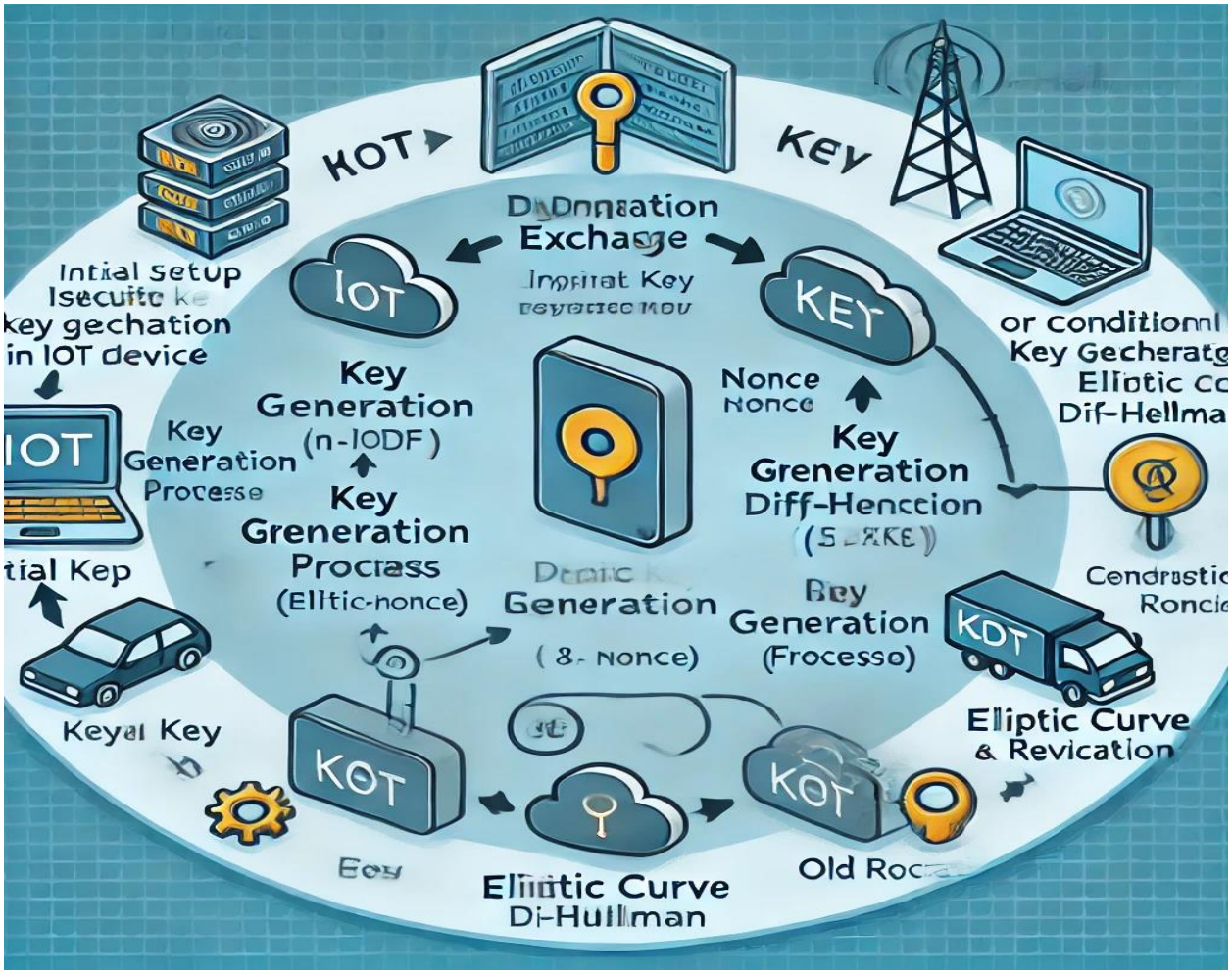

Fig. 4 visual representation of key generation of IoT devices

The phases of initial setup, key generation, data transfer, key regeneration, and key rotation are depicted in this diagram of dynamic key generation in Internet of Things devices [12]. This diagram ought to make the procedure more understandable.

Use of unique round keys improves both computing speed and security. Instead of sticking with the present secret key, it could be wise to update it for the best durability of the security feature[16]. A data block size of 4 or 8 bytes might be required in situations where speed is prioritized and the input block size is limited. You can also choose between two and eight bytes for the key size. As shown in Equation (1), if the current secret cannot be used for the required amount of time, The initial two bits of the key are used to change the key for the shared secret variable (K).

$$a = Z[1], b = Z[2] \qquad (1)$$

In the first equation of the suggested method, the sequence diagrams for generating and updating the private key and security label are detailed. It depicts a situation when malicious changes to the content do not affect the usual functioning of communication. The proposed methodology was finally put into action to guarantee the safe transfer of data between various systems and devices.

IV. Conclusions and Future Work

A gateway device facilitates the connection between consumer client PCs and the Internet. It has the capability to transmit control sequences and alert building maintenance about abnormal requests or important events. The growing connectivity of control systems to the Internet has given rise to significant security concerns. The majority of these inquiries revolve around user authentication and governance. It includes checking that users are who they say they are, making sure the session is secure, and making sure clients can only do what they're told to. By using the enhanced the process, memories, and connectivity of IoT devices, integrating the functionalities of control systems and gateways with consumer IoT devices can potentially address these challenges. This study implemented real-time identity management to enhance security capabilities. The researchers verified that the implementation of secret keys, which rely on a continuous notification timer and a periodic key replacement, was executed accurately. Additionally, they discovered that it posed challenges in our testing environment, which relies on an internal bridge network.

References

[1] V. D. Alagdeve, R. Singh, V. G, B. Parihar, S. Dhananjeyan and B. Ashreetha, "Efficient Data Encryption and Signature Generation Scheme for Resource-Constrained IoT Environments," *2023 7th International Conference on I-SMAC (IoT in Social, Mobile,*

Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 262-269, doi: 10.1109/I-SMAC58438.2023.10290224.

[2] S. S, R. S, R. Singh, R. Vinoth and P. Mishra, "An Improved Anomaly Detection in Wireless Sensor Network using Artificial Intelligence Evolving Optimization Tools," *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, Trichy, India, 2023, pp. 19-24, doi: 10.1109/ICAISS58487.2023.10250678.

[3] Gupta, S., Sharma, M. K., Singh, R., Almashaqbeh, H. A., Rajat, & Gangodkar, D. (2022). "IoT Based Multi-Layered Security Network Authentication System Development Using Blockchain Technology Management". 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022, 2234–2238. https://doi.org/10.1109/ICACITE53722.2022.9823518

[4] Kumar, Y., Koul, A. & Singh, C. A "deep learning approaches in text-to-speech system: a systematic review and recent research perspective". Multimed Tools Appl 82, 15171–15197 (2023). https://doi.org/10.1007/s11042-022-13943-4

[5] G. Manogaran, M. Alazab, P.M. Shakeel, C.H. Hsu, "Blockchain assisted secure data sharing model for the Internet of Things-based smart industries", IEEE Trans. Reliab. 71 (1) (2021) 348–358.

[6] Girdhar, K., Singh, C., Kumar, Y. (2023). "AI and Blockchain for Cybersecurity in Cyber-Physical Systems: Challenges and Future Research Agenda". In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security, vol 102. Springer, Cham. https://doi.org/10.1007/978-3-031-25506-9_10

[7] Rani, S., Ahmed, S.H. & Rastogi, R. "Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications". Wireless Netw 26, 2307–2316 (2020). https://doi.org/10.1007/s11276-019-02083-7

[8] Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., & Singh, P. (2021). "Secure and energy-efficient smart building architecture with emerging technology IoT". Computer Communications, 176, 207–217. https://doi.org/https://doi.org/10.1016/j.comcom.2021.06.003

[9] Singh, R., & Kumar, D. (2017). "Anomaly Prevention Mechanism for Wireless Networks using the Wireless Node Integrity Assessment Program". *Indian Journal of Science and Technology*, *10*(10), 1–5. https://doi.org/10.17485/ijst/2017/v10i10/109291

[10] Singh R., "Enhanced Technique for Energy Efficient Secured Routing Protocol in Manet". (2020). *Journal of Xidian University*, *14*(5), 882–893. https://doi.org/10.37896/jxu14.5/095

[11] Kumar, Y., Garg, P., Moudgil, M. R., Singh, R., Woźniak, M., Shafi, J., & Ijaz, M. F. (2024). Enhancing parasitic organism detection in microscopy images through deep learning and fine-tuned optimizer. *Scientific Reports*, *14*(1), 1–29. https://doi.org/10.1038/s41598-024-56323-8

[12] A. Sachan, D. N. Kumar and A. Adwiteeya, "Light Weighted Mutual Authentication and Dynamic Key Encryption for IoT Devices Applications," *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/ICICT46931.2019.8977672.

[13] T. Ara, P. G. Shah and P. M, "Dynamic key Dependent S-Box for Symmetric Encryption for IoT Devices," *2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Bangalore, India, 2018, pp. 1-5, doi: 10.1109/ICAECC.2018.8479442.

[14] H. Noura, A. Chehab and R. Couturier, "Lightweight Dynamic Key-Dependent and Flexible Cipher Scheme for IoT Devices," 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 2019, pp. 1-8, doi: 10.1109/WCNC.2019.8885976.

[15] Bawa, S. S., Sing, H. (2019). Factor Influencing the Formulation of Effective Marketing Strategies of Indian Railways. *International Journal of Innovative Technology and Exploring Engineering,* 8(9S), 357-362.

[16] Kumar, Y., Singh, R., Moudgil, M.R. *et al.* A Systematic Review of Different Categories of Plant Disease Detection Using Deep Learning-Based Approaches. *Arch Computat Methods Eng* **30**, 4757–4779 (2023). https://doi.org/10.1007/s11831-023-09958-1