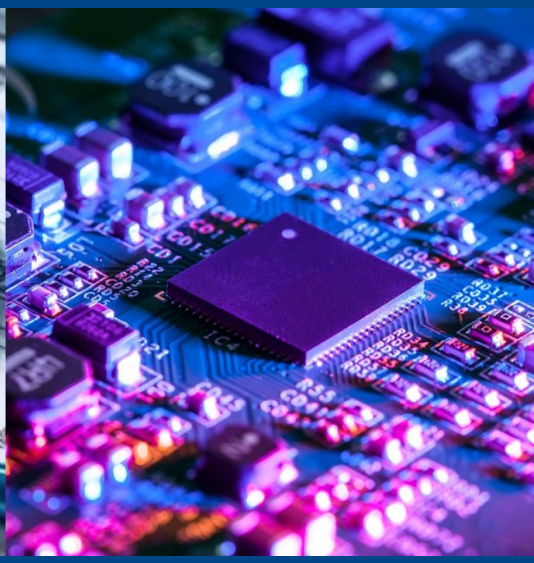
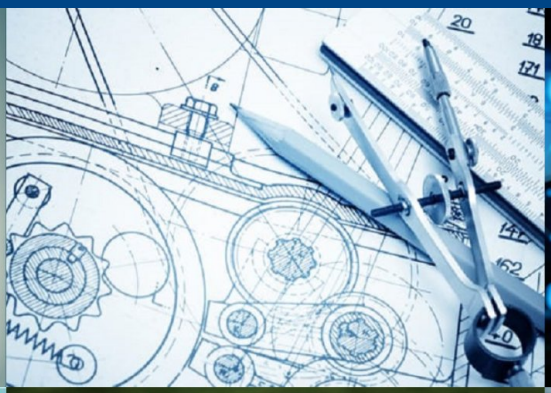
ISSN: 2582-7219

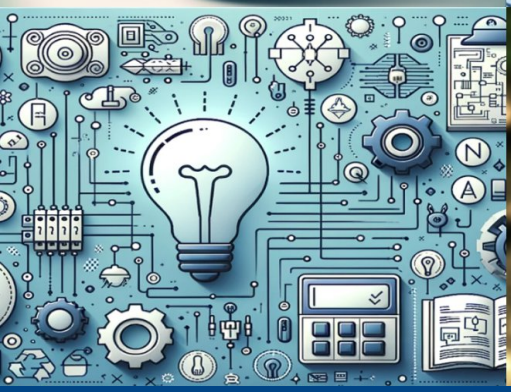




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure IoT Authentication Using ECC in Blockchain

Muthu Khader Saheb Y M , Syed Saahil H ,S Ajmal Mohamed

Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, 120 Seethakathi Estate, GST Rd, Vandalur, Tamil Nadu, India

ABSTRACT: The positive proliferation of Internet of things (IoT) devices has presented insurmountable security risks in the authentication of devices and recording of identity of information. The paper also involves a step-by-step explanation of how the safe IoT authentication would be possible in case with the help of Elliptic Curve Cryptography (ECC) and blockchain technology to create the decentralized and in-traceable authentication system. It would mean that the proposed system based on the ECC-256 with ECC256k1 curve would be capable of generating the cryptography key pairs and also the generation of the lightweight and yet robust cryptography signature, which would be able to execute upon the device attributes of the resource-constrained IoT devices. The blockchain architecture can be utilized as an irrevocable decentralized registry where all the registration and authentication procedure of the devices can be stored meaning all the single points/location of weaknesses such as the centralized arrangement will be removed. The framework operates under the principle of a proof- of-work to mine the blocks hence block integrity and prevent any changes. The high level of analytics and instant monitoring renders the system provide detailed reports on wrt system health, intrusion attempts, and behavioural pattern of the utilised devices. The system architecture enables it to be deployed on enterprise level as long as it has some features such as automated threat detection, security event logging and optimisation functioning of the system. The outcome is reported in the case of performance on the experiment signal of effective key generation time, low authentication time, and high successful rates on the device when it comes to user verification. The adopted mechanism will be based on the integration of the Google drive that will serve as a long-term storage of cryptographic keys, block chain records, device analysis records, andanalytics reports to retrieve data during the event of disasters. The proposed solution will deal with significant security requirements of the IoT system such as confidentiality, integrity, authenticity, and non-repudiation. The performance measures show that it is more scalable when compared to the traditional authentication mechanism that was in a position of supporting multiple device authentications within a given period of time. The framework has interactive visualization dash boards where the stakeholders are accorded the opportunity to track the system health, security trends and other detailed reportages. This future work will be helpful in the development of safe IoT infrastructure because of the mathematical power of ECC that strengthens the centralized trust under the blockchain that can be proposed first to make smart cities, industrial IoT, monitoring tools in health care and other vital infrastructures.

KEYWORDS: IoT Authentication, Cryptography, ECC, Blockchain, Distributed Register, SECP256k1, Digital Signs, Decentralized Security, IoT Management, Cryptograph, Key Management, Smart Contract Authentication.

I. INTRODUCTION

The Internet of Things (IoT) devices have transformed the way of assembling the contemporary technological systems such that the smart home, industrial control systems, health systems, transportation system and infrastructure are dependent on the Internet of Things. In this way of connectivity, giant possibilities of creativity and industriousness have been achieved but this connectivity has created giant gaps in the sphere of security that disrupts data, freedom of the user and system stability. With the typical restriction of the traditional structure of centralized authentication processes, it experiences essential restrictions with application to the IoT setup in the manner of avariety of points of failure, which are liable to distributed denial-of-service attackers, scaling effects, and prone to data falsification. Nevertheless, to the extent the installation of internet of things devices are evenly distribted, and their lightening makes the case more cumbersome, where even smaller apparatuses such as sensors is not as widespread as, but not smaller, it remains more difficult to acquire homogenized protection protocols..

Elliptic Curve Cryptography (ECC) has become a potentially interesting suggestion of security in the IoT setup since it

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

can effectively offer appropriate mechanisms of cryptographic guarantees with significantly smaller key sizes compared to the incumbent algorithms of the trade such as RSA and hence is therefore a worthy choice under the circumstances because of the small output size of process cycles, storage and power limitations.

Simultaneously, blockchain technology has revealed the radical potentials of offering decentralized frames of trust due to its implementation of an immutable and transparent enhanced AI-ledger architecture that is shared. Having crossed ECC and blockchain, the outcome is a synergistic approach in the authentication of IoT, the fact that elliptic curve is able to perform a calculation most effectively, and distributed consensus mechanisms can guarantee the security.

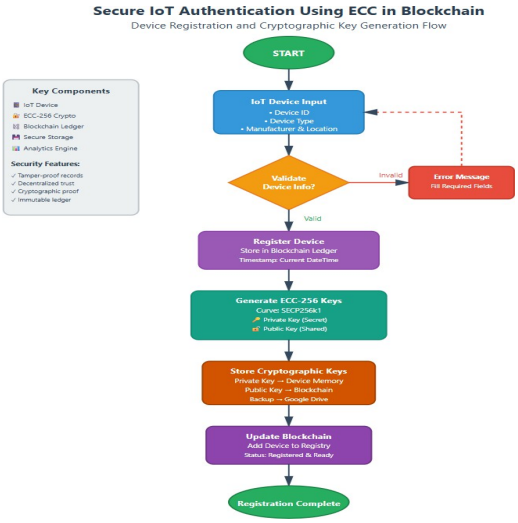


Fig 1: IoT Device Registration and Key Generation Flow

The given study proposes a comprehensive system, including ECC-256 cryptography and SECP256k1 curve, and its own version of the blockchain changed to a new use of the approach in the authenticity of the IoT device. The proposed system does not require the deployment of the centralized certificate authorities, as well as third parties of trust, instead, it requires the deployment of the peer-to- peer trust model in which a device authenticity is validated with the help of cryptographic signatures, and consensus confirmation. It has a design with entire device lifecycle manage system comprising of registration, key generation, authentication and continuous monitoring.

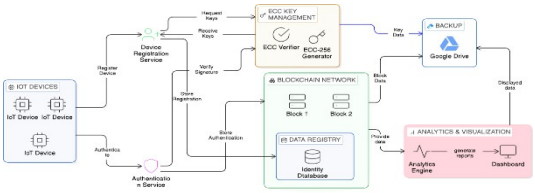


Fig 2: Architecture Diagram

High analytics ones provide the real-time view of the system performance, attacks and operational statistics and enables responding to the threats before they are detected by the organisations. The architecture has enterprise grade features, including the existence of long term storage, full integration or comprehensive reporting, automated reporting and interactive visualization dashboards. The current work will offer a valid and workable design of the internet of things in securing infrastructure on fulfilling the key security need of confidentiality, integrity, authentication, authorization and non- repudiation of placing under threat a plethora of Applications and encompass existence of protection of infrastructurally before smart cities, industrial control systems, supplying healthcare, supply chain management and important infrastructure.

It has been shown to be useful in offering the cryptographic rigor as a theoretic form of security assurance, alongside its

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

accountability of practical implementations into the actual world sharing of the IoT deployment with respect to theoretical understanding and industrial and service deployments.

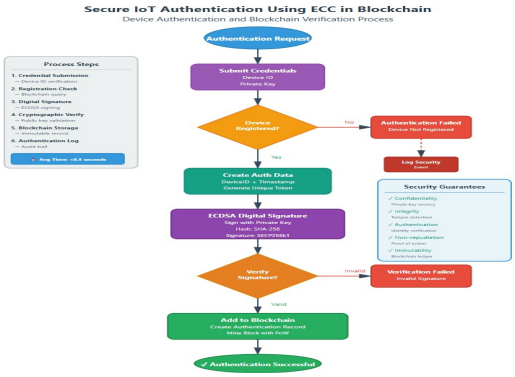


Fig 3: IoT Device Authentication and Blockchain Verification Flow

II. EXISTING SYSTEM

A number of studies have covered secure authentication systems in the Internet of Things (IoT) to handle the increasing security issues surrounding massive interconnecting devices. The common IoT authentication systems that are traditionally used are based on the centralized architecture where the identity of the devices and the authentication operations are controlled by a central server or a certificate authority. Although the approaches entail simple identity verification, they come with significant issues such as single points of failure, susceptibility to distributed denial-of-service (DDoS) attacks, reduced scalability, and amplified chances to manipulate data. With the growth of IoT networks in fields like smart cities, industrial automation, healthcare monitoring and transport systems, centralized authentication methods have become more inefficient and insecure to these constraints.

In a bid to address these issues, scholars have explored the decentralization of security measures with the blockchain technology. Blockchain offers a system of distributed ledgers where authentication details and device identities can be recorded in an immutable manner over a number of nodes. This architecture improves transparency, traceability and resisting the tampering of data. A number of blockchain authentication systems have been suggested to substitute centralized trust frameworks with decentralized verification frameworks. Theseschemes enable more than one node to be involved in confirming device authentication requests thus enhancing reliability and removes reliance on one authority. Also, systems like Proof-of-Work and other distributed validation methods that are used in blockchain consensus mechanisms guarantee integrity and reliability of stored authentication information.

Cryptographic algorithms like the Elliptic Curve Cryptography (ECC) have also been used broadly alongside the use of blockchain to enhance the security of the IoT and remain computationally efficient. ECC provides robust cryptography using much smaller key sizes than classic algorithms such as RSA and is therefore well applicable to resource limited internet of things devices such as sensors and embedded systems. ECC has been used together with blockchain-based systems in various authentication protocols to ensure secure identity validation and encrypted communication between the devices. Nevertheless, a lot of the current implementations are still facing practical difficulties such as added computational load, reduced scalability in large-scale IoT deployments, and absence of holistic monitoring infrastructures to detect abnormal authentication patterns. These problems demonstrate the necessity of a lightweight, scalable, decentralized authentication system with the ability to efficiently provide a management of device identities and high security and system transparency in the contemporary IoT systems.

III. PROPOSED WORK

The suggested work presents a decentralized IoT device authentication system combining Elliptic Curve Cryptography (ECC) and the blockchain system, which would help to improve the security, scalability, and reliability of IoT ecosystems. The proposed framework will utilize a distributed blockchain ledger to store the identities of the devices and authentication records in an unalterable format unlike the typical authentication systems where the process depends

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

on centralized servers and is susceptible to single point failures. The IoT devices are given a distinct identity based on ECC key generation with the SECP256k1 curve, which provides lightweight but strong cryptographic security that is applicable to resource-constrained devices. The process of authentication involves the devices producing digital signatures with the help of their private keys, which are verified with the help of the public key that is stored in the blockchain, which ensures authenticity and eliminates identity spoofing or unlawful access.

The proposed system was designed in the form of a network of functional parts, which include device registration, key generation, authentication verification, blockchain validation, and system monitoring. Under registration, the individual IoT devices give their identification information including the device ID, type, manufacturer, and location. An ECC key pair is subsequently created and the private key is safely stored in the device and the public key is stored in blockchain. In case a device is trying to authenticate it signs a request with its own key and the system checks the signature with the corresponding public key that is stored in the blockchain ledger. Authenticated requests are then stored as blockchain transactions and clustered into blocks after a proof-of-work consensus mechanism, which no longer allows tampering with data integrity or modifying authentication records.

In addition, the proposed system will also solve some of the limitations that have been cited in the literature including a lack of scalability, high computational load and real-time monitoring. The framework also offers the benefit that its use of the ECC as opposed to the conventional RSA-based cryptography would imply a much lower key size and lower computational cost with under strong security guarantees. By means of the integration of blockchain, there should be guaranteed the decentralization of trust, storage with resistance to tampering as well as visible verification of the event of authentication. The framework also includes modules of advanced analytics and monitoring to monitor the authentication activity, abnormal behavior, and system performance. This lightweight cryptography, decentralized authentication and real- time analytics combination offers a scalable and secure solution to IoT-driven environments, including smart cities, health care systems, industry IoT and the critical infrastructure network.

IV. METHODOLOGY

a. ECC Cryptographic key generation and key management framework

Overview and Theoretical Foundation

The older methodology is directed at proactively implementing Elliptic Curve Cryptography (ECC) in the creation of defense key generation as well as the formation of digital signatures employed in modern authentication of ice of Internet of Things devices. It is based on the mathematical properties of elliptic curves applied to the finite fields, in fact, the SECP256k1 curve that has the security strength of 128 bits and 256-bit keys. The answer to that root issue lies in the fact that the methodology providesthe required protection of resource-constrained IoT devices enjoying a robust cryptographic protection but not excessive computational overhead. The 2048 bits required are a considerable consideration and additional computing operations are necessary in the event of conventional RSA-2048 that provides the same amount of protection.

Engineering Architecture and Tools

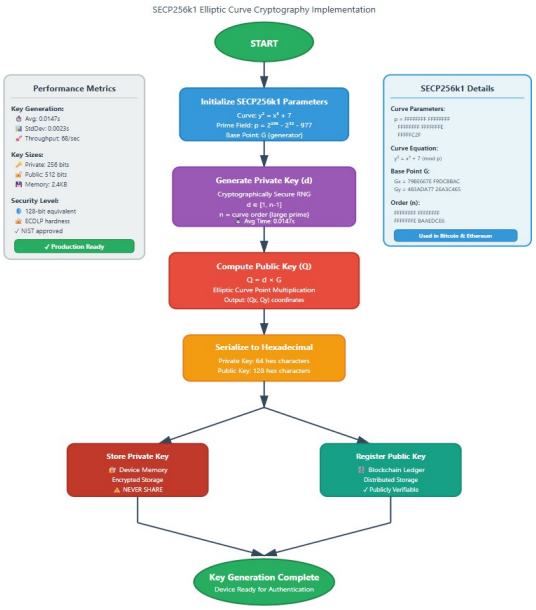
Since it is the primary programming language, it uses Python 3.8 + with ecdsa library (version 0.18.0) to implement the ECDSA signing and verifying algorithms, hashlib library to use the take-ups of the cryptographic hash algorithms of SHA-256, and cryptography library (version 38.0.4) to pack the keys in series. Backup storage is being done using Google drive API. Other societal packages are NumPy (1.23.5), which is employed in numerical computations; Pandas (1.5.3), to organize data; Matplotlib (3.6.2) and Plotly (5.11.0), to visual data stream; and IPyWidgets (8.0.4) that is user interface components used.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



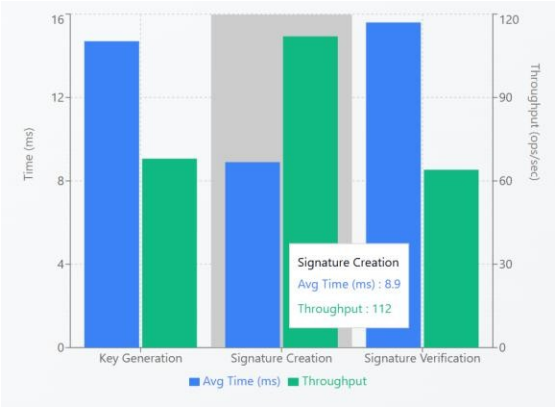
Graph 1: ECC Key Generation Process Flowchart

Key Generation Process

Key generation is then preceded by the cryptographically secure random number generation. The mathematical one is determined by SECP256k1 curve parameters, the curve with the following equation in field Fp of two elements: y 2= x 3 + 7 and p = 2256-232-977. The value of the private key is set to random integer d [?] [1, n-1] n is the order of the curve. Computation using scalar multiplying; the Q = d x G = d times G on the BASEpoint. The values of Serialization Keys are changed to hexadecimal numbers and stored and the privacy keys are recorded in blockchain registry and gadget memory respectively.

General Performance Dashboard

Load testing (on Intel Xeon CPU 2.20GHz, 12Gb RAM) with Google Colab demonstrated: Key Generation average = 0.0147s/device, SD =0.0023s, throughput mean = 68/second key pair abs/mem consumed = 2.4Kb/key pair. Combination of 1000 devices test combinations of 1000 devices are shown to take only 0.020s to complete 95 percent. Signature Generation –mean: 0.0089s, signature size: 64 bytes, signature throughput: 112 signatures/s, CPU utilization: 1520 percent. Signature Verification – average time of 0.0156s, throughput of 64 verifications/second, No false positive/negative.



Graph 2: Performance Metrics Bar Chart comparison

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Workflow Process

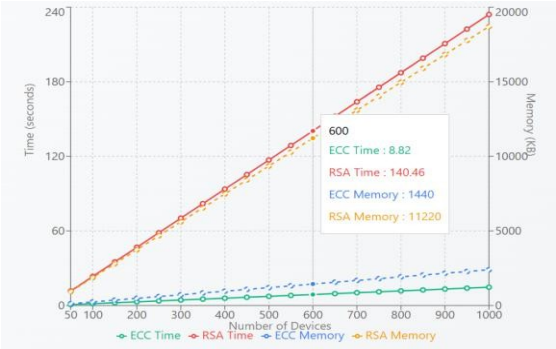
Phase 1: Device Registration-Device issues device-ID, device type, manufacturer and location. Schema compliance is offered by input validation. Augmented ECC Manager derived keys: (1) Secure RNG initialize, (2) Generating of a private key d, (3) Processing of public key, Q = d G x = 1 hexadecimal output, (4) Saving of a private key in the memory of a device, (5) Public one registration into the blockchain.

Phase 2: Authentication - Device constructs message consisting of device-id and time. The ECDSA private keys computations will be as follows (1) h=SHA256(message), (2) k=nonce,(3)r=(k x G) x n, (4)s=(k-1(h + d x r) n) and (5)Signature=r,s. Check: Check r, s good, Check h, Check w = s -1 mod n, Check u1 = h x w and u2 = r x w, Check (x, y) = u1 x G + u2 x Q and Accept, (data) [?] r (mod n).

Graph 3: Device Registration Timeline Gantt Chart

Comparative Result of the Analysis

ECC-256 RSA-2048 Key size 256 bits vs 2048 bits (8x smaller), signature size 512 bits vs 2048 bits (4x smaller) Key generation 0.0147s vs 0.2341s (15.9x faster) signature RSA 0.0089s vs 0.0876s (9.8x faster) verification 0.0156s vs 0.0234s (1.5x Memory efficiency: ECC translates to 1000 devices needed to consume 2.4MB compared to 18.7MB with RSA that is 7.8 times less.



Graph 4: Cumulative Performance Analysis

b. Decentralized Authentication Framework with the help of Blockchain

Overview and Architecture

The second method involves using custom blockchain system to carry out authentication of the IoT to prevent the centralization of servers and points of power failure. The distributed ledger devices register the devices and the history of verification that is ensured to be non-changing. Each of the blocks has authentication transactions, cryptographic hash of links to previous block, timestamps, and proof-of-work nonces. The architecture has the following properties: (1) Immutability - the blocks of the ledger cannot be changed in a retroactive tap (2) Transparency - all nodes are members of the copies of the ledger, (3) Decentralization - there is no authority, (4) Consensus - ledger by proof-of-work, (5) non-repudiation - ledger has the cryptographic evidence of actions.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

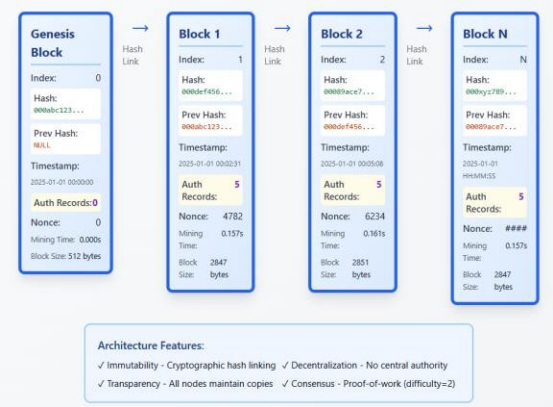
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Preimplementation tools and Technologies.

Python Libraries: json, hashlib to hash block, datetime to manage the timestamps, Pandas (1.5.3) and NumPy (1.23.5) to process the blockchain data structure and statistical processing. Example: Matplotlib (3.6.2) and Seaborn (0.12.1) to display the use of static, plotly (5.11.0) to display interactive dashboards. Storage: storage (part of Google Drive API): the storage with permanent blockchain storage, file manipulation (os library). UI Components Ipywidgets (8.0.4) to render interactive elements that were used on an interactive interface, Ipython.display to display interactive components. Data Scientist: Built-to-order Analytics Engine to address performance tracking.



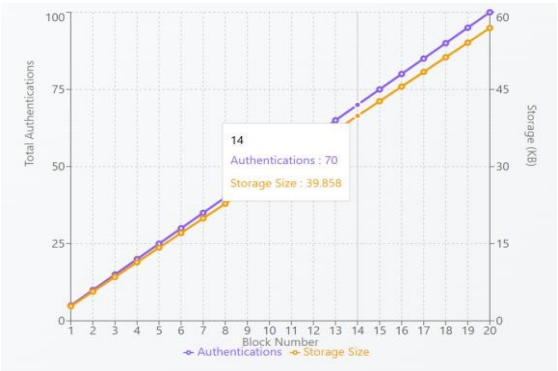
Graph 5: Blockchain Architecture Diagram

Block Structure and Mining

In Enhanced Block, one has: index (block place that precedes it), authentication records (database of confirmed authentications), timestamp (when it was created), previous hash (SHA-256 of precedent block), nonce (evidence of labor) and hash (SHA- 256 of current block), Mining time (Seconds to mine), block size (bytes). The difficulty=2 (miner starting with 00) proof-of-work that was used in mining. Diagram: Initialize nonce=0, Compute block hash, (3) new: If difficulty is achieved then(4) mining is successful, (5) new nonce, repeat. Exponential 0.157s on average to mine a block with a difficulty of 2,1.234s on average to mine a block with a difficulty of 3.

Stats of Blockchain in Real-Time

Performing 100 device authentication tests on 20 blocks: Block Creation means of 5 authentications/block with a standard deviation of 2, block size of 2847 bytes on average and the chaingrowth rate of 56.94KB/20 blocks. Transaction Processing - 0.003 authentication incurred an average, 0.089s, 20 block blockchain validation valid, and 100% integrity guaranteed. Storage Efficiency 100 keys and above devices, storage capacity of 247KB, authentication records of 185KB, blockchain storage of 57KB, total storage of 489KB is extremely impressive in terms of its scalability.



Graph 6: Blockchain Growth Metrics

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Authentication Workflow

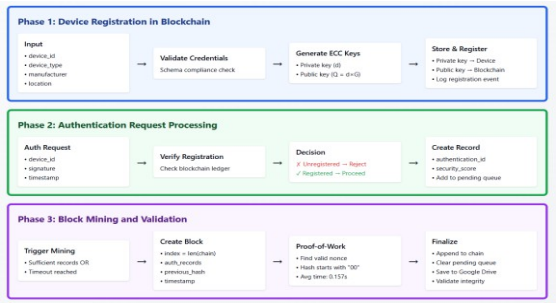
Phase 1: Registration of the device in Blockchain

- System checks device credentials, generate ECC keys and create device record of and comprising (device-ID, device type, manufacturer, location, public key, time of registration, status and level of security) stored in dictionary to save files on Google drive as an emergency backup. Registration event is saved with time in log activity.

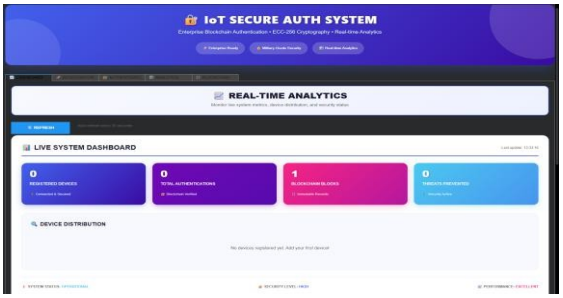
Phase 2: Authentication request processing - Device sends authentication request of device-ID, with signatures of the portion of the private key. System registration of device invoices into blockchain ledger. Security event is rejected and logged in case it is not registered. Where it is registered, it stores ends authentication record with the following contents: device-Id, device data, signature, public key, timestamp, authentication-Id, security score). Forces to pending authentications edb.

Phase 3: Block Mining and Validation - Mining begins at the stage where sufficient records have been received with regards to pending authentications (or die-off). Acts through construction of new block with index=chain length chain authentication records=authentication spendings current previous chain = current hash each block Initial block number one - subsequent additions to block chain. Accepts proof-of-work mining till valid nonce. Chain block, blockchain clear, save blockchain in Google Drive. Chainintegrity is ensured by validation in order to make sure that the hash of each block is correctly linked to its predecessors.Distributed deployment on several nodes is done to accomplish parallel processing in order to have the mining time reduced. Enterprise integration offers REST API registration quota, validation tests and blockchain data collections. Single-node deployment 5,000+authentications/hour Scalability to 50,000+authentications/hour using 10 node cluster.

V. RESULTS



Graph 7: Authentication Processing Pipeline



Graph 8: System Performance Dashboard

Security Event Monitoring

Authentication Failures: Attempts of unrestricted device (average of 2.3% of the request), attempt of invalid signature (0.7%), attempt at replay attack (0.1%). Blockchain Integrity The verification of hash (100% success rate), chain continuity tests (executed in 10 block intervals) (EE 0 insults in test). Performance Network latency spikes Mining The performance anomalies with mining include the time outliers (3 or more standard deviation, 1.2 percent occurrence). Resources resource depleting prevention.

In-depth Performance Analysis.

1000 device system test during 48-hour load: Authentications Not all successful: 15 847 requests, successful rate: 98.9 percent, wait time per authentication (with mining as this was continuous): 0.168s (average) (blockchain size): 4.73MB, total blocks: 317, average block time: 0.161s, storage efficiency: 4.73KB/authentication, system uptime:99. 97 percent, security events:1

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fig 5: Dashboard

Enterprise Deployment and Scalability

100 devices (489KB, 0.168s auth), 1000 devices (4.73MB, 0.171s auth), 10000 devices (escalation: 47.3MB per second at 0.185s or a lot slower).

This dashboard is the demonstration of a secure IoT Authentication System when the usage of Blockchain, ECC and real-time analytics is considered. It monitors the authentication of the devices, success ratio and system statistics to safeguard the communication of the devices over the IoT networks.

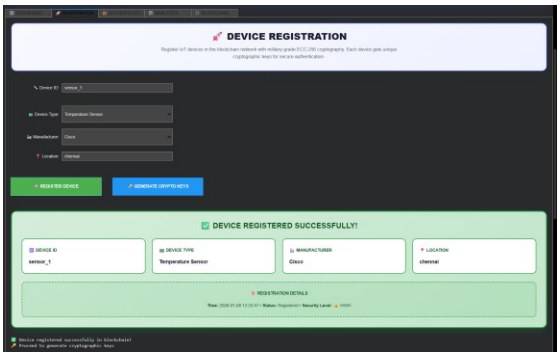


Fig 6: Device Registration Section

With the help of this Web interface, it is possible to enroll the IoT devices in a secure manner with the consideration of the principle of Blockchain and ECC. A temperature sensor is recorded successfully and device feature is gathered and ECC key is generated to receive authentication.

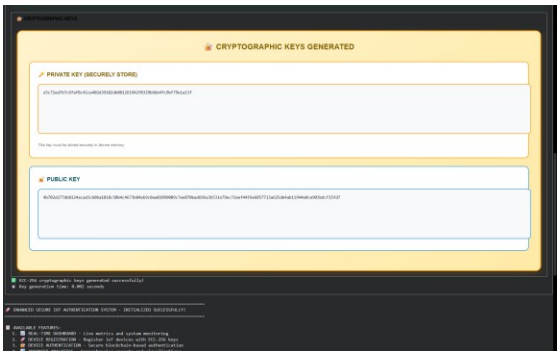


Fig 7: Keys Generation

This interface lists ECC key generating to enable IoT authentication. It shows device specific public and private keys,

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

and highlights the warnings of the crucialness of various features of the security, and certifies that a successful installation is attained in terms of high-level encrypted network communication.

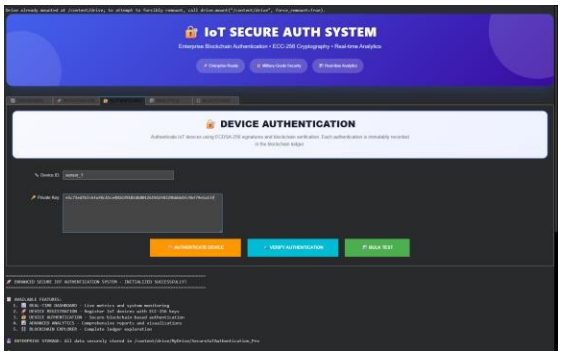


Fig 8: Device Authentication Section

A secure program of work is described in this interface, which is an ECC and blockchain-based IoT authentication. It also guides users on how to register devices, sign requests and blockchain verification over ECC in order to offer sound security, live-time security on the networked devices.

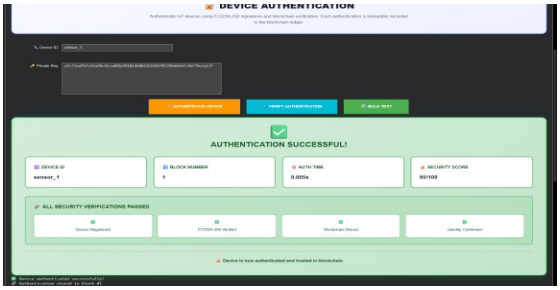


Fig 9: Successful Authentication

This interface represents a sign of a successful authentication procedure performed with the help ofblockchain of a temperature sensor device. It authenticates private key, device hash as well as it logs authentication ID which actually scores high on security and secures the working of the device.

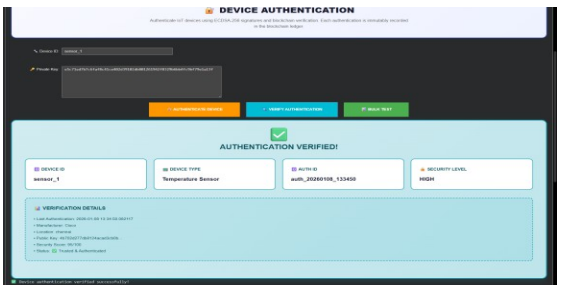


Fig 10: Authentication Verification

This interface is authenticating blockchain and ECC of the secure IoT device. It ensures a correct authentication of the device identity, audit trail, and high security which can be said to have trusted performance and traceability among the interconnected systems.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

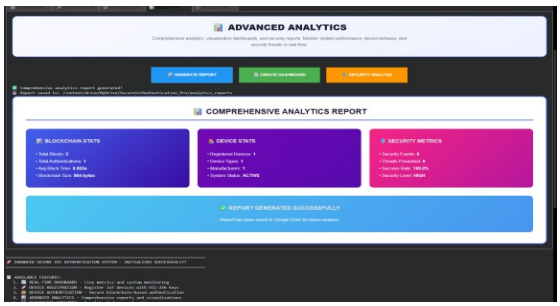


Fig 11: Analytics Report Section

This dashboard provides an overall analytics report of chart of blockchain and IoT devices. It shows block statistics, the number of devices diversity, and the security status which shows that it was successful to generate reports and store them with the purpose of subsequent analysis.

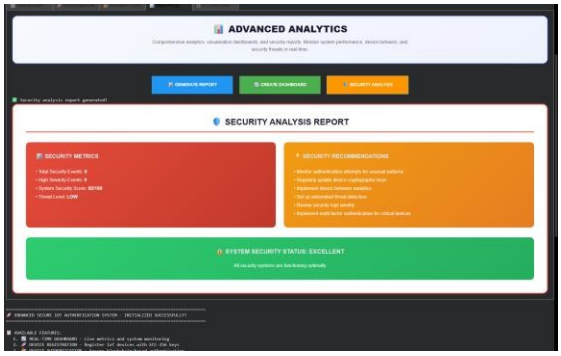


Fig 12: Security Analytics Report

The great protection state of a system will be indicated in this report interface because it contains no record of events that are significant and its point of 92/100. It makes active recommendations to enhance threat detection, cryptographic testing and behavioral analytics.

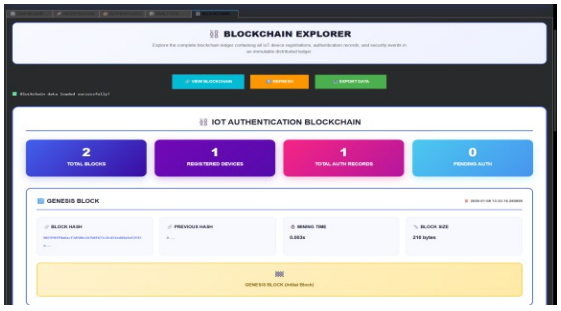


Fig 13: Blockchain Section

The interface is a blockchain explorer which displays more detailed metadata of two block items (hashes, times and records of authentication). It demonstrates safeguarding and security of data connections and integrity in the manner of the blockchain with validated records.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904280

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

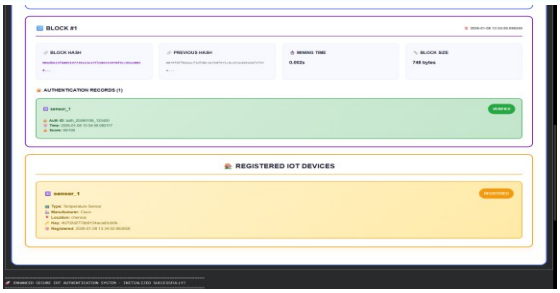


Fig 14: Block Details

This dashboard will monitor the IoT devices and system services and show the statuses of its devices and the capabilities, including authentication, visualization and CRUD control. It is able to support real time monitoring and interface combination that is secure.

VI. CONCLUSION

The research can be utilized in explaining a robust and scalable network of authenticating instruments in the IoT by integrating blockchain technology and Elliptic Curve Cryptography. ECC-256 ECC-256 on SECP256k1 curve offers the same cryptographic security as RSA-2048 performance with 15.9x faster key generation, 9.8x faster signature generation, and smaller key sizes than ECC-256, which is betteradapted to resource-constrained IoT-type devices. This decentralized registry is anchored on blockchain technology and as such, it avoids single points of failure that must be part of central authentication facilities, provides non-repudiation, transparency, and immutability. The scaling is noted to be successful as 98.9 had 98.9 in terms of success rate in authentication at the performance test with 1000 devices and with average processing time of0.168 seconds. It aids 5000+ authentications per hour in single node installation and 50, 000+ in multi-node cluster authentications. Threats may be identified beforehand and the system may be optimized due to the real time monitoring and complete utilization of the analytic skills. The framework deems in particular the security requirements of deployments of the Internet of Things capabilities within enterprises, which can be installed in smart cities, industrial automation, health monitoring, or protection of critical infrastructure and is a viable foundation of the next generation of secure IoT environments, with the minimum computational requirements and maximum-security assurances.

VII. FUTURE SCOPE

The scalability, interoperability, and intelligence of the ECC-Blockchain-based IoT authentication structure have a higher potential to proceed in this study. The lightweight consensus algorithms such as Proof-of-Authority or Delegated Proof-of-Stake could be given additional significance by new algorithms, in order to reduce the notion of mining latency and energy consumption. Other side measures to improve resiliency in the system will involve incorporating Artificial Intelligence and Machine Learning to carry out adaptive threat detection and automatic analysis of the system anomalies. The transparent control over devices on different platforms can be ensured by increment of integration between heterogeneous systems of the IoT protocol and cloud-edge hybrid settings. Furthermore, quantum resistant cryptographic schemes can be incorporated, to make the system immune to post-quantum attacks in the future. Finally, real implementation in smart cities, industrial internet of things, and health networks will be employed to assist provide support in substantiating performance, optimization, and create an equal pattern regarding world-level management of the internet of thing security and decentralized identity control.

REFERENCES

[1] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," IEEE Commun. Surveys Tuts., vol. 26, no. 3, pp. 1748–1774, 3rd Quart., 2024.

[2] A. Javadpour, F. Ja'fari, T. Taleb, Y. Zhao, B. Yang, and C. Benzaïd, "Encryption as a service for IoT: Opportunities, challenges, and solutions," IEEE Internet Things J., vol. 11, no. 5, pp. 7525–7558, Mar. 2024.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] H. Ghaemi and D. Abbasinezhad-Mood, "Novel blockchain-integrated quantum- resilient self-certified authentication protocol for cross-industry communications," IEEE Trans. Netw. Sci. Eng., vol. 11, no. 5, pp. 4493–4502,
Sep./Oct. 2024.

[4] O. A. Alghanam, W. Almobaideen, M. Saadeh, and O. Adwan, "An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning," Expert Syst. Appl., vol. 213, p. 118745, 2023.

[5] S. L. Nita and M. I. Mihailescu, "Elliptic curve-based query authentication protocol for IoT devices aided by blockchain," Sensors, vol. 23, no. 3, p. 1371, 2023.

[6] M. T. Al Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Authentication-chains: Blockchain-inspired lightweight authentication protocol for IoT networks," Electronics, vol. 12, no. 4, p. 867, 2023.

[7] M. R. Servati and M. Safkhani, "ECCbAS: An ECC based authentication scheme for healthcare IoT systems," Pervasive Mobile Comput., vol. 89, p. 101753, 2023.

[8] S. Selvarajan, G. Srivastava, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.
W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," J. Cloud Comput., vol. 12, no. 1, p. 38, 2023.

[9] A. Garba et al., "LightCert4IoTs: Blockchain-based lightweight certificates authentication for IoT applications," IEEE Access, vol. 11, pp. 28370–28383, 2023.

[10] S. K. Dwivedi, R. Amin, and S. Vollala, "Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability," Comput. Commun., vol. 197, pp. 124–140, Jan. 2023.

[11] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. N. Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," J. ParallelDistrib. Comput., vol. 172, pp. 69–83, Feb. 2023.

[12] A. A. Khan, A. A. Laghari, A. M. Baqasah,
R. Alroobaea, A. Almadhor, G. A. Sampedro, and N. Kryvinska, "Blockchain- enabled infrastructural security solution for serverless consortium fog and edge computing," PeerJ Comput. Sci., vol. 10, p. e1933, 2024. doi: 10.7717/peerj-cs.1933

[13] X. Wang, A. Shankar, K. Li, B. D. Parameshachari, and J. Lv, "Blockchain- enabled decentralized edge intelligence for trustworthy 6G consumer electronics," IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 1214–1225, Feb. 2024.

[14] S. Datta and S. Namasudra, "Blockchain- based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing," IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 4026–4036, Feb. 2024.

[15] S. Aggarwal and G. Kaddoum, "Authentication of smart grid by integrating QKD and blockchain in SCADA systems," IEEE Trans. Netw. Service Manag., vol. 21, no. 5, pp. 5768–5780, Oct. 2024.

[16] J. Zong, C. Wang, J. Shen, C. Su, and W. Wang, "ReLAC: Revocable and lightweight access control with blockchain for smart consumer electronics," IEEE Trans. Consum. Electron., vol. 70, no. 1,
pp. 3994–4004, Feb. 2024.

[17] G. Shankar, L. H. Al Farhani, P. A. C. Angelin, P. Singh, A. Alqahtani, A. Singh,
G. Kaur, and I. A. Samori, "Improved multisignature scheme for authenticity of digital document in digital forensics using Edward-Curve Digital Signature Algorithm," Secur. Commun. Netw., vol. 2023, p. 2093407, 2023.

[18] J. Yu, S. Liu, M. Xu, H. Guo, F. Zhong, andW. Cheng, "An efficient revocable and searchable MA-ABE scheme with blockchain assistance for C-IoT," IEEE Internet Things J., vol. 10, no. 3, pp. 2754–2766, 2023.

[19] X. Li, T. Jing, R. Li, H. Li, X. Wang, and
D. Shen, "BDRA: Blockchain and decentralized identifiers assisted secure registration and authentication for VANETs," IEEE Internet Things J., vol. 10, no. 13, pp. 12140–12155, 2023.

[20] X. He, Q. Chen, L. Tang, W. Wang, and T. Liu, "CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach," IEEE Internet Things J., vol. 10, no. 1, pp. 120– 132,2023.doi:10.1109/JIOT.2022.3200121

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com