Secure IOT Authentication Using ECC in Blockchain

Aditya Ankana[1] , Nandiraju Bhargav[2], Koduru Mahesh Reddy[3], Mallempalli Gagan Chandra[4]

[1]Koneru lakshmaiah foundation, Department of IoT, Vaddeswaram, Andhra Pradesh, India,aditya.ankana@gmail.com

[2]Koneru lakshmaiah foundation, Department of IoT, Vaddeswaram, Andhra Pradesh, India,nandirajusgt@gmail.com

[3]Koneru lakshmaiah foundation, Department of IoT, Vaddeswaram, Andhra Pradesh, India,mrk2122004@gmail.com

[4]Koneru lakshmaiah foundation, Department of IoT, Vaddeswaram, Andhra Pradesh, India,gaganchandramallampalli9@gmail.com.

Corresponding Author: Aditya Ankana, Koneru lakshmaiah foundation, Department of IoT, Vaddeswaram, Andhra Pradesh.

Abstract

The optimistic increase in Internet of things (IoT) devices has imposed unrivalled security threats in authentication of devices and recording of identity of information. The paper also presents a detailed description of the way that safe IoT authentication would become possible under the assistance of Elliptic Curve Cryptography (ECC) and blockchain technology to develop a decentralized and un-traceable authentication system. The proposed system using the ECC-256 with ECC256k1 curve would be able to achieve the generation of the cryptography key pairs as well as the generation of the lightweight and yet robust cryptography signature that would be able to run on device characteristics of the resource-constrained IoT devices. The blockchain design can be employed in the form an irrevocable decentralized registry, where all the registration and authentication operation of the devices can be located meaning all the single points/location of vulnerability like the centralized arrangement is eliminated. The structure works based on the concept of a proof-of-work to web mine the blocks therefore block integrity and avert any modifications. The advanced analytics and real- time monitoring make the system give detailed view wrt system health, breach attempts, and behaviour patterns of the devices used. The system architecture allows it to deploy at enterprise level given that it contains some features like automated threat detection, security event logging and optimising functioning of the system. Results are presented in the case of experimental performance showing effective key generation time, low authentication time and high success rates during user verification on the device. The implemented

mechanism will utilize the combination of Google drive that will be a long-term repository of cryptographic keys, block chain records, device analysis records, and analytics reports to access data in case of disasters. The proposed solution will address major security standards of the IoT system like confidentiality, integrity, authenticity, and non-repudiation. The performance metrics indicate that it is more scalable as compared to the traditional authentication mechanism that had the capability of supporting various device authentications during a certain time frame. The framework possesses interactive visualizations dashboards through which the stakeholders are provided with the chance to monitor the system health, security trends and other detailed reportages. This work in the future will assist in creating safe IoT infrastructure due to the mathematical strength of ECC supporting the centralized trust under the blockchain in the first place that can be suggested to render smart cities, industrial IoT, monitoring tools in health care and other essential infrastructures.

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

1). Introduction

The devices of the Internet of Things (IoT) have revolutionized the manner of gathering modern technological systems to the extent that billions of smart devices in smart homes, industrial control systems, health systems, transportation system, and infrastructure rely on it. With such connectivity, massive potentials of creativity and industrious activity have been realized but such connectivity exposes massive openings in the domain of security

causing interference with data, user privacy as well as system stability. Having the normal limitation with the conventional arrangement of centralized authentication procedures, it undergoes critical limitations with application to the IoT configuration similar to a single point of fails, vulnerable to distributed denial-of-service assailants, scaling repercussions and inclined to data distortion.

However, as far as the deployment of internet of things devices are distributed evenly, and their lightening complicates the case, where even more modest devices like sensors is not as ubiquitous as, but no smaller, it is still more challenging to gain homogenized protection protocols. In the wake of the continuously-changing degrees of cybersecurity and the threat degree at any particular time, the necessity to implement solid, interchangeable and scalable authentication systems have been left as a second consideration as the priority need.

Elliptic Curve Cryptography (ECC) has emerged as a potentially intriguing recommendation towards security in the IoT context as it can potentially provide suitable mechanisms of cryptographic assurances using considerably smaller key sizes than traditional algorithms of the trade such as RSA and therefore makes a deserving selection under the conditions due to the small output size of process cycles, storage and power constraints.

At the same time, blockchain technology has demonstrated the revolutionary possibilities of providing decentralized frames of trust through its application of an immutable and transparent enhanced AI-ledger architecture that is disseminated. With the intersection between ECC and blockchain, the result is a synergistic method in the authentication of IoT by the fact that elliptic curve can execute computations as efficiently as distributed consensus mechanisms ensure the security.

In this context, integrating ECC with blockchain for IoT authentication not only enhances security but also improves efficiency and scalability. By leveraging ECC's lightweight cryptographic operations, even resource-constrained IoT devices can participate in secure communications without being burdened by heavy computation or large key sizes. Meanwhile, blockchain provides a decentralized and tamper-proof ledger, ensuring that authentication records are transparent, verifiable, and resistant to unauthorized modifications. This combination addresses the critical challenges of centralized authentication systems, such as single points of failure and susceptibility to attacks, while offering a flexible framework capable of adapting to the dynamic and heterogeneous nature of IoT networks. As IoT ecosystems continue to expand, such a hybrid approach promises to strengthen device trustworthiness, safeguard user data, and enable the seamless deployment of secure and scalable IoT applications.

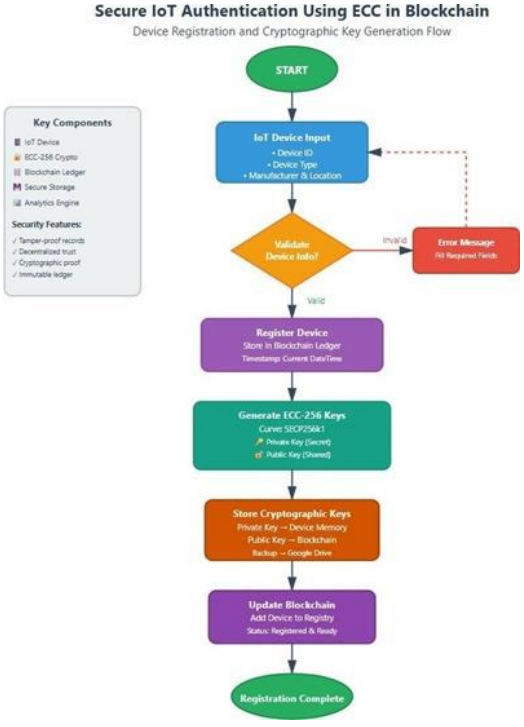


Fig 1: IoT Device Registration and Key Generation Flow

The presented research offers an all-encompassing framework, incorporating ECC-256 cryptography and SECP256k1 curve, with its own blockchain version adapted to a new application of the method in authenticating IoT devices. The proposed system replaces the use of centralized certificate authorities and third parties of trust with the use of the peer-to- peer trust model where a device authenticity is approved by using cryptographic signatures and confirmation by consensus. The design has an entire device lifecycle manage system that consists of registration, key generation, authentication, and continuous monitoring.

High analytics ones give the real-time insight into the system performance, attacks, and operational statistics and allow reacting to the threats prior to the organisations detection. The architecture uses enterprise grade characteristics such as the presence of persistent storage, full integration or complete logging, automated reporting, and interactive visualization dashboards. The present study will present a valid and practical architecture of the internet of things in securing infrastructure on the satisfying of the fundamental security requirement of confidentiality, integrity, authentication, authorization and non-repudiation of putting under threat a myriad of Applications and encompass existence of protection of infrastructurally ahead of smart cities, industrial control systems, supplying healthcare, supply chain management and important infrastructure.

It has been proven to be valuable in providing both the cryptographic rigor as a theoretic kind of security assurance, as well as its consideration of practical implementations into the real world sharing of IoT deployment with regard to theoretical comprehension and industrial and service deployments.

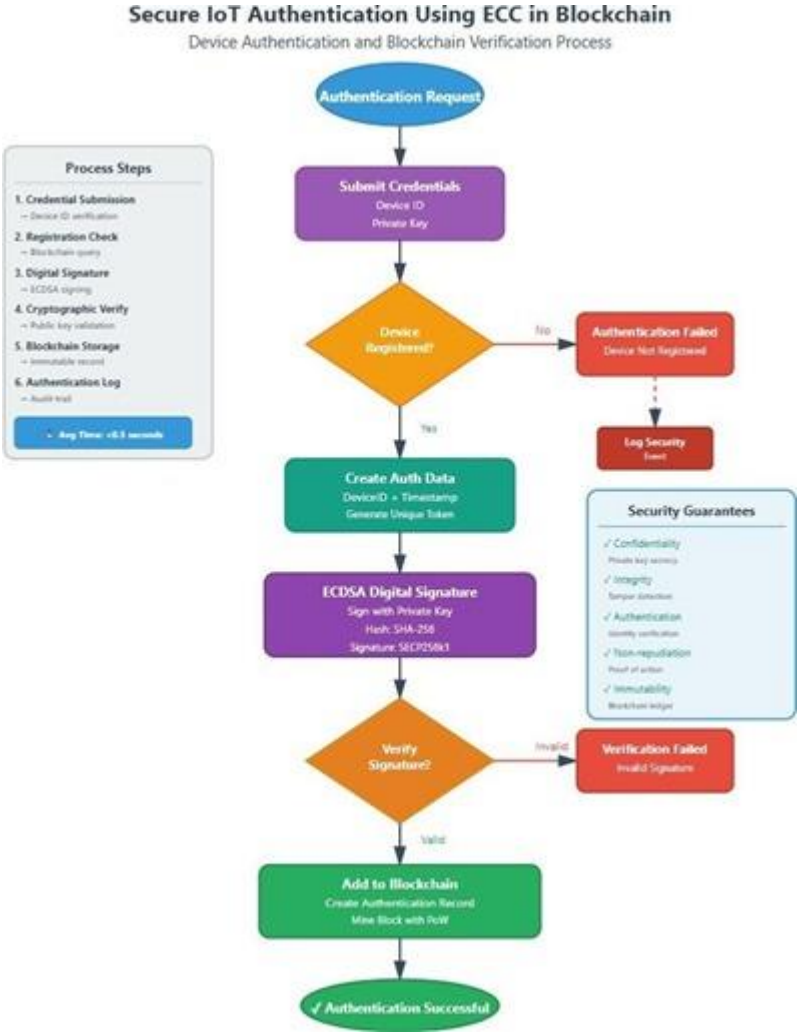


Fig 2: IoT Device Authentication and Blockchain Verification Flow

2). Literature Review

It has been mentioned that there would be a need to merge the blockchain technology platform with the Internet of Things (IoT) systems hence proposing a line of critical research that would analyse the safety concerns present in the distributed networks of devices. The first author who made a study on the applications of blockchain in the IoT was the works of Christidis and Devetsikiotis [1] and the reason is that it demonstrated how the distributed ledger technology can mitigate centralized weaknesses of the traditional authentication frameworks. Then, Dorri et al. [2] came up with a lightweight blockchain-based architecture that is focused on IoT ecosystems and argued the need to have resource- efficient consensus designs that can be used in constrained devices. Hankerson et al. [3] have also conducted many studies on the application of Elliptic Curve Cryptography (ECC) in the security of IoT systems and established technical groundwork that explained the high-efficiency of ECC over cryptosystems based on RSA and especially its keysize and computational capabilities.

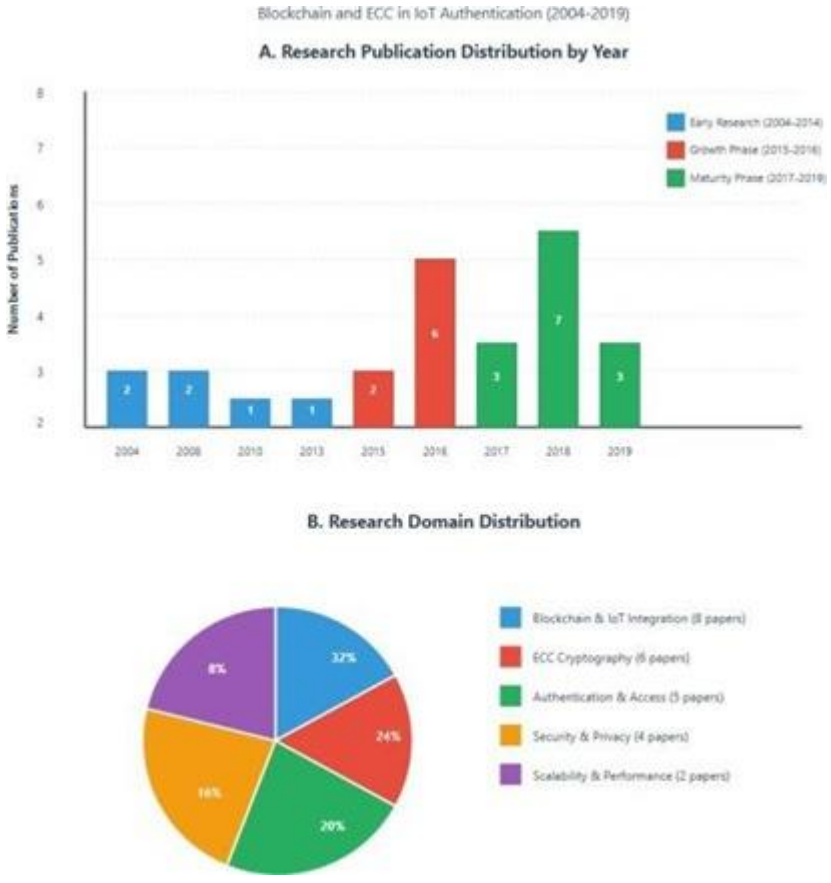


Fig 3: Rese arch Publication Timeline and Domain Distribution

The decentralization of personal data management based on blockchain, as further developed by Zyskind et al. [4], provided the foundation to the discussions on decentralized identity verification, being without a central authority in identity verification. Ali et al. [6] focused on blockchain- authentication protocols of IoT devices, introducing the frame-based models, which will use smart contracts to avert or authenticate the automated systems to importance by incorporating cryptographic guarantees using SECP256k1 elliptic curve as the main technology to achieve digital authentication of the signature scheme.

Brown [5] fully analysed the SECP256K1 elliptic curve to give the cryptographic assurance of the digital signature schemes in a distributed system. Roman et al. [7] systematically defined the IoT authentication security requirements, with confidentiality, integrity, availability, authentication, and non-repudiation being the key pillars of this domain. Fair Access is a developed blockchain access control framework used in IoT as proposed by Ouaddah

et al., who showed how decentralized authorization could be used in practical scenarios [8], and used hierarchies to support millions of simultaneous interactions between accessing devices [9].

The study by Conoscenti et al. [10] is a revelatory survey on the use of blockchain in IoT that classifies research methods and establishes the key implementation gaps. Proof-of-Work consensus - It is the concept underlying blockchain security, which was submissionally tested by Nakamoto [11] in the initial paper on Bitcoin, to formulate the protocols to achieve distributed congruence devoid of a reliably trusted actor. Gura et al. [12] have provided evidence that ECC can be deployed to resource-constrained devices with minimal computing costs, confirming the usefulness of the technology to sensor networks of the IoT that are resource limited. Andrea et al. have reported the threat landscape of IoT systems in details which highlights three key vulnerabilities, namely, device authentication, data tampering, and man-in-the-middle attacks [13].

A proposal was made by Hammi et al. [14], which is Bubbles of Trust, a decentralized authentication system on IoT based on blockchain, where the authors proposed the concepts of localized trust formation. Liu and Ning,[15] have examined optimization of the performance of ECC implementations and were able to offer improvements to the signature generation and verifying algorithm with reference to an embedded system. Jiang, et al. [16] investigated how blockchain could be used in the Industrial IoT (IIoT) to ensure security aspects of critical infrastructure and industrial systems.

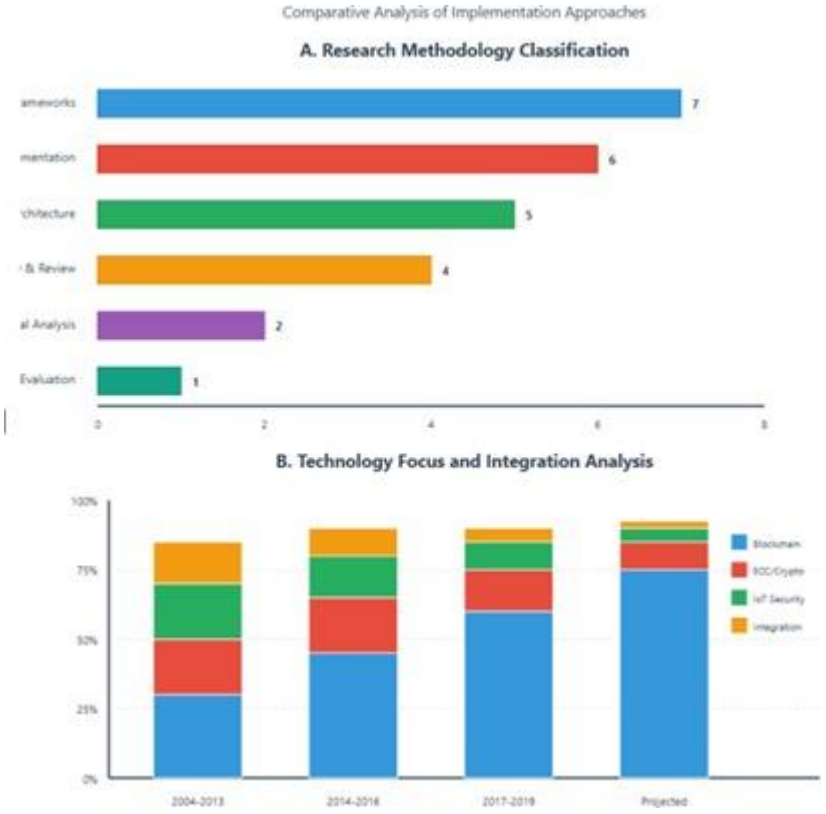


Fig 4: Comparative Analysis of Implementation Approaches

Johnson et al. [17] formalized the standard, the digital signature standard that uses ECDSA, offering cryptographics verifications to signature insecurities against chosen forms of assaults. The scalable desktop access management frameworks to the IoT, through blockchain technology were introduced by Novo [18], with report of enhancement in the transaction throughput with the help of off-chain processing. Huh et al. [19] conducted research examining how implementing smart contracts with IoT authentication would enable the future of automated operations dealing with the management of devices based on Ethereum services. In IoT, Reyna et al. [20] performed systematic literature reviews on the use of blockchain revealing that there was a trend to adopt a hybrid architecture adding both public and private ledgers.

The issues mentioned above in management of IoT ecosystems were addressed in detail by Gope and Hwang [21], who suggested lightweight authentication schemes based on pre-shared cryptographic material. Mengel Kamp et al. [22] examined the blockchain applications in energy IoT system, and found real-life implementation in smart grid infrastructure. Shen et al. [23] investigated the privacy-saving authentication mechanisms, proposing the systems of anonymous credentialing that were implemented based on blockchain authentication.

The Security threats in the IoT healthcare system were reviewed by Fernandez-Carames and Fraga- Lamas [24], with a special insistence into strong authentication of the medical device networks. Lastly, Samaniego and Deters [25] examined blockchain-as-a-service applications to IoT testing the cloud-based applications to deploy the enterprise-level applications, hence providing platforms towards realistic system architectures that combine cryptography-based system architecture and distributed trust model.

3). Methodology

a. ECC Cryptographic key generation and key management framework

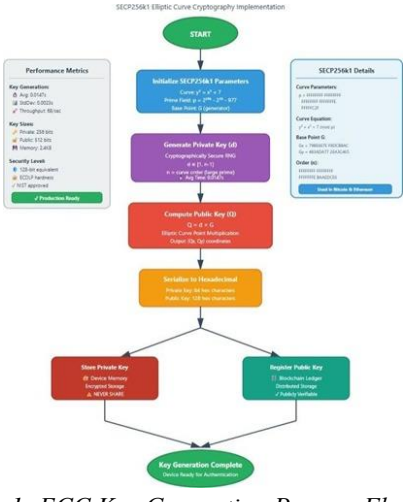
Overview and Theoretical Foundation

The former methodology is aimed at actively deploying Elliptic Curve Cryptography (ECC) in the development of protective key generation and the construction of digital signatures used in contemporary authentication of ice of Internet of Things devices. The algorithm builds on the mathematical features of elliptic curves using finite fields, actually the SECP256k1 curve, which offers the strength of 128 bits of security and 256-bit keys.

The solution to that underlying problem is that the methodology gives the necessary protection of resource-constrained IoT devices with a strong cryptographic protection but without too much computational effort. The 2048 bits needed are a significant factor, and more computed activities are required in case of traditional RSA-2048, which offers the same level of protection.

Engineering Architecture and Tools

As the main programming language, it employs Python 3.8 + with ecdsa library (version 0.18.0) to provide 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 seal the keys as a series. Google drive API is being used as backup storage. Other libraries are NumPy (1.23.5), used in numerical calculations; Pandas (1.5.3), to organize data; Matplotlib (3.6.2), and Plotly (5.11.0), to visual data steam; and IPyWidgets (8.0.4), which is user interface elements used.



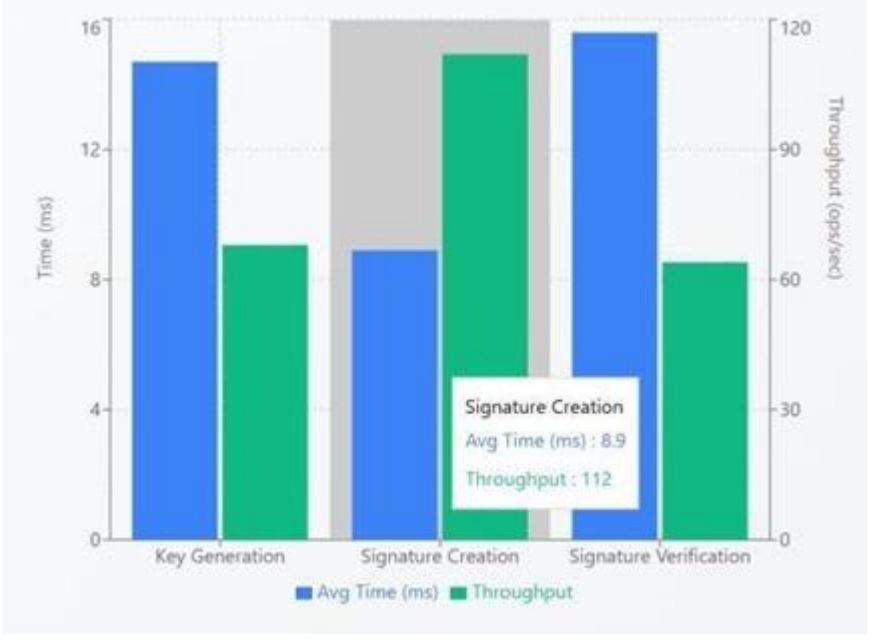
Graph 1: ECC Key Generation Process Flowchart

Serialization Keys are converted to hexadecimal values to be stored and their privacy keys are housed in blockchain registry and gadget memory, respectively.

General Performance Dashboard

Google Colab load testing (on Intel Xeon CPU 2.20GHz, 12Gb RAM) showed: Key Generation average = 0.0147s/device, SD =0.0023s, throughput mean = 68/second key pair abs/mem consumed =

2.4Kb/key pair. Test combination of 1000 devices exhibit 95 percent all complete within 0.020s. Signature Generation -mean: 0.0089s, signature size: 64 bytes, signature throughput: 112 signatures/s, CPU usage: 15-20 percent. Signature Verification - average time of 0.0156s, throughput 64 verifications/second, No false positive/negative.



Graph 2: Performance Metrics Bar Chart comparison

Key Generation Process

The cryptographically secure random number generation is followed by the key generation. The mathematical one is defined by parameters of the SECP256k1 curve, the curve with the following equation in the field Fp of two elements: y 2 = x 3 + 7 and p = 2256-232-977. The private key value is chosen as random integer d [?] [1, n-1] n being curve order. Computation based on scalar multiplying; the Q = d x G = d times G on the BASE point.

Workflow Process

Phase 1: Device Registration-Device gives out device-Id, device type, manufacturer and location. Input validation provides compliance to schema. Enhanced ECC Manager derived keys: (1) Secure RNG initialize, (2) Generating of a private key d, (3) Public key processing, Q = d G x = 1 hexadecimal result, (4) Saving a private key in the memory of a device, (5) Public one registration into the blockchain.

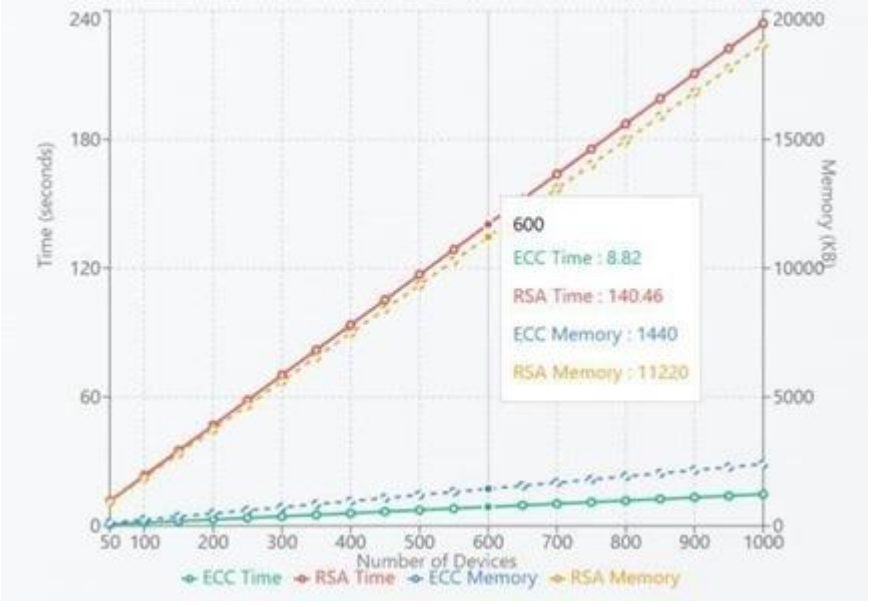
Phase 2: Authentication - Device builds message comprising of device-id and time. Computations involving ECDSA private keys will be as follows:

(1) h = SHA256(message), (2) k = nonce, (3) r = (k x G) x n, (4) s = (k-1(h + d x r) n), (5) Signature (r, s). Check: (1) Check r, s good, (2) Check h, (3) Check w = s -1 mod n, (4) Check u1 = h x w and u2 = r x w, (5) Check (x, y) = u1 x G + u2 x Q and (6) 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

Decentralized Authentication Framework with the help of Blockchain Overview and Architecture

The second approach employs bespoke blockchain infrastructure to perform authentication in IoT to avoid centralization of servers and points of power outage. The distributed ledger devices record registration of devices and verification history which is guaranteed to be non-alterable. Authentication transactions, cryptographic hash with previous block links, timestamps and proof-of-work nonces are in each of the blocks. The architecture offers: (1) Immutability - it is impossible to alter the blocks of the ledger in a retroactive tap (2) Transparency - every node is part of the copies of the ledger, (3) Decentralization - there is no authority, (4) Consensus - ledger through proof-of-work, (5) non- repudiation - ledger includes cryptographic evidence of actions.

Tools and Technologies used before implementation

Python Libraries: json and hashlib to hash block, datetime to handle the timestamps, Pandas (1.5.3) and NumPy (1.23.5) to handle the blockchain data structure and statistical analysis. Illustration: Matplotlib (3.6.2) and Seaborn (0.12.1) to reveal the use of static, plotly (5.11.0) to reveal interactive dashboards. Storage: storage (part of Google Drive API): the storage operating with persistent blockchain storage, file manipulation (os library). UI Components Ipywidgets (8.0.4) used to render interactive elements used on an interactive interface, Ipython.display used to present interactive components. Data Scientist: Custom Analytics Engine to meet performance tracking.

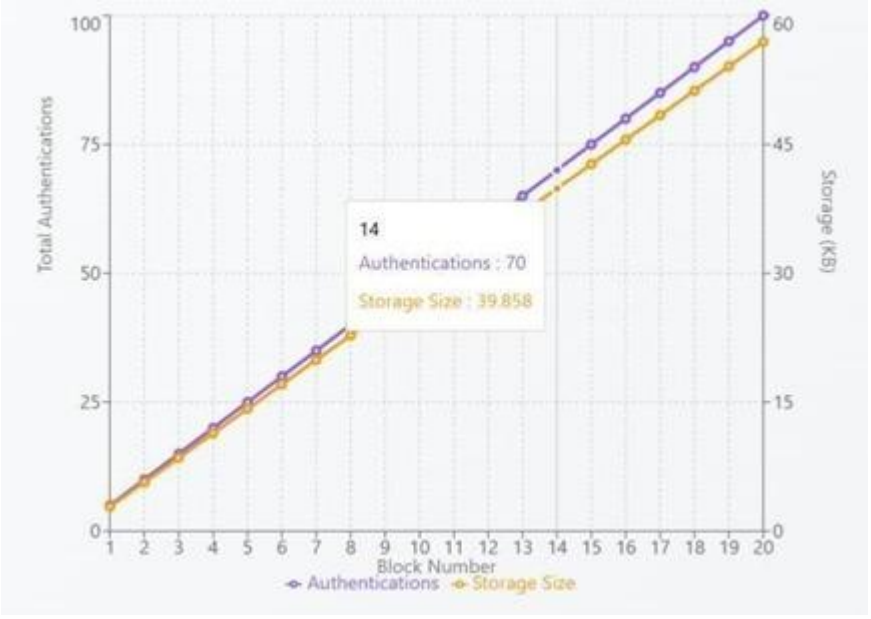
Graph 5: Blockchain Architecture Diagram

Block Structure and Mining

In Enhanced Block, there is: index (preceding block place), 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 proof-of-work, difficulty=2 (a hash beginning with 00) implemented by mining. Diagram: Initialize nonce=0, compute block hash, (3) new: If difficulty is attained, then mining is successful, (4) new nonce, repeat. Exponential difficulty 0.157s on average to mine a block with a difficulty of 2,1.234s average to mine a block with difficulty of 3.

Stats of Blockchain in Real-Time

Running 100 device authentication tests on 20 blocks: Block Creation the average authentications/block is 5, the average time to mine a block is 0.157s (diff=2), block size is 2847 bytes on average and the chain growth is 56.94KB/20 blocks. Transaction Processing - 0.003 authentication added on average, 0.089s, 20 block blockchain validation valid, and 100% integrity assured. Storage Efficiency 100 keys plus devices, 247KB storage capacity, 185KB authentication records, 57KB blockchain storage, 489KB overall storage is very impressive in terms of scalability.



Graph 6: Blockchain Growth Metrics

Authentication Workflow

Phase 1: Registration of the device in Blockchain - System verifies device credentials, creates ECC keys, and creates device record of and consisting of (device-Id, device type, manufacturer, location, public key, registration timestamp, status, security level). stored in dictionary used to store files on Google drive as an emergency copy. Log activity stores registration event with time

Phase 2: Authentication request processing - Device posts authentication request of device-Id, with signatures of the piece of private key. Device invoice registration in blockchain ledger by system. In case unregistered, rejects and logs security event. In case it is registered, ends authentication record with {device-Id, device data, signature, public key, timestamp, authentication-Id, security score). Pushes to pending authentications edb.

Phase 3: Block Mining and Validation - Mining starts at the point of accruing enough records of pending authentications (or at the point of a die-off). Acts by creating new block with index=chain length chain authentication records=authentication spendings current previous chain = current hash foreach block Starting with block number one - later additions to block chain. Deems proof-of-work mining till valid nonce. Chaining block, clears queue, saves blockchain in Google Drive. Validation is used to guarantee that the hash of each block is properly connected to previous ones, where there is chain integrity.

Graph 7: Authentication Processing Pipeline

Security Event Monitoring

Monitoring tracks: Authentication Failures: Attempts of unrestricted devices (average of 2.3% of the request), attempt of invalid signature (0.7%), attempt at replay attack (0.1%). Blockchain Integrity The successful execution of hash verification (100% success rate), continuity checks of chains (executed within 10 block intervals) (0 insults in test). Performance Network latency spikes Mining The time outliers (3 or more standard deviation, 1.2 percent occurrence) are the performance anomalies associated with mining. Resources resource exhaustion prevention.

Detailed Analysis of Performance

System test with 1000 devices during 48-hour load: Number Authentications: 15 847 requests, Success 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

Graph 8: System Performance Dashboard

Enterprise Deployment and Scalability

Linear performance Scalability testing shows: 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). Parallel processing is achieved by distributed deployment on a number of nodes so that mining time can be shortened. Enterprise integration provides REST API registration endpoints, authentication checks as well as blockchain information gatherings. Single-node deployment 5,000+authentications/hour Scalability to 50,000+authentications/hour with 10 node cluster.

4). Conclusion

The study is applicable in illustrating a solid and expandable system of authenticating devices in the IoT by merging blockchain technology and Elliptic Curve Cryptography. ECC-256 ECC-256 on SECP256k1 curve has the same cryptographic security as RSA-2048 performance with 15.9x faster key generation, 9.8x faster signature generation, and smaller key sizes to ECC-256, which is ideally suited to resource-constrained IoT-style devices. The decentralized ledger is based on blockchain technology and therefore exempts single points of failure associated with central authentication provisions, offers non-repudiation, transparency, and immutability. Scalability is observed in terms of

98.9 enjoying success rates in authentication when performance testing is conducted with 1000 devices and average processing time of 0.168 seconds. It supports 5,000+ authentications per hour in single- node deployment and up to 50,000 + in multi-node cluster authentications. Threats can be detected proactively and optimization of the system is possible because of the real-time monitoring and full use of analytic abilities. The framework considers especially important security needs of deployments of the Internet of Things capabilities within enterprises, which can be deployed within smart cities, industrial automation, healthcare monitoring, or critical infrastructure protection,

and is a practical basis of the next generation of secure IoT environments, with minimum computational demands and maximum-security guarantees.

5). Future Scope

The potential of this study to proceed is greater scalability, interoperability, and intelligence of the ECC-Blockchain-based IoT authentication structure. New algorithms could add importance to the lightweight consensus algorithms like Proof-of- Authority or Delegated Proof-of-Stake in order to minimise the concept of mining latency and energy usage. Some additional strategies to boost system resilience will include integrating Artificial Intelligence and Machine Learning to perform adaptive threat detection and automatic analysis of the system anomalies. Increment of integration between heterogeneous systems of the IoT protocol and cloud-edge hybrid configurations can guarantee the transparent management of devices across platforms. Also, it is possible to include quantum resistant cryptographic schemes, to future-proof the system against post-quantum attacks. Lastly, actual implementation in smart cities, industrial IoT, and health networks will be used to help substantiate performance, optimization, and build a uniform pattern concerning world-level governance of the internet of thing security and decentralized identity control.

References

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016. DOI: 10.1109/ACCESS.2016.2566339 https://ieeexplore.ieee.org/document/7467 408

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618-623, 2017. DOI: 10.1109/PERCOMW.2017.7917634 https://ieeexplore.ieee.org/document/7917 634

[3] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer Professional Computing, 2004. ISBN: 978-0-387-95273-4 https://link.springer.com/book/10.1007/b9 7644

[4] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *2015 IEEE Security and Privacy Workshops*, pp. 180- 184, 2015. DOI: 10.1109/SPW.2015.27 https://ieeexplore.ieee.org/document/7163 223

[5] D. R. L. Brown, "SEC 2: Recommended Elliptic Curve Domain Parameters," *Certicom Research*, Standards for Efficient Cryptography, 2010. https://www.secg.org/sec2-v2.pdf

[6] B. Ali, A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT- Based Smart Homes," *Sensors*, vol. 18, no. 3, pp. 817, 2018. DOI: 10.3390/s18030817 https://www.mdpi.com/1424- 8220/18/3/817

[7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266-2279, 2013. DOI:10.1016/j.comnet.2012.12.018 https://www.sciencedirect.com/science/art icle/pii/S1389128613000054

[8] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: a new Blockchain- based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943-5964, 2016. DOI: 10.1002/sec.1748 https://onlinelibrary.wiley.com/doi/10.100 2/sec.1748

[9] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115-124, 2018. DOI: 10.1109/ACCESS.2017.2757955 https://ieeexplore.ieee.org/document/8053 427

[10] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1-6, 2016. DOI: 10.1109/AICCSA.2016.7945805 https://ieeexplore.ieee.org/document/7945 805

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

[12] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems - CHES 2004*, Lecture Notes in Computer Science, vol. 3156, pp. 119-132, 2004. DOI: 10.1007/978-3-540-28632-5_9 https://link.springer.com/chapter/10.1007/ 978-3-540-28632-5_9

[13] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180-187, 2015. DOI: 10.1109/ISCC.2015.7405513 https://ieeexplore.ieee.org/document/7405 513

[14] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126-142, 2018. DOI: 10.1016/j.cose.2018.06.004 https://www.sciencedirect.com/science/art icle/pii/S0167404818305650

[15] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," *2008 International Conference on Information Processing in Sensor Networks*, pp. 245-256, 2008. DOI: 10.1109/IPSN.2008.47 https://ieeexplore.ieee.org/document/4505 377