Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Secure And Lightweight Authentication Protocols for Devices in Internet of Things

[1] Boddupalli Anvesh Kumar, [2] Dr. V. Bapuji

[1]Research scholar, Bir Tikendrajit University
[2]Research Supervisor, Bir Tikendrajit University

Abstract: The proliferation of Internet of Things (IoT) devices has led to an unprecedented level of connectivity, transforming the way we interact with the digital world. As the IoT ecosystem expands, ensuring the security of communication between devices becomes paramount. This paper presents a comprehensive exploration of secure and lightweight authentication protocols designed specifically for IoT devices. In contrast to traditional authentication methods, IoT devices often operate under resource-constrained environments, with limited processing power, memory, and energy. Consequently, conventional authentication protocols may prove impractical, leading to vulnerabilities that can be exploited by malicious entities. Recognizing this challenge, our research focuses on the development of authentication mechanisms that strike a balance between robust security and minimal resource overhead. The proposed protocols leverage advanced cryptographic techniques to provide a secure foundation for device authentication while mitigating the computational burden on resource-constrained IoT devices. We analyse the strengths and weaknesses of existing authentication protocols and identify opportunities for improvement. Additionally, our research introduces novel approaches that optimize authentication processes, ensuring efficiency without compromising security.

Background:

The Internet of Things (IoT) has ushered in a new era of interconnected devices, enabling seamless communication and automation across various domains, including smart homes, healthcare, industrial processes, and transportation. As the number of IoT devices continues to skyrocket, so does the complexity of managing their security. One critical aspect of IoT security is the authentication of devices, ensuring that only legitimate entities can access and communicate with each other within the IoT ecosystem. Traditional authentication protocols, such as username-password combinations, are often ill-suited for IoT devices due to their resource constraints. Many IoT devices operate on low-power processors with limited memory and energy resources, making it challenging to implement and sustain conventional security measures. Moreover, the sheer scale of IoT deployments introduces new challenges, as the need for efficient and scalable authentication becomes paramount.

In this context, the research on secure and lightweight authentication protocols for IoT devices becomes essential. The goal is to develop authentication mechanisms that can provide a robust security foundation while accounting for the resource limitations inherent in many IoT devices. The inadequacy of existing authentication methods in addressing these challenges necessitates the exploration and development of innovative protocols specifically tailored to the unique characteristics of the IoT environment. Common security threats to IoT devices include unauthorized access, data breaches, and device tampering. Attackers may exploit vulnerabilities in authentication processes to compromise the integrity and confidentiality of data transmitted between IoT devices. Therefore, there is a critical need for authentication protocols that not only resist traditional security threats but are also optimized for the constrained environments typical of IoT deployments. The background of this research involves a thorough examination of existing authentication protocols for IoT devices, identifying their limitations and areas for improvement. It encompasses an understanding of the diverse applications of IoT technology and the security requirements unique to each use case. Additionally, the background delves into cryptographic techniques suitable for resource-constrained devices, aiming to strike a balance between security and efficiency. As the IoT landscape continues to evolve, the development of secure and lightweight authentication protocols becomes a foundational element in ensuring the trustworthiness and resilience of IoT ecosystems. This research builds upon the current state of IoT security, addressing the pressing need for authentication solutions that can safeguard the growing multitude of interconnected devices while respecting their inherent limitations.

Development of WSN towards IoT:

The development of Wireless Sensor Networks (WSN) towards the Internet of Things (IoT) involves the evolution and integration of these two technologies to create a more extensive and interconnected network of devices. Here's a theoretical perspective on the development of WSN towards IoT:

1. WSN Foundation:

- Sensing and Data Collection: WSNs are initially designed for sensing and collecting data from the physical world. Sensor nodes are deployed to monitor various environmental parameters such as temperature, humidity, light, and more.
- Limited Communication: Traditional WSNs have limited communication capabilities and are often designed for short-range, low-power communication.

2. Integration of WSN with IoT:

- Communication Protocols: As WSNs evolve towards IoT, there is a need for standardized communication protocols that enable seamless integration. Protocols like MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) are commonly used for efficient data exchange.
- Interoperability: IoT emphasizes interoperability among devices and systems. WSNs need to adapt to standardized communication interfaces, allowing them to seamlessly integrate with other IoT devices and platforms.

3. Scalability and Heterogeneity:

- Scalability: WSNs often deal with a limited number of nodes. In the transition to IoT, the network must scale to accommodate a massive number of diverse devices. This requires addressing issues related to network congestion, data routing, and management at scale.
- Heterogeneity: IoT involves a wide range of devices with diverse capabilities. WSNs must evolve to handle the heterogeneity in terms of device types, communication protocols, and data formats.

4. Energy Efficiency:

- Power Management: Energy efficiency is critical for both WSNs and IoT devices. As WSNs transition to IoT, there's a need for more efficient power management solutions, including low-power modes, energy harvesting, and optimization of communication protocols to extend the lifespan of devices.

5. Security and Privacy:

- Data Security: The integration of WSN with IoT introduces new security challenges. Ensuring the confidentiality, integrity, and authenticity of data becomes more critical. Encryption, secure key exchange, and secure communication protocols are essential components.
- Privacy Concerns: With the increased connectivity and data exchange in IoT, there are growing concerns about privacy. WSNs need to incorporate mechanisms to address privacy issues, such as anonymization of data and user consent management.

6. Edge and Fog Computing:

- Distributed Processing: WSNs traditionally process data at the node level. In the IoT era, there's a shift towards distributed processing, where edge and fog computing are leveraged to perform data processing closer to the data source. This reduces latency and bandwidth requirements.

7. Analytics and Decision Making:

- Data Analytics: WSNs evolve towards supporting more advanced analytics and machine learning algorithms. This allows for real-time analysis of data collected from the sensors, enabling more informed decision-making.
- Autonomous Decision-Making: As WSNs become more integrated into IoT, there is a trend towards autonomous decision-making by devices. This requires sophisticated algorithms and AI models to process data and respond to changing conditions without human intervention.

8. Standardization and Collaboration:

- Open Standards: The development of WSN towards IoT necessitates the establishment of open standards to promote interoperability and collaboration among different vendors and technologies.
- Collaborative Ecosystem: An ecosystem approach involves collaboration among stakeholders, including device manufacturers, software developers, and policymakers, to ensure a cohesive and effective deployment of WSNs within the broader IoT framework.

In summary, the development of WSN towards IoT involves addressing challenges related to communication, scalability, energy efficiency, security, and privacy while leveraging emerging technologies such as edge computing and advanced analytics. The evolution towards IoT signifies a shift from standalone sensor networks to a more interconnected, intelligent, and autonomous network of devices that contribute to a smarter and more efficient world.

Security Threats in Different Layers of IoT:

1. Device/Edge Layer:

- Diversity of Devices: The proliferation of diverse IoT devices introduces challenges in maintaining consistent security measures, leading to potential vulnerabilities.
- Resource Constraints: Many IoT devices operate with limited computational resources, making it challenging to implement robust security mechanisms.

- Physical Vulnerabilities: The physical nature of IoT devices exposes them to physical tampering, adding an extra layer of security concerns.

2. Communication Layer:

- Interoperability Issues: The heterogeneity of communication protocols and standards across IoT devices may result in interoperability issues, creating security loopholes.
- Data Integrity Challenges: Ensuring the integrity of data during transmission becomes complex due to the multitude of communication pathways and potential for data manipulation.
- Wireless Communication Risks: The reliance on wireless communication exposes IoT devices to eavesdropping, unauthorized access, and interference.

3. Network Layer:

- Scalability Concerns: The exponential growth of IoT devices challenges the scalability of network infrastructure, potentially leading to congestion and increased susceptibility to attacks.
- Decentralized Nature: The decentralized nature of IoT networks may introduce difficulties in implementing centralized security measures, requiring distributed and adaptive solutions.
- Dynamic Network Topologies: The dynamic nature of IoT networks, with devices joining and leaving frequently, poses challenges in maintaining stable and secure network topologies.

4. Cloud/Backend Layer:

- Data Privacy Concerns: Centralized storage of IoT data in the cloud raises concerns about data privacy and the potential for unauthorized access, especially given the sensitive nature of some IoT applications.
- Dependency on Service Providers: Reliance on third-party cloud services introduces dependencies and potential security risks associated with the trustworthiness of service providers.
- Insecure APIs: Insecure Application Programming Interfaces (APIs) between IoT devices and the cloud backend may lead to unauthorized access and data breaches.

5. Application Layer:

- Complex Application Ecosystem: The complex ecosystem of IoT applications may result in the integration of insecure or poorly designed applications, exposing vulnerabilities.
- User Authentication Challenges: Ensuring secure user authentication mechanisms becomes crucial to prevent unauthorized access and misuse of IoT applications.
- Inadequate Software Updates: The timely deployment of security patches and updates for IoT applications may be challenging, leaving devices and systems exposed to known vulnerabilities.

In addressing these theoretical challenges, a comprehensive and multidimensional security strategy is essential, encompassing device-level security, secure communication protocols, robust network architecture, secure cloud practices, and resilient application design.

Security Issues in Perception Layer in IoT:

The security issues in the Perception Layer of the Internet of Things (IoT) can be analysed through various theoretical frameworks. One useful approach is to consider these issues within the broader context of cybersecurity principles. Here's a theoretical overview of the security issues in the Perception Layer of IoT:

1. Confidentiality:

The confidentiality of data in the Perception Layer is crucial to prevent unauthorized access and disclosure of sensitive information. Unauthorized access to sensor data can lead to privacy breaches and misuse of information.

2. Integrity:

Data integrity ensures that sensor data remains accurate and unaltered during transmission and processing. Tampering with sensor data, either through physical attacks or malicious manipulation, can compromise the integrity of information and lead to incorrect decisions.

3. Authentication:

Proper authentication mechanisms are essential to verify the identity of devices and prevent unauthorized access. Lack of strong authentication can result in unauthorized devices gaining access to the Perception Layer, leading to potential data manipulation or disruptions.

4. Authorization:

Authorization mechanisms control access rights and permissions, ensuring that only authorized entities can perform specific actions. Inadequate access controls may allow unauthorized entities to read or modify sensor data, leading to security breaches and compromised system functionality.

5. Availability:

Availability ensures that the Perception Layer and its components are accessible and operational when needed. Denial-of-service attacks or physical tampering can disrupt the availability of sensor data, affecting the overall functionality of the IoT system.

6. Non-repudiation:

Non-repudiation ensures that the origin and authenticity of sensor data can be verified, preventing entities from denying their involvement. Without proper mechanisms for non-repudiation, malicious actors may manipulate sensor data without accountability.

7. Trustworthiness:

Trust in the Perception Layer is critical for the proper functioning of the entire IoT ecosystem. Security vulnerabilities and breaches in the Perception Layer can erode trust in the reliability and accuracy of sensor data.

8. Resilience:

Resilience involves the ability of the Perception Layer to withstand and recover from security incidents. Inadequate resilience measures can result in prolonged disruptions and failures in the Perception Layer, impacting the overall IoT system.

Addressing these security issues in the Perception Layer requires a holistic approach, incorporating encryption, secure communication protocols, regular updates, and ongoing monitoring to ensure the integrity and reliability of sensor data in IoT environments.

Symmetric Key Negotiation with ECC:

Device authentication with symmetric key negotiation using Elliptic Curve Cryptography (ECC) involves several steps to establish a secure communication channel between two devices. Here's a methodical approach to this process:

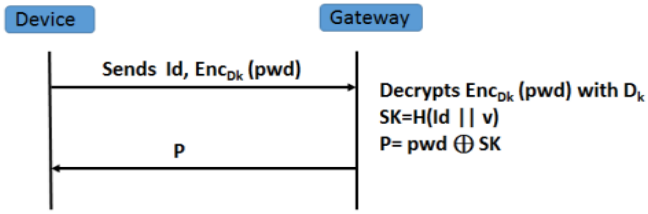

Figure 1: Device Registration Phase

1. Key Pair Generation:

- Each device generates an ECC key pair consisting of a public key and a private key.
- The private key is securely stored on the device, while the public key is shared openly.

2. Key Exchange:

- Devices exchange their public keys securely. This can be facilitated through a secure initial setup or a trusted third party.
- The exchanged public keys are not directly used for encryption but serve as the basis for key derivation.

3. Key Derivation:

- Both devices independently compute a shared secret key using their private key and the received public key.
- The ECC mathematical operations ensure that both devices derive the same shared secret key.

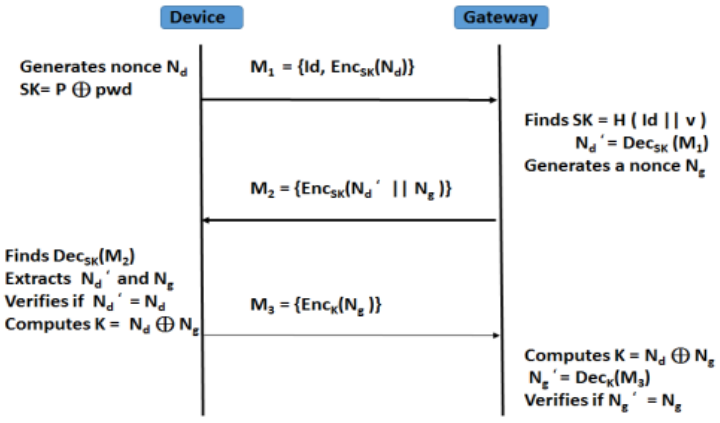

Figure 2: Device Authentication Phase

4. Symmetric Key Negotiation:

- The derived shared secret key is then used for symmetric key negotiation between the two devices.
- This negotiation can involve a secure protocol such as Diffie-Hellman or other key agreement mechanisms.

5. Symmetric Key Storage:

- Once the symmetric key is agreed upon, it is securely stored on each device.

- Care should be taken to protect the key from unauthorized access or exposure.

6. Secure Communication:

- Subsequent communication between the devices is encrypted and decrypted using the agreed symmetric key.
- Symmetric encryption algorithms such as AES (Advanced Encryption Standard) are commonly used for this purpose.

7. Periodic Key Rotation:

- To enhance security, devices can periodically renegotiate and derive new symmetric keys.
- This mitigates the impact of a compromised key and reduces the window of vulnerability.

8. Authentication Tokens:

- Alongside key negotiation, devices can exchange authentication tokens or messages to verify each other's identity.
- These tokens can include digital signatures or other authentication mechanisms.

9. Security Considerations:

- Ensure the security of ECC parameters, including the choice of elliptic curve and key lengths.
- Implement secure key storage mechanisms to protect both the private ECC keys and the derived symmetric key.

10. Monitoring and Anomaly Detection:

- Implement mechanisms for monitoring the authentication process and detecting any anomalous activities.
- This includes identifying failed authentication attempts or unexpected changes in key negotiation patterns.

11. Regular Audits and Updates:

- Conduct regular security audits to assess the overall effectiveness of the authentication process.
- Update ECC parameters, algorithms, and key negotiation protocols based on emerging security standards and best practices.

By following this method, devices can establish a secure and authenticated communication channel using symmetric key negotiation with ECC in the IoT environment. This approach combines the efficiency of symmetric cryptography with the security benefits of ECC, providing a robust solution for device authentication.

Asymmetric Key Negotiation with ECC:

Device authentication using Asymmetric Key Negotiation with Elliptic Curve Cryptography (ECC) involves a process where devices exchange public keys and use them to derive a shared secret key for secure communication.

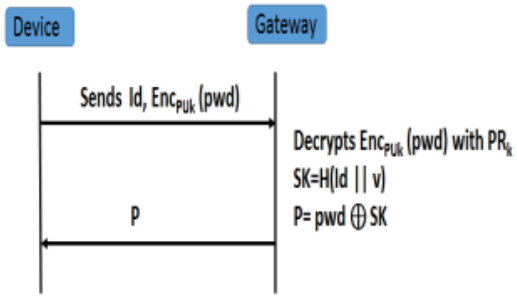

Figure 3: Registration Phase

Here's a methodical approach to this process:

1. Key Pair Generation:

- Each device generates an ECC key pair consisting of a private key and a corresponding public key.
- The private key is securely stored on the device, and the public key is openly shared.

2. Key Exchange:

- Devices exchange their public keys through a secure channel during an initial setup or through a trusted third party.
- This exchange may use a secure protocol, such as TLS/SSL, to ensure the confidentiality of the key transfer.

3. Key Derivation:

- Using their private key and the received public key, each device independently computes a shared secret key using ECC mathematical operations.
- ECC ensures that both devices derive the same shared secret key.

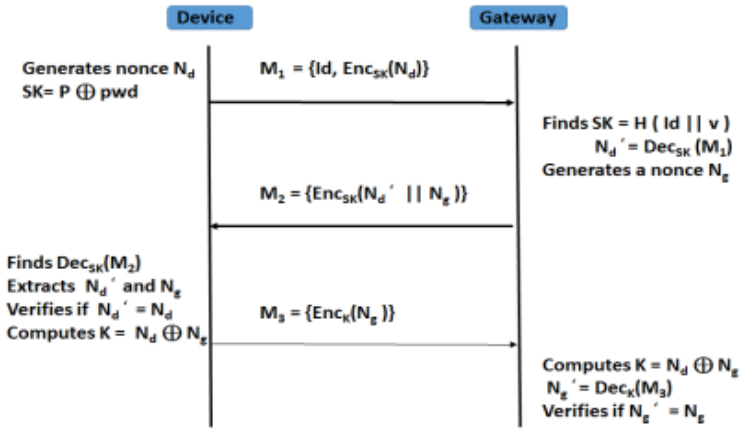

Figure 4: Authentication Phase

4. Asymmetric Key Negotiation:
- The derived shared secret key is used for asymmetric key negotiation between the two devices.
- This may involve a key agreement protocol, such as Diffie-Hellman key exchange, which utilizes the shared secret to establish a common secret without transmitting it.

5. Session Key Generation:
- From the agreed-upon shared secret, devices generate a session key for use in subsequent communication.
- This session key is unique to the ongoing communication session and is used for encrypting and decrypting messages.

6. Secure Communication:
- Subsequent communication between the devices is encrypted and decrypted using the session key derived from the asymmetric key negotiation.
- Symmetric encryption algorithms like AES can be employed for this purpose, providing efficient and secure communication.

7. Authentication Tokens:
- Alongside the key negotiation, devices may exchange authentication tokens or messages to verify each other's identity.
- These tokens may include digital signatures or other authentication mechanisms.

8. Security Considerations:
- Ensure the security of ECC parameters, including the choice of elliptic curve and key lengths.
- Implement secure key storage mechanisms to protect both the private ECC keys and the derived shared secret key.

9. Monitoring and Anomaly Detection:
- Implement mechanisms for monitoring the authentication process and detecting any anomalous activities.
- This includes identifying failed authentication attempts or unexpected changes in key negotiation patterns.

10. Regular Audits and Updates:
- Conduct regular security audits to assess the overall effectiveness of the authentication process.
- Update ECC parameters, algorithms, and key negotiation protocols based on emerging security standards and best practices.

By following this method, devices can establish a secure and authenticated communication channel using asymmetric key negotiation with ECC in the IoT environment. This approach leverages the security benefits of ECC to ensure robust device authentication and secure communication.

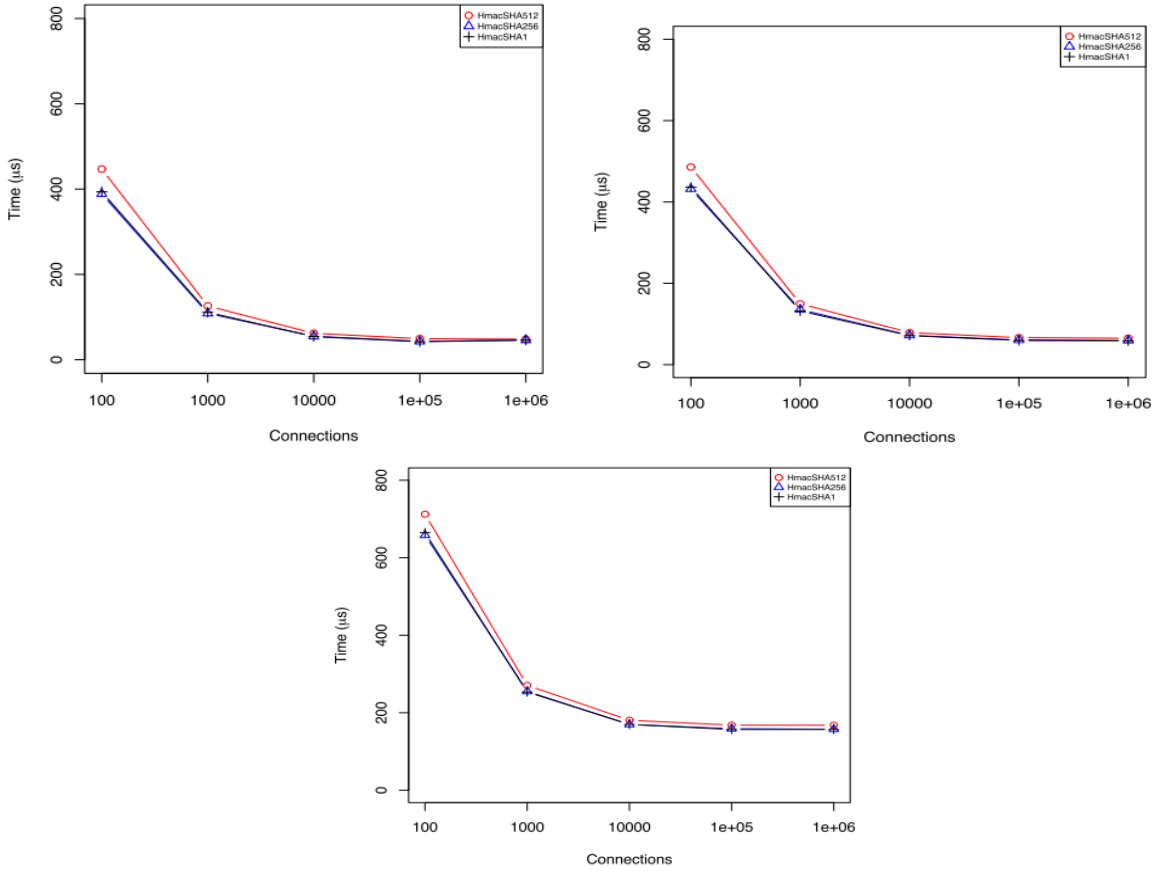

Figure 5: Average OTP generation time - Secp Curves

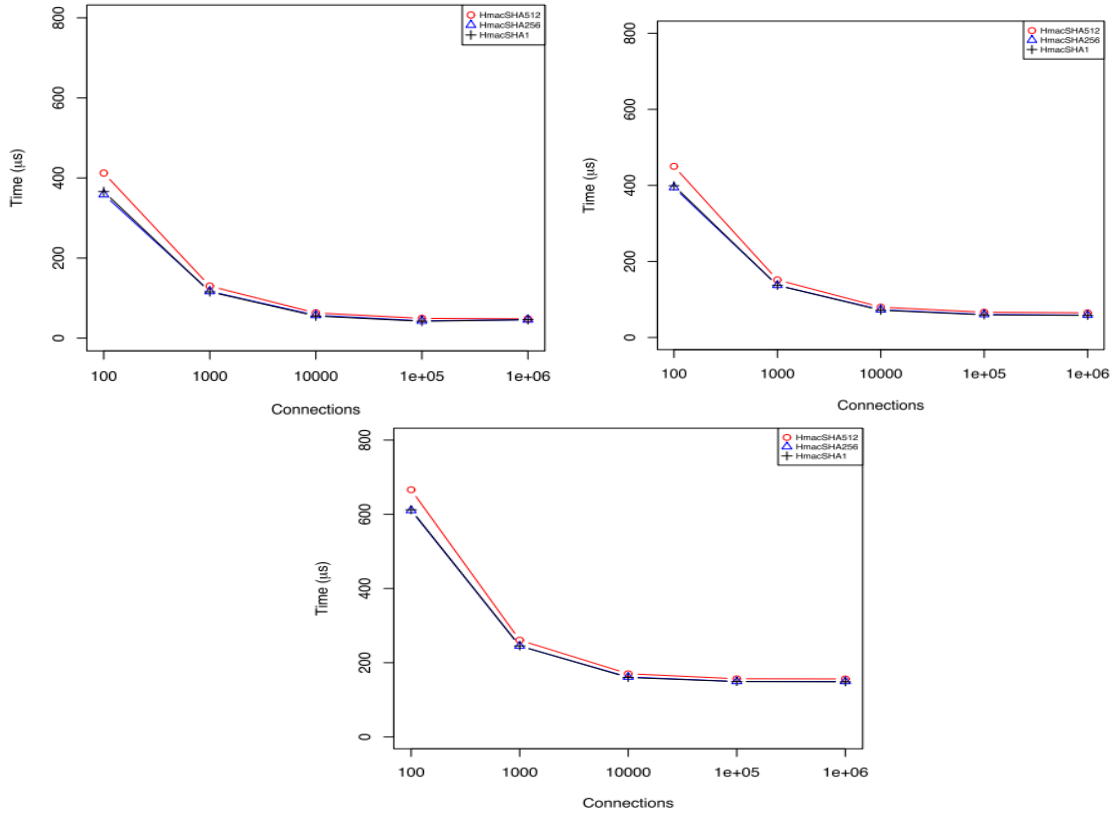

Figure 6: Average OTP generation time – Brain pool Curves

Conclusion:

In conclusion, this research contributes to the ongoing efforts in securing IoT ecosystems by introducing innovative, secure, and lightweight authentication protocols. As IoT continues to permeate various aspects of daily life, the significance of robust security measures cannot be overstated. The protocols presented in this paper provide a foundation for secure authentication, ensuring the integrity and confidentiality of communication in the diverse and dynamic landscape of the Internet of Things.

References:

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013, pp. 663–667.
[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[3] M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7–10, 2008.
[4] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: State of the art," in Robots and Sensor Clouds. Springer, 2016, pp. 55–75.
[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012, pp. 257–260.
[6] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012, pp. 1282–1285.
[7] Y. R. Shi and T. Hou, "Internet of things key technologies and architectures research in information processing," in Applied Mechanics and Materials, vol. 347. Trans Tech Publ, 2013, pp. 2511–2515.
[8] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," Communications Surveys & Tutorials, IEEE, vol. 17, no. 4, pp. 2347–2376, 2015.
[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[10] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[11] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application." IEEE Communications Magazine, vol. 49, no. 11, pp. 68–75, 2011.
[12] M. Yun and B. Yuxin, "Research on the architecture and key technology of internet of things (iot) applied on smart grid," in Advances in Energy Engineering (ICAEE), 2010 International Conference on. IEEE, 2010, pp. 69–72.
[13] H.-E. Lin, R. Zito, and M. Taylor, "A review of travel-time prediction in transport and logistics," in Proceedings of the Eastern Asia Society for transportation studies, vol. 5, 2005, pp. 1433–1448.
[14] L. Coetzee and J. Eksteen, "The internet of things-promise for the future? an introduction," in IST-Africa Conference Proceedings, 2011. IEEE, 2011, pp. 1–9.
[15] M. L. Das, "Privacy and security challenges in internet of things," in Distributed Computing and Internet Technology. Springer, 2015, pp. 33–48.
[16] Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for iot security," in Computing, Networking and Communications (ICNC), 2014 International Conference on. IEEE, 2014, pp. 183–188.
[17] Whitmore, A. Agarwal, and L. Da Xu, "The internet of things a survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.
[18] Yan and G. Huang, "Supply chain information transmission based on RFID and internet of things," in Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on, vol. 4. IEEE, 2009, pp. 166–169.
[19] Sarkar, S. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IOT applications," in Internet of Things (WF-IoT), 2014 IEEE World Forum on. IEEE, 2014, pp. 508–513.
[20] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (IACAC) for the internet of things," Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.