SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I12P109

Volume 10 Issue 12, 87-94, December 2023

Original Article

Secure Communication in Advanced Metering Infrastructure Environment

S. Shabana Banu[1,2*], M.S. Sujatha[3]

[1]*Discipline of EEE, JNTU Ananthapur, Andhra Pradesh, India.*
[2]*Department of EEE, Annamacharya Institute of Technology & Sciences, Andhra Pradesh, India.*
[3]*Department of EEE, MB University, Andhra Pradesh, India.*

[*]*Corresponding Author : shabnam240@gmail.com*

Received: 09 October 2023 Revised: 12 November 2023 Accepted: 10 December 2023 Published: 23 December 2023

Abstract *- Recently, the smart grid has fascinated increasing attraction compared to the conventional methods of power generation with its specific characteristics. Due to its reliability, flexibility and efficiency, the smart grid is predicted to be the future contemporaries' power system all over. Yet there are also significant security issues with smart grids, like confidentiality, message authentication and several security attacks. Therefore, developing an authentication system and a key management protocol has been determined to be one of the most challenging problems in the creation of smart grids. This paper proposes an efficient authentication mechanism using RSA and Elliptic Curve Digital Signature Algorithm (ECDSA). The results were generated with different key sizes for RSA and different standardized elliptic curves for ECDSA.*

Keywords *- Security threats in Advanced Metering Infrastructure (AMI), Authentication mechanism in AMI, Elliptic Curve Digital Signature Algorithm (ECDSA), HES, RSA.*

1. Introduction

Electrical power supplied by utilities must be fed to consumers through transmitting and distributing lines without affecting the quality of power. In addition to providing interruption-free power, there must be a network to convey information from utilities to consumers and vice versa. This is possible by exploring new techniques with a focus on the distribution side. This has paved the way for smart grid electricity networks. In the smart grid, energy and demand are managed by proper communication between utilities and consumers. This way of grid management of demand and protection of the distribution network results in reduced costs with savings in the economy.

It has necessitated increased research on emerging smart grid concepts to strengthen power system architecture. Smart grid architecture is explained in [1], showing the interlink between electric utilities, substations and residential communities, depicting different modes of communication. Display quotations of over 40 words or as needed. Smart meters are used in smart grids for their practical function. 'Advanced Metering Infrastructure (AMI)' provides communication between smart meters and end users in a two-way manner. A sophisticated infrastructurein the smart grid for meter reading offers a path for improvement of load profile and makes data error-free; the problems in the network can also be identified easily. All these result in the fulfilment of AMI's objectives, which include energy audit and, depending on the situation, load curtailment. According to the literature, the different components of AMI are advanced meter devices termed smart meters, communication networks for two-way communication, and data acquisition systems from smart meters and meter data management system for information analysis. The significance of the organization of Internet of Things (IoT) technology in smart grids for economic power transfer is explained in [2]. The reason for increased concern towards smart grid techniques is reduced human intervention. An Artificial Intelligence (AI) model capable of continuously adapting to data changes is proposed in [3] for technology and innovation management with the aim of minimizing manual effort.

A novel technique based on computational intelligence to communicate Transmission Control Centre (TCC) is proposed in [4] using a Remote Terminal Unit (RTU) and Global Positioning System (GPS) for the location of faults in smart grids. A description and analysis of developments in blockchain technology are presented in [5, 24] for a peer-to-peer network and security provided by cryptography-based methods. The main reason for the application of this technology to smart grids is its decentralized nature. Cyber security plays a crucial role in establishing secure smart grids. "Man in the Middle" attack (MITM), denial of services, impersonation attack, etc., which affects computer security

and the process of rerouting is demonstrated in [6]. Many authentication schemes and protocols were proposed, but few are discussed in this paper. There is a need to improve the security that provides efficient communication in the network by using algorithms. This paper proposes an efficient authentication scheme using Elliptic Curve Digital Signature Algorithm (ECDSA) and RSA. The route map of the paper includes section 2, in which the importance of AMI in smart grid is described, section 3 covers security requirements and threats explained section 4 describes the authentication mechanisms thatalready exist and, based on the research gap, an efficient authentication mechanism is proposed andfurther the results are shown.

2. Related Work

Many authors propose several authentication schemes, which are briefly described in this section. Several cyber-incursions like Man in the Middle Attack (MIMA), repetition attacks, DoS, and spoofing against AMI communication affecting authentication mechanisms have already been identified. Without an authentication scheme where the AMI server sends a command to various components based on the same Question Response (QR), any unauthorized entity can corrupt the data, which can lead to AMI instability and even blackout. Several authors have discussed the proposed mechanisms in this regard. A Merkle tree-based authentication scheme, which not only ensures the authentication of the electricity consumption source but also reduces the computation cost of smart meters given by Li et al. [18] developed, the suggested authentication method was contrasted by the authors with the Rivest-Shamir-Adelman (RSA) based authentication strategy with the various numbers of smart meters to demonstrate the scalability of their scheme. However, this scheme involves a lot of storage costs.

A mutual authentication plan and core protocol to protect AMI from cyber-attacks is proposed by Nicanfar et al. [19]. The suggested system uses a password to provide effective and secure shared validation among the AMI server and smart meters, but it is mainly prone to desynchronization [26]. Nabeel et al. [20] projected an effective hardware-based validation strategy for smart meters, which is an efficient key management scheme. This strategy warranties the secrecy and wholeness of messages exchanged and also prevents leakage of secret keys used by smart meters but does not provide AMI authentication. Mohammadali et al. [21] analyzed different AMI security authentication schemes. They projected two authenticated key chord schemes, namely NIKE and NIKE. These schemes are protected against various intrusions such as spoofing, repetition, MITM, and desynchronization intrusion. Yet, these strategies are based on elliptic curve cryptography, which requires multiple multiplications of oblong curve points, which enhances the computational burden. A lightweight mechanism using a hybrid cryptosystem built using the Advanced Encryption Standard (AES)-HMAC-Diffie-Hellman-RSA algorithms was given by Mahmood et al. [22]. The authors employed the RSA algorithm to generate Public-Private Key (PPK) pairs, the AES algorithm to encrypt the information from the SM needed to send to the server-sent application, the HMAC algorithm, and the Diffie-Hellman key exchange algorithm for the standard authentication of stations to obtain message integration. The scheme proposed in [22] extenuates replay attacks by including a timestamp in message transmission, which is assailable to Man in the Middle (MITM) attacks. Also, although its signature time can be obtained using scheduled encryption operations, the signature verification process leads to a lot of time for practical implementation because it involves a decoding procedure that takes 5.18 seconds.

SM Farooq et al. [23] proposed a certificate-based authentication based on ECDSA using key sizes defined by the National Institute of Standards and Technology (NIST). Additionally, The open SSL library has been used to implement a number of ECDSA authentication schemes that use the RSA digital signature scheme. The execution outcomes are equivalenced to determine if they are appropriate for practical usage. To resolve this research gap, this article suggests a strategy conferred in [23] and proposes an ECDSA-based certificate-based authentication with key sizes determined by the National Institute of Standards and Technology (NIST).

3. Advanced Metering Infrastructure

Advanced Metering Infrastructure (AMI) is one of the important building blocks of the smart grid. It is an infrastructure that communicates with other metering devices and measures gathers, transfers, and analyzes energy usage. It enables end users to take part in energy management system contributions and peak load demand reduction. In addition to this, meters also capture, receive and execute remote commands like connecting and disconnecting loads [7].

AMI executes advanced operations in the metering of electricity systems for utilizing smart meters in place of using conventional meters. This function of AMI renders 2-way communication among energy consumers and utility companies, which helps consumers read the meter readings remotely, perform some authorized control, and utilize demand response [8]. AMI enables the following characteristics to the electricity infrastructure in comparison to the conventional metering systems.

1. The power quality and more authentic billing system will be improved.
2. Acquiring new customers is more flexible and can increase daily.
3. The reliable system and security have improved.
4. It has standout features and an appropriate method for connecting the communication backbone to enable energy trading signals and system emergency notifications.

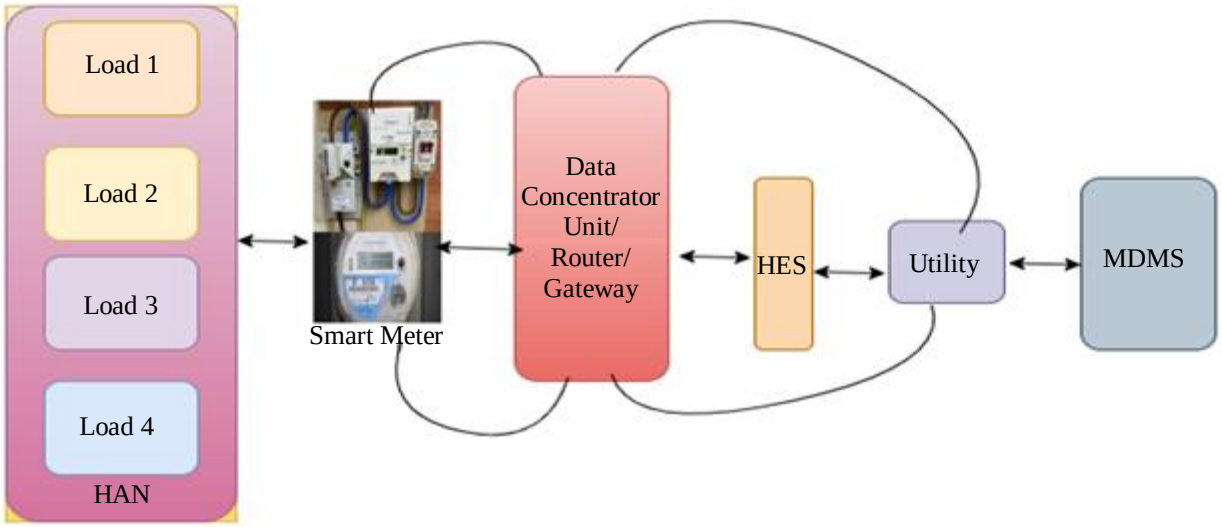

Fig. 1 Typical architecture of AMI

AMI provides financial benefits like reducing the number of equipment equipment maintenance costs, reducing the support budget, quick fixing, shorter delay, and better inventory management [9].

Figure 1 represents the typical architecture of AMI, which consists of smart meters, Data Concentrator Units (DCU), Utility or a Head End System, Meter Data Management System (MDMS) and communication networks like Home Area Network (HAN), Neighbor Area Network (NAN), Wide Area Network (WAN), Field Area Network (FAN) [10].

3.1. Components and Functions of AMI

3.1.1. Smart Meters

Multiple loads can be connected to smart meters, and multiple smart meters can be connected to the data concentrator unit further; the data collected is sent to the utility through the Data Concentrator Unit (DCU) and HES [11].

3.1.2. Data Concentrator Unit

DCU is a smart device that acquires information from a set of smart meters, stores the data, and transfers it into a utility [12].

3.1.3. Head End System

The software which acquires the data flow from a smart meter or utility and sends it to the utility/smart meter, enabling two-way communication so that the data can be validated.

3.1.4. Meter Data Management System

MDMS is the heart of the AMI. A typical MDM system will acquire the data and validate and process the data before the billing analysis. An MDMS can perform long-term information retention and organization for the multiple amounts of data transmitted by smart metering systems. Here, data comprises utilization data and functions that are received from the Head End System (HES) that handles the information aggregation in Advanced Metering Infrastructure (AMI) [13].

3.1.5. Communication in AMI

AMI comprises communication technologies like HAN, FAN/NAN and WAN. The home area network connects the devices within the home. All the smart appliances in a home, including the smart meter connected to the consumer premises, connect with HAN. In Neighborhood Area Network (NAN), also known as a Field Area Network (FAN), multiple smart meters communicate with one DCU. In between the smart meters and the HES, the DCU acts as an intermediary. Through the FAN/NAN, a 2-way communication is provided between the smart meter and HES.

3.1.6. Wide Area Network (WAN)

The connected DCUs with HES are arranged in the Wide Area Network (WAN). Over the WAN, all data from the DCUs is aggregated and transmitted to the HES [14].

3.2. Benefits of AMI

1. AMI helps reduce the time and cost required for the meter data entry.
2. When a meter is read manually, there is a possibility of human errors, which can be reduced with the implementation of AMI, and time is also saved.
3. AT&C losses will be reduced as AMI enables real-time accounting, which reduces electricity theft and improves billing efficiency.
4. It provides better estimation of loads using appropriately in peak and off-peak hours due to which frees the utility from the burden of purchasing costly power in peak hours.
5. It enables faster restoration of electricity service after a fault.
6. For customers disposing of the property as non-paying

clients, under pre-paid agreements and configured event conditions, exceed the sanctioned load; in such case, the utility can connect /disconnect a customer remotely.

7. Power quality data will be acquired from multiple sources to the utility in real-time; it enhances the quality of power in time in case of an occurrence of fault as everything is monitored in- time and reduces the I2R losses [10].

4. Security Issues in Advanced Metering Infrastructure

The most crucial functioning block in the smart grid is AMI. Smart meters record the energy intake and send the data again to the AMI host system for billing and monitoring. In order to carry out the required control actions, it is also in charge of putting control commands and price signals into work.

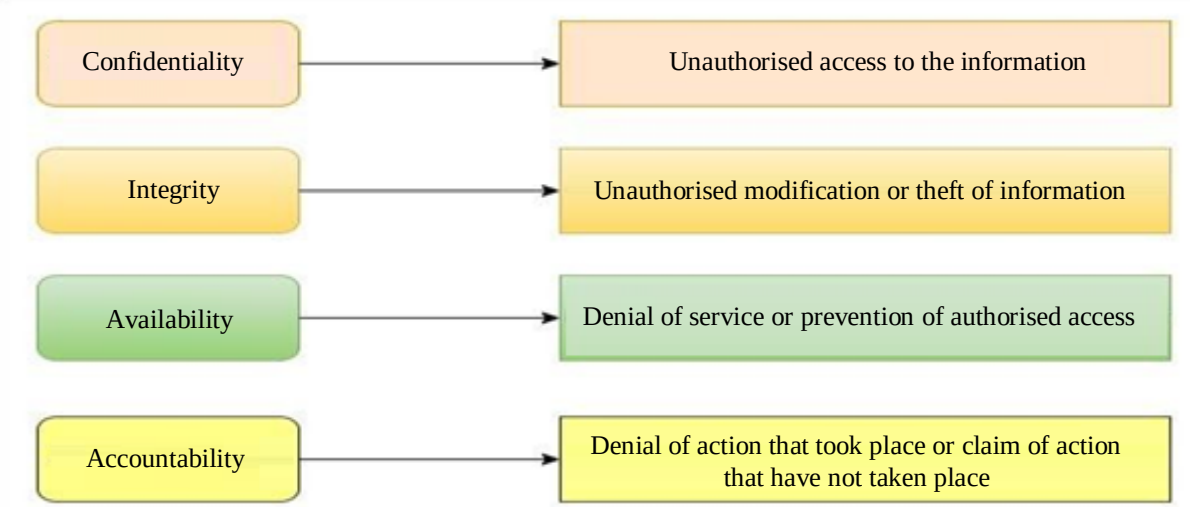

Fig. 2 Security requirements of AMI

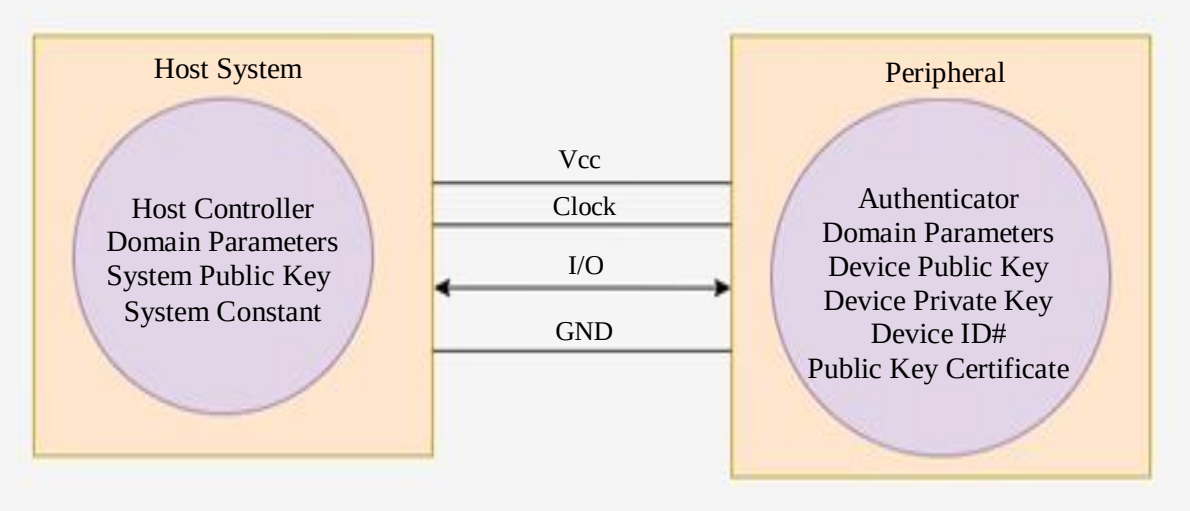

Fig. 3 Hardware configuration of ECDSA authentication system

The introduction of smart meters and the availability of two-way communication are the two most important technical aspects of AMI.As the entire AMI system possesses bilateral communication, every component in AMI is connected to the internet, which is prone to security threats. It deals with AMI's security problems, which are pivotal and critical.

5. Authentication in AMI Communication

The authentication in AMI communication is between the authenticated authority present in the smart grid to deliver the data in the form of packets. There are different variables and functions in the authentication procedure. The other parts used in ECDSA are shown in Table 1.

Table 1. Algorithms and information of functions

Algorithms	Function	Information
Authorized authority	To grand authentication function to FCDSA	AA lists (I)
Smart meter	To measure the quantity of powerconsumed by the device	(IDSMID) Private key (SMP) (Ra, Rb)
RSA	Uses to keys for encrypting	Primary keys (RSAP) (P)
EDCSMA	To provide the efficient using the public keys	Public key (EDCSMA) (Sa, Sb)
Meter data management system	It manages the data from the system	(MDMS)
User device	Smart grid equipments in customer domain	ID SGDP(i)

It provides information on the different types of devices and meters with their functions with the information of the keys used in their function. In the AMI architecture, we have to use RSA with different vital sizes to get the computational time using the standardized curves.

Algorithm 1. Building algorithm for ECDSA with RSA

Input: Smart meter gateway with MDMS

Begin
Read data from smart meter and AA gateway
Provide private key Ra and Rb
Calculate respective public keys Sa and Sb.
Exchange public keys of them.
var - > i of user devices
Communicate with the authenticated receiver
I= (RaSa+ RbSb)
P=i (Sa and Sb)
Compute I and P
Authenticate the keys I and P, verify them with the receiver and store them for future reference.
Accept key only if I= i(P)
End

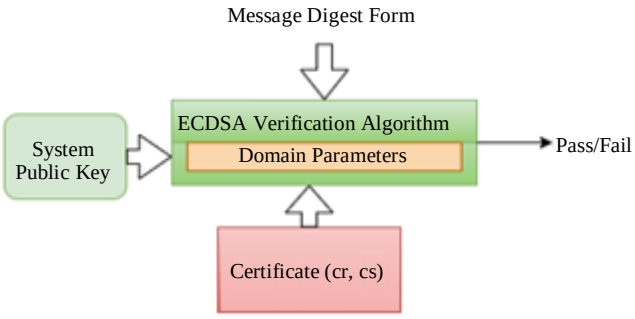

Fig. 4 Verification the authenticator's public key using certificate

In Figure 4, the process shows the verification of the authenticator's public key, which is generated with certificate values Cr and Cs.

6. Results and Comparisons

Authentication can be done using public key cryptography. RSA is a well-accepted general key cryptographic algorithm in the literature.

In the present paper, we have implemented the process of authentication using RSA and Elliptic Curve Digital Signature Algorithm (ECDSA). The results were generated with different key sizes for RSA and different standardized elliptic curves for ECDSA.

Table 2. Key sizes comparison between ECC and RSA

Algorithms /Key Sizes	Computational Time in Milliseconds			
	1024	2048	4096	8192
RSA	7	7	7, 8, 9	8

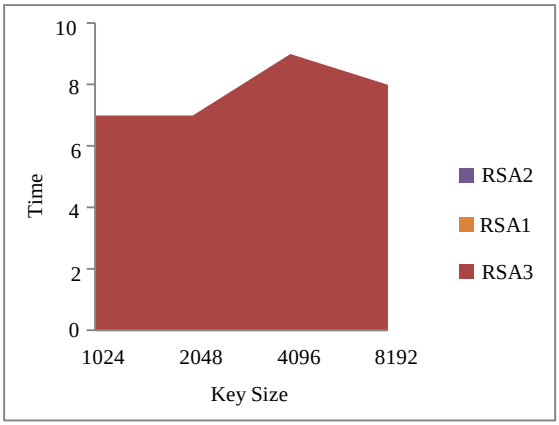

Fig. 5 Comparison of RSA with different key size

From the Table 2, we have compared with respect to the critical sizes of the RSA and the computational time is shown in Figure 5; the y-axis is considered the time in seconds, and the x-axis is regarded as the primary key size.

Table 3 is divided into two more for the easy analysis of the performance of AMI with respect to the RSA and ECDSA (Elliptic Curve Digital Signature Algorithm). It uses the various keys and the algorithms that are used in AMI to provide security in terms of the key sizes.

Table 3. Different standardized curves and their computational time

ASN1 OID	NIST Curve	Public-Key	C-Time(ms)
secp521r1	P-521	512	4, 8
secp128r1		128	9, 4
secp128r2		128	7, 4
secp160k1		161	8, 4
secp160r1		161	8, 4
Secp160r2		161	7, 4
secp192k1		192	8, 4
secp224r1	P-224	224	7, 8
secp256k1		256	8, [4, 8]
secp384r1	P-384	384	9, [4, 8, 12]
secp521r1	P-521	521	9, [4, 8, 12]
prime192v1	P-192	192	9, 4
prime192v2		192	9, [4, 8]
prime192v3		192	8, 4
prime239v1		239	8, [4, 8]
prime239v2		239	5, [4, 8]
prime239v3		239	7, 4
prime256v1	P-256	256	6, [4,8]

As shown in Figure 6, the x-axis is given with the primary key size and the y-axis are given by the different time for the execution of the algorithm in the network.

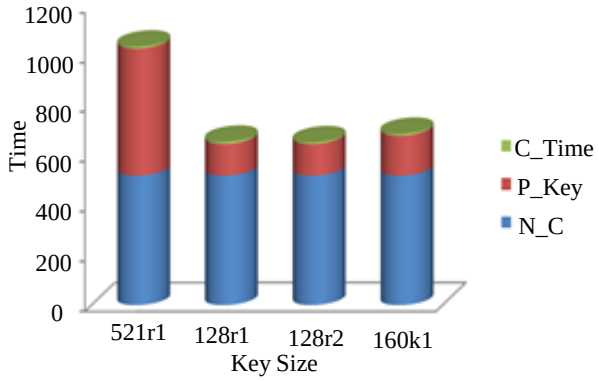

Fig. 6 Comparison of RSA with ECDSA

Table 4. Different standardized curves and their computational time and critical size

ASN1 OID	NIST Curve	Public-Key	C-Time(ms)
sect113r1		113	6, [4, 8]
sect113r2		113	7, [4, 8]
sect131r1		131	6, 4
Sect131r2		131	8, [4, 8]
sect163k1	k-163	163	8, [4, 8]
sect163r1		162	8, [4, 8]
sect163r2	B-163	163	8, 4
sect193r1		193	9, [4, 8, 12]

Table 5. Different standardized curves and their computation values for RSA

ASN1 OID	NIST Curve	Public-Key	C-Time(ms)
sect193r2		193	5, 4
sect233k1	K-233	232	4, [0+4]
sect233r1	B-233	233	9, 8
sect239k1		238	9, [4+4]
sect283k1	K-283	281	10, [4, 8]
sect283r1	B-283	282	18, [4, 8]
sect409k1	K-409	407	14, [4, 8, 12,16]
sect409r1	B-409	409	13, [4, 8, 12,16]
sect571k1	K-571	570	17, [8, 12, 16]
sect571r1	B-571	570	19, [8, 12, 16]
c2pnb163v1		163	8, [4, 8]
c2pnb163v2		162	8, [4, 8]
c2pnb163v3		162	7, [4, 8]
c2pnb176v1		161	8, [4, 8]
c2tnb191v1		191	8, 8
c2tnb191v2		190	8, [8, 9]
c2tnb191v3		189	8, 8
c2pnb208w1		193	9. [8, 9]
c2tnb239v1		238	9, [8, 9, 10]

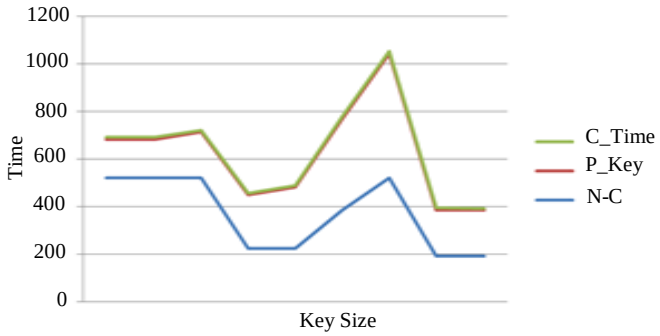

Fig. 7 Comparison of RSA with ECDSA (512 keys)

After the comparison between the RSA and ECDSA with respect to the primary key size; now further, the comparison is done with the increase in the size of the primary key length.

It is shown in Figure 7 comparison of the algorithm with the Primary key (P-key). Authentication can be done using public key cryptography.

Table 6. Different standardized curves and their computation values ECDSA

ASN1 OID	NIST Curve	Public-Key	C-Time(ms)
wap-wsg-idm-ecid-wtls1		112	8, [6, 8]
wap-wsg-idm-ecid-wtls3		163	9, [8, 9]
wap-wsg-idm-ecid-wtls10		232	10, [8, 9, 10]
brainpoolP384r1		384	10, [10,9]
brainpoolP512r1		512	12, [12, 9, 11, 13, 10]
brainpoolP512t1		512	10, [10, 12, 11, 9, 7]

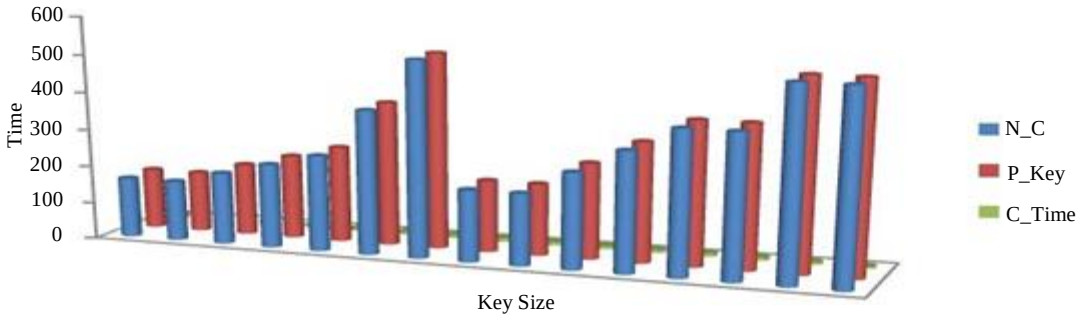

Fig. 8 Comparison of RSA with ECDSA (for all key sizes)

RSA is a well-accepted public key cryptographic algorithm in the literature. In the present paper, we have implemented the process of authentication using RSA and ECDSA (Elliptic Curve Digital Signature Algorithm), shown in Figure 8. The results were generated with different key sizes for RSA and different standardized elliptic curves for ECDSA. The above results help compare earlier authentication of ECDSA results with proposed authentication with key size with respect to the time.

7. Conclusion

AMI faces critical security issues. In this article, it focuses on AMI authentication, which is considered one of the essential security measures. Authentication schemes proposed by different authors are discussed. First, we defined AMI security vulnerabilities, existing authentication mechanisms, how they work, and authentication security vulnerabilities in Smart Grid AMI systems.

Based on the above authentication schemes, an efficient authentication mechanism using RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) is proposed, and the results were generated using different RSA key sizes and different ECDSA standardized elliptic curves. This mechanism can be implemented very securely for authenticating AMI communication systems.

References

[1] Xi Fang et al., "Smart Grid - The New and Improved Power Grid: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944-980, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[2] Martinez Luis, and Philippe Crist, "Urban Mobility System Upgrade - How Shared Self-Driving Cars Could Change City Traffic," *International Transport Forum*, no. 6, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[3] Christian Mühlroth, and Michael Grottke, "Artificial Intelligence in Innovation: How to Spot Emerging Trends and Technologies," *IEEE Transactions on Engineering Management*, vol. 69, no. 2, pp. 493-510, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] M. Jaya Bharata Reddy et al., "Smart Fault Location for Smart Grid Operation Using RTUs and Computational Intelligence Techniques," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1260-1271, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[5] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics*, vol. 36, pp. 55-81, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Muhanna Saed, and Ahamed Aljuhani, "Detection of Man in the Middle Attack Using Machine Learning," *2nd International Conference on Computing and Information Technology (ICCIT)*, pp. 388-393, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] I.S. Jha, Subir Sen, and Vineeta Agarwal, "Advanced Metering Infrastructure Analytics - A Case Study," *Eighteenth National Power Systems Conference (NPSC)*, pp. 1-6, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[8] K.S. Kavithakumari, P. Pravina Paul, and E. Catherine Amala Priya,"Advance Metering Infrastructure for Smart Grid Using GSM," *Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, pp. 619- 622, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hira Naseer, Muhammad Nasir Mumtaz Bhutta, and Mohammed Ali Alojail, "A Key Transport Protocol for Advance Metering Infrastructure (AMI) Based on Public Key Cryptography," *International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1-5, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ramyar Rashed Mohassel et al., "A Survey on Advanced Metering Infrastructure and its Application in Smart Grids," *IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, Toronto, Canada, pp. 1-8, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[11] Gouri R. Barai, Sridhar Krishnan, and Bala Venkatesh, "Smart Metering and Functionalities of Smart Meters in Smart Grid - A Review," *IEEE Electrical Power and Energy Conference (EPEC)*, pp. 138-145, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[12] Basil Hamed, and Mohamed Elhiendi, "Management of Customers Loads on a Transformer Using Data Concentrator Unit," *International Conference on Electric Power Engineering - Palestine (ICEPE- P)*, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ignatius Rendroyoko, Antonius Darma Setiawan, and Suhardi, "Developmentof Meter Data Management System Based-on Event-Driven Streaming Architecture for IoT-Based AMI Implementation," *3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS)*, pp. 403- 407, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Amit Jain, and Hemanth Singabhattu, "Multi-Communication Technology Based AMI for Smart Metering in India," *IEEE 5th International Conference for Convergence in Technology (I2CT)*, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] F.M. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure (AMI)," *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pp. 1-5, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mourad Benmalek, Yacine Challal, and Abdelouahid Derhab, "Authentication for Smart Grid AMI Systems: Threat Models, Solutions, and Challenges," *IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp. 208-213, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ye Yan et al., "An Efficient Security Protocol for Advanced MeteringInfrastructure in Smart Grid," *IEEE Network*, vol. 27, no. 4, pp. 64-71, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[18] Hongwei Li et al.," An Efficient MerkleTree-Based Authentication Scheme for Smart Grid,"*IEEE Systems Journal*, vol. 8, no. 2, pp. 655-663, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[19] Hasen Nicanfar et al., "Efficient Authentication and Key Management Mechanisms for Smart Grid Communications," *IEEE Systems Journal*, vol. 8, no. 2, pp. 629-640, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohamed Nabeel et al.," Scalable End-to-End Security for Advanced Metering Infrastructures," *Information Systems*, vol. 53, pp. 213-223, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[21] Amin Mohammadali et al., "A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2834-2842, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Khalid Mahmood et al., "A Lightweight Message Authentication Scheme for Smart Grid Communications in the Power Sector," *Computers and Electrical Engineering*, vol. 52, pp. 114-124, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[23] Shaik Mullapathi Farooq, S.M. Suhail Hussain, and Taha Selim Ustun, "Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate Based Authentication Scheme for Advanced Metering Infrastructure," *Innovations in Power and Advanced Computing Technologies (i-PACT)*, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[24] S.M. Suhail Hussain, and Shaik Mullapathi Farooq, "Blockchain-Based Security and Privacy Scheme for Smart Meter Communication," *IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT)*, Male, Maldives, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] S.M. Suhail Hussain et al., "An Effective Security Scheme for Attacks on Sample Value Messages in IEC 61850 Automated Substations," *IEEE Open Access Journal of Power and Energy*, vol. 10, pp. 304-315, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Junho Hong et al., "Implementation of Secure Sampled Value (SeSV) Messages in the Substation Automation System," *IEEE Transactions on Power Delivery*, vol. 37, no. 1, pp. 405–414, 2022. [CrossRef] [Google Scholar] [Publisher Link]