www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

Efficient Multi-linear Key Pairing Cryptosystem for Reliable Cloud-based Service Provisioning

Dr. Sabout Nagaraju[1]; S.K.V. Jayakumar[2]; C. Swetha Priya[3]

[1]Assistant Professor, Department of Computer Science, Community College, Central University of Pondicherry, Lawspet, India.

[1]saboutnagaraju1983@gmail.com

[2]Associate Professor, Dept. of Computer Science, School of Engineering & Technology, Pondicherry University, Kalapet, Pondicherry, India.

[2]skvjay.csc@pondiuni.edu.in

[3]S-201, Shri Annai Apartment, 12th Cross, Bharathi Nagar, Lawspet, Pondicherry, India.

[3]swethapriyataru@gmail.com

Abstract

Cloud computing has gained rapid growth in the development of different fields of science and engineering. However, due to the distributed nature of cloud computing, session key generation and establishment is the pressing issue. Session key management plays the utmost important role in the secure exchange of sensitive login credentials and transaction information. Moreover, conventional session key management mechanisms are inadequate and cannot be directly adopted in cloud-based environments. Hence, session key management is very much solely needed solution for reliable cloud-based service provisioning. In mutual authentication, bi-linear key pairing cryptosystem plays a critical role to generate and establish a session key. The existing mutual authentication schemes fail to support true mutual authentication in cloud-based environments as they are vulnerable to secret key leakage, perfect forward secrecy, and untraceability. To mitigate the effect of these attacks, this research develops an efficient multi-linear key pairing cryptosystem. In this cryptosystem, challenge-response messages are used for generating and establishing a one-time shared session key. Furthermore, the performance analysis of the proposed cryptosystem depicts a significant reduction of computation cost, authentication accuracy rates, and resistance to the aforementioned attacks.

Key-words: Bi-linear, Multi-linear, Cryptosystem, Mutual Authentication, Cloud Computing.

1. Introduction

User authentication process plays a vital role in protecting any information communication system from illegal access. Authentication is a secret process to verify the identities of a user for proving their genuineness. Users have many solutions to prove their genuineness. Password-based authentication is a widely-used approach for user authentication. For higher security, a user can use biometrics details (what we are) and/or smart card/ secure token/ secure certificates (what we have) along with user ID and password (what we know) for the authentication. It is observed that usually each and every traditional web or mobile application itself authenticates the users and stores all the credentials information required for the user authentication. The traditional authentication techniques have been widely used in conventional communication systems and working well for a long time. However, for modern-day's communication systems, it could be better to use a combination of two or more techniques which is also called multi-factor authentication (MFA). In fact, traditional authentication techniques cannot be directly adopted in cloud environments due to the openness, distributed, and non-transparent nature of the cloud services (Dewni Weeraman, 2018).

To provide appropriate security in cloud-based communication systems, mutual authentication is a desirable solution. Mutual authentication critically depends on the nature of authentication protocols (e.g., Kerberos) and session key establishment cryptosystems (e.g., Bilinear key pairings). A Public Key Infrastructure (PKI) (Techotopia, 2016) is a powerful back-end cryptosystem for creating, storing, distributing, managing, and revoking the identities and access keys, and to perform mutual authentication. This cryptosystem involves the registration and certificate authorities (for instance, Verisign, COMODO, Symantec, IdenTrust, GlobalSign, DigiCert, and others) also called as trusted third parties to issue valid identity and access keys for the communication entities.

For many conventional communication systems, a centralized trusted third party approach has been used to set up PKI access keys. The Kerberos authentication is a widely-used mechanism in centralized PKI for access keys generation and establishment (C. Neuman et al., 2005). Kerberos allows the clients and servers to authenticate each other by using encrypted tickets. Thus, the Kerberos protocol not only performs the authentication also performs authorization. For user authentication, many operating systems including Windows 2000 and later, UNIX, IBM'S AIX and Z/OS, and others use the Kerberos cryptosystem. Kerberos-based PKI cryptosystem withstands against replay and eavesdropping attacks. However, the Kerberos protocol cannot be applied to the distributed cloud-based environments (Dewni Weeraman, 2018) because it generally works only for trusted/known users and service providers. Moreover, security vulnerabilities exist in Kerberos-based authentication because it is still using DES for data encryption.

Another an extensively-used mechanism for centralized PKI is the SSL/TLS (R. Barnes et al., 2015). SSL/TLS allows the clients and servers to authenticate each other by using ECDH-based session key generation and establishment. Thus, the SSL/TLS approach not only performs secure authentication also safeguards the internet connections. Many applications including voice over IP, instant messaging, email, and other use SSL/TLS-based solutions for secure communications. SSL/TLS-based solutions provide perfect forward secrecy. However, SSL/TLS-based solutions are vulnerable to the man-in-the-middle attack. The centralized-based PKI management approach suffers from the single point of failure which results in whole system failure. One of the notable incidents is WoSign/StartCom bogus HTTPS certifications (L. Tung, 2016). WoSign issued bogus HTTPS certificates for GitHub which led to the failure of whole systems. Mozilla proposed a ban on WoSign/StartCom newly issued certificates for one year. Moreover, most of the centralized PKI authentication solutions require trustee participation, and the trustee could become a bottleneck for user authentication.

Many modern days' communication systems use the distributed PKI mechanism to construct access keys. In this approach, each participating entity mutually generates a random encryption key for accomplishing privacy-preserved mutual authentication. The limitations and vulnerabilities of the centralized PKI solutions can be achieved by using distributed PKI cryptosystem (J. Callas, 2007). The main advantages of the distributed PKI solutions are there is no single point of failure, and the trustee bottleneck problem can be avoided. The OpenPGP authentication is a widely-used mechanism using a distributed public key infrastructure for access keys generation and establishment (Open PGP, 2019). OpenPGP allows the clients and servers to authenticate each other by using the receiver's public key and shared session key. Thus, the OpenPGP approach not only performs the authentication also preserves privacy. Many applications including signature generation, emails, whole disk partition, encryption and decryption of text files, instant messaging, email, and others use OpenPGP-based solutions for secure communications. However, OpenPGP-based solutions are lacking in providing perfect forward secrecy and ubiquity.

Another widely-used mechanism in a distributed PKI is the Bitcoin digital currency system (G. Hurlburt, 2016). Bitcoin mechanism allows the users to broadcast their transactions to other communication entities in the network. Other Bitcoin entities authenticate the user transaction by using a public-ledger also called a blockchain. However, this Bitcoin digital currency system is vulnerable to malicious Bitcoin insiders. Managing identities and access keys in the cloud are an utmost challenging issue. Moreover, traditional PKI solutions are no longer sufficient. AWS Microsoft AD (Peter Pereira, 2017) and Windows Azure Active Directory (AAD) (Jason Wilson, 2018) services are examples of the identity and key management models in the cloud computing environments. These services allow the cloud service consumers to log in to the cloud service based on AD passwords and digital certificates. Cloud-based distributed PKI solutions are more resilient and scalable for consumer identity and key management. However, these solutions are vulnerable to major authentication attacks such as insider threats, Sybil, collusion, and impersonation attacks. Also, use higher computation and communication overhead. As well as it is harder to keep track of all the distributed communication entities.

A. Our Contribution

The main contribution of our research is to develop an efficient multi-linear key pairing cryptosystem for generating and establishing a unique one-time session key. Where in key generation phase, each entity E_i computes intermediate secret and passes it to the next entity along with the previous flow and ends when $E_{i+1} = E_n$. In key establishment phase, intermediate secrets will be sent to the communication entity group to generate a shared session key. Our proposed cryptosystem effectively supports true mutual authentication and mitigates the effect of aforementioned authentication attacks.

B. Paper Organization

Further, this paper is presented as follows. Existing literature is presented in Section 2. Section 3 describes the phases of the multi-linear key pairing cryptosystem. Performance analysis is depicted in Section 4. The significant contribution of this research is summarized in Section 5.

2. Literature Study

This section summarizes the literature study, specifically on mutual authentication and session key management. To bring stronger security in the user authentication, L. Lamport (1981) has investigated a first authentication scheme for insecure networks by using a sequence of hashed passwords. The adversary may impersonate the user or the server by stealing the verifier tables. This scheme is not able to resist the replay and impersonation attacks. To establish improved security in the Lamport authentication scheme, M.S Hwang et al. (2002) have proposed a simple remote user authentication by using smartcard-based hashed password with a secret number. This scheme can able to protect from replay attacks, verifier table is not required, and never reveals the password to the server. However, E.J. Yoon et al. (2005) cryptanalysis proved that M.S Hwang et al. scheme failed to achieve mutual authentication and there is a chance of denial of service attack (DoS) if a secret number or smart card is stolen and also consumes more computation cost. E.J. Yoon et al. (2005)

Received: 06.07.2021 – Accepted: 05.08.2021

have developed a mutual authentication scheme to enhance the security in M.S Hwang et al. scheme. E.J. Yoon et al. scheme can protect DoS, spoofing, impersonation, replay, and forgery attacks and also consumes less computation cost. Liao et al. (2006) improved the M.S Hwang et al. scheme and developed a password-based mutual authentication approach by using hash collision-resistant function and discrete logarithm problem.

To improve security in Liao et al. authentication scheme, M. Kumar et al. (2011) have developed an efficient password-based authentication approach for open networks. However, Y Wang et al. (2015) have pointed out that Liao et al. and Kumar et al. schemes failed to support forward secrecy and perform practically poor performance. Moreover, Kumar et al. scheme has security risks in using static-ID. S.H. Islam et al. (2014) have proposed a dynamic-ID based mutual authentication with different hash collision-resistant functions and new variant elliptic curves (ECs) to achieve the perfect forward secrecy. However, S.H. Islam et al. scheme is vulnerable to impersonation attack as an adversary may intercept the user service request and can trace out the user identities.

S Kumari et al. (2014) have proposed a session key agreement authentication scheme to provide true mutual authentication and cannot resist online password guessing attacks. To establish secure session keys for improving security in mutual authentication using dynamic-IDs, Y.J Shi et al. (2015) have developed a remote user authentication scheme.

However, S Kumari et al. and Y.J Shi et al. schemes cannot be able to support perfect forward secrecy and fail to resist server masquerading and smart card loss attacks. Moreover, Shi et al. scheme fails to support parallel session, impersonation, forgery, DoS, and replay attacks. To achieve secure mutual authentication, V. Odelu et al. (2015) have proposed multi-server biometric-based authentication schemes. However, the schemes are vulnerable to insider threats and consume more expensive computations. S.D Kaul et al. (2016) have established improved security in user authentication to provide true mutual authentication with unique one-time session key agreements'. However, Chen et al. and Kaul et al. schemes cannot be able to support the perfect forward secrecy and are insecure against server masquerading, smart card loss attacks, parallel session, impersonation, forgery, DoS and replay attacks. C.C. Lee et al. (2017) have proposed an anonymous secure authentication scheme to support replay and man-in-the-middle attacks. But Lee et al. scheme failed to resist perfect forward secrecy, impersonation, user anonymity, and offline password guessing attacks. Xu Wu et al. (2018) and Feng Wang et al. (2020) have designed secure authentication schemes to withstand impersonation, secret key leakage, and other known authentication attacks with lightweight computations. However, Xu Wu et al. and Feng Wang et al. (2020) schemes cannot resist the Sybil and collusion attacks. To achieve anonymity-based energy-efficient mutual authentication, Prosanta G et al. (2016) have proposed a lightweight key agreement cryptosystem. However, the scheme is vulnerable to ephemeral secret leakage attack. Debiao et al. (2018) have established improved security in Jia-Lun et al. (2015) scheme to provide true mutual authentication using smartcard-based bilinear cryptosystem. However, Jia-Lun et al. and Debiao et al. schemes cannot be able to support the perfect forward secrecy and are insecure against impersonation, DoS and replay attacks.

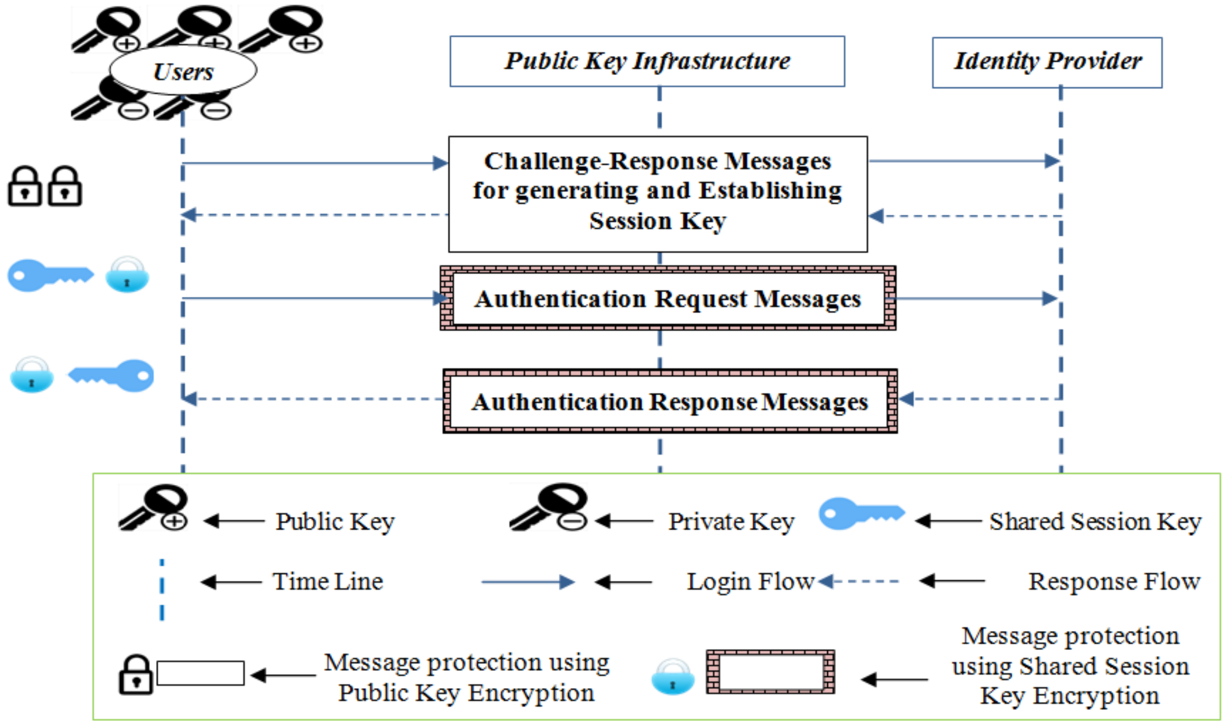
Biometric Cryptography is the next innovation in mobile IoT, financial, retail, healthcare, government, and education sectors for cryptography key generation and establishment (Cai Li et al., 2015). Amioy Kumar et al., (2016) presented a new framework for a bio-cryptosystem in which a cryptographic key is concealed with biometric modalities. Majid Alotaibi (2018) proposed an enhanced biometric-based anonymous user authentication and the key agreement scheme for wireless sensor networks. Nima Karimian et al. (2019) presented a next-generation biometric authentication system in resource-constrained healthcare systems and IoT. The major significances of the biometric cryptosystems are more convenience, high accuracy, and accountability. Xiwei Shan et al. (2021) have proposed biometric-based digital signatures to support secure authentication using bilinear key pairings. However, Amioy Kumar et al., Majid Alotaibi, Karimian et al., and Xiwei Shan et al. schemes failed to resist perfect forward secrecy, impersonation, and user anonymity attacks.

3. Proposed Cryptosystem

The control flow of the proposed cryptosystem is briefed in Figure 1. In this cryptosystem, challenge-response messages which include communication entities ID, random nonce, and intermediate secret key materials are used for generating and establishing one-time shared session keys. Public key infrastructure is used to verify whether the challenging entity is genuine by using public-key cryptography. If so, the identity provider generates a shared one-time session key by using up-flow intermediate secret key materials and gives the response. In the down-flow stage, user and service entities compute a shared session key from the received intermediate secret key materials. By using the newly constructed shared session key, communication entities can establish authentication communication. In Figure 1, dashed lines represent the interaction timelines of the challenge-response and authentication messages.

In this cryptosystem, a unique one-time session key generation and agreement process is divided into three phases as described below:

Figure 1 - Control Flow of the Key Generation and Establishment


Users
Public Key Infrastructure
Identity Provider
Challenge-Response Messages for generating and Establishing Session Key
Authentication Request Messages
Authentication Response Messages
Public Key
Private Key
Shared Session Key
Time Line
Login Flow
Response Flow
Message protection using Public Key Encryption
Message protection using Shared Session Key Encryption

In the **Initialization Phase**, each communication entity needs to choose a common multi-linear key pairing function as defined below.

Definition 1. Let G_1, G_2, G_3... G_n, and G_T represents additive cyclic cryptographic groups with prime order P and their *n*-linear pairing forms $\hat{e}$: $G_1\times G_2\times G_{3\ldots} \times G_n\rightarrow G_T$ that has characteristics as follow:

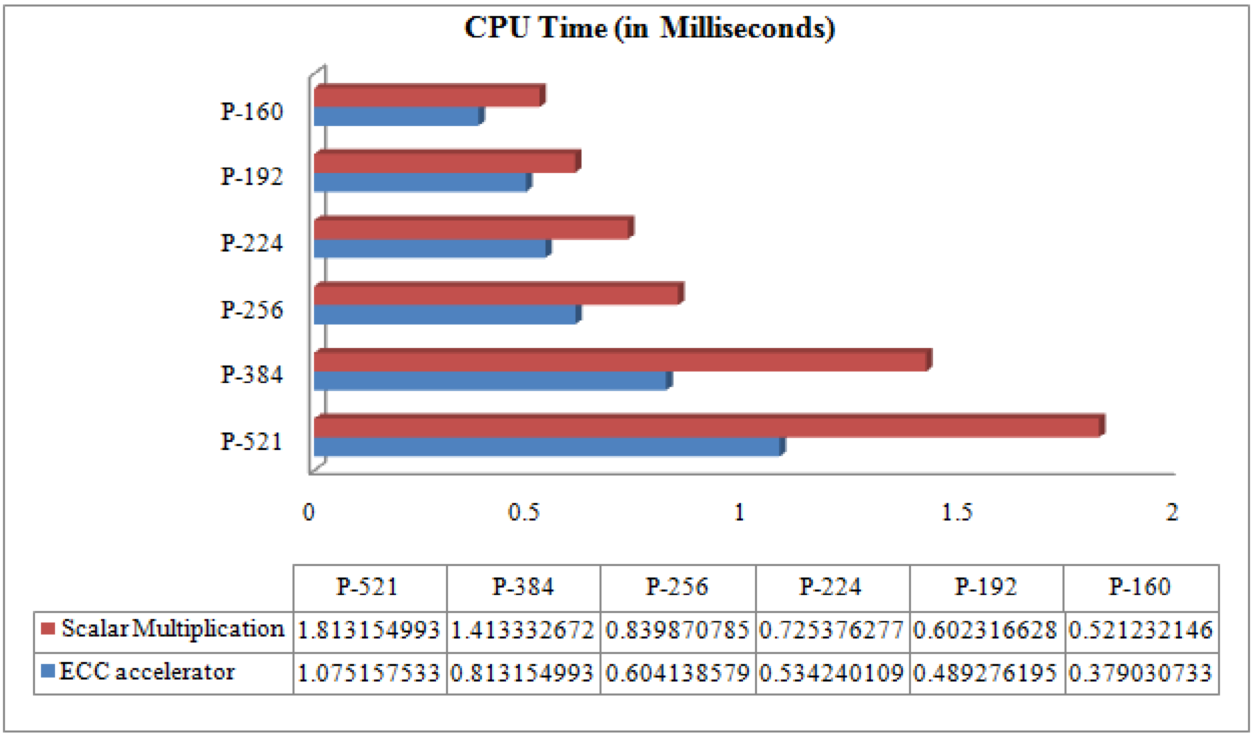
1. Multi-linearity: $\forall a_1, a_2, \ldots, a_n \epsilon F_P^*$, $\forall G\epsilon(G_1, G_2, G_3, \ldots, G_n)$, $\hat{e}(a_1.G_1, a_2.G_2\ldots, a_n. G_n)=\hat{e}(G_1, G_2\ldots, G_n)^{\Pi(a1,\ a2,\ldots,an)}$.
2. Computability: Multi-linear groups and their mapping are computed efficiently.
3. If $\hat{e}(G_1, G_2\ldots, G_n)=1$, then multi-linear pairing preserves a non-degeneracy property.

Definition 2. Let $\hat{e}$ be an Elliptic Curve Diffie-Hellman (ECDH) multi-linear key pairing function on $(G_1, G_2, G_3, \ldots, G_n)for\forall a_1, a_2, \ldots, a_n \epsilon F_P^*$) can be computed as $\hat{e}(a_1.G_1, a_2.G_2\ldots, a_n. G_n) mod\ P=\hat{e}(G_1, G_2, G_3, \ldots, G_n)^{\Pi(a1,\ a2,\ldots,an)}.mod\ P$.

In **Key Generation Phase**, each communication entity E_i chooses a pair $(k_i, Q_i)|i\epsilon(1, n)$, where $k_i\epsilon Zp$ be the random secret and $Q_i = \alpha^{ki}\ mod\ P$ be the common pairing function, where α is an elliptic curve over Zp. In the up-flow stage, each entity E_i performs a single modular exponent and concatenates the result with preceding intermediate values as given in equation (1) and then sends it to E_{i+1}.The control flow of the key generation phase is represented in Figure 2.

$$E_1 \xrightarrow{(\alpha^{k_1},\alpha^{k_1k_2},\dots,\alpha^{k_1k_2\cdots k_i})} E_{i+1} \xrightarrow{(\alpha^{k_1},\alpha^{k_1k_2},\dots,\alpha^{k_1k_2\cdots k_{n-1}})} E_n \qquad (1)$$

Figure 2 - Computation Cost Minimization



	P-521	P-384	P-256	P-224	P-192	P-160
🟥 Scalar Multiplication	1.813154993	1.413332672	0.839870785	0.725376277	0.602316628	0.521232146
🟦 ECC accelerator	1.075157533	0.813154993	0.604138579	0.534240109	0.489276195	0.379030733

In Key Establishment Phase, entity E_n up-on receipt of the up-flow computes the shared session key K by using chosen secret value k_n and is given in equation (2).

$$K = (\alpha^{k_1},\alpha^{k_1k_2},\dots,\alpha^{k_1k_2\cdots k_{n-1}})^{k_n} \; mod\ P \qquad (2)$$

After the up-flow stage, the down-flow starts when $E_{i+1}= E_n$. In the down-flow stage, intermediate secrets will be sent to the communication entity group to generate a shared session key. The down-flow is comprised of *n-1* intermediate values as represented in equation (3).

$$E_1 \xleftarrow{(\alpha^{k_1k_n},\alpha^{k_1k_2k_n},\dots,\alpha^{k_1k_2\cdots k_{n-2}k_n})} E_n \qquad (3)$$

Upon receipt of *n-1* intermediate values, each entity E_i computes the shared session key as given in equation (4).

$$K = (\alpha^{k_1k_2\cdots k_{i-1}k_{i+1}\cdots k_n})^{k_i} \; mod\ P \qquad (4)$$

The down-flow ends when $E_i = E_1$. The multi-linear key pairings cryptosystem is described in Algorithm 1.

Algorithm 1: Multi-linear key pairings Cryptosystem

```
    Initialization: Pair$(k_i, Q_i)|i\epsilon(1, n)$, where $k_i\epsilon Zp$ is a random secret, $Q_i = \alpha^{ki}$ mod $P$, $\alpha$is an elliptic curve over $Zp$.
    Begin
    1. Generation: Each entity $E_i$ computes intermediate secret and passes it to the next entity along with the previous flow and ends when $E_{i+1} = E_n$.
        • i ← 1, Y← Null
        • $Q_i = \alpha^{ki}$ mod P
        • For i ← 2:n-1
            $Y=Y||Q_i$
            $Q_i = (Q_{i-1})^{ki}$ mod P
        • End For
    2. Establishment: Each $E_i|i\epsilon(n, n-1,\ldots 1)$ computes a shared session key and ends when $E_i = E_1$.
        • If $E_{i+1} = = E_n$, then
              $K_n = (\alpha^{k_1}, \alpha^{k_1k_2}, \ldots, \alpha^{k_1k_2\cdots k_{n-1}})^{k_n} \, mod \, p$
        • End If
        • For $i$ ← $n$-$1$:$1$
              $K_i = (\alpha^{k_1k_2\cdots k_{i-1}k_{i+1}\cdots k_n})^{k_i} \, mod \, p$
    End For
    Output: Shared Session Key K
```

4. Performance Analysis

A. Experiment Setup

The current research is evaluated by using Windows Azure Compute and Storage Emulator on C#.NET framework 4.5. This platform helps to develop, test and deploy the proposed cryptosystem on Windows Azure. More than five lakh as represented in equation (3).

$$E_1 \xleftarrow{(\alpha^{k_1k_n}, \alpha^{k_1k_2k_n}, \ldots, \alpha^{k_1k_2\cdots k_{n-2}k_n})} E_n \quad (3)$$

Upon receipt of n-1 intermediate values, each entity E_i sample login records for authentication accuracy analysis are obtained from Google Cloud Trace logs.

B. Efficiency Analysis

The Efficiency analysis of the proposed cryptosystem is analyzed in terms of computational cost reduction, authentication accuracy rates, and resistance to aforementioned authentication attacks. As described in Section 3, a unique one-time session key is generated and established using ECDH multi-linear key pairing function. Expensive modular exponents are used in this key pairing function. The computational costs of the modular exponents are minimized with interleaved modular reduction called double-add reduction (Jorge G. et al., 2006). Modular exponents of the proposed cryptosystem are implemented with an ECC accelerator (Utsav Banerjee, 2017). ECC accelerator is configured in a way to support our proposed key pairing cryptosystem over NIST-recommended elliptic cures (of the form, $y^2 = x^3 + ax + b \bmod P$) (M. Brown et al., 2001). We consider the length of the prime fields is up to 521-bits (≤P-521) and the ECs coefficients are initialized with a=−3 and NIST-recommended values for b to yield fast modular reduction. In the ECC accelerator, the main digital components we used for the reduction of computation cost of the modular exponents are one modular inverter, two logical left shifters, conditional subtraction, three adders, and two multiplexers. All of these components together perform modular exponent operation with a common clock pulse. This makes sure that the proposed multi-linear pairing cryptosystem consumes constant timings for scalar multiplications. The CPU time (in Milliseconds) required for existing Jia-Lun Tsai et al., Prosanta et al., Xu Wu et al., and Debiao He et al. schemes using proposed cryptosystem. In this comparison, we observed that the True Positive and Negative Rates of our authentication scheme are higher than the existing schemes as depicted in Figures 3 and 4. Figure 5 and 6 illustrates the comparison of the False Negative and Positive Rates. Comparison analysis clearly shows that the proposed cryptosystem helps to increase authentication accuracy than the existing schemes for variant (P-521, P-384, P-256, P-224, P-192, and P-160 respectively) ECC-based encryption algorithms.

In our proposed research, true mutual authentication is achieved among the communication entities by mutually verifying each other identities (for instance, ID, a random nonce, and intermediate secret key materials) through asymmetrically protected login/ response messages. So, no adversary is able to forge a legal login or response message. Furthermore, our proposed cryptosystem provides perfect forward secrecy and secret key leakage using a random nonce and unique one-time session key. Based on the proposed session key material generation and establishment, no attacker is able to forge the shared session key. Due to the randomness of *nonce* and session key, the adversary cannot able to produce future login messages with the previously intercepted messages. Moreover, current research helps to withstand impersonation attacks and insider threats. An the scalar multiplications with double-add reduction is illustrated in Figure 2. In addition, we removed redundant and over usage of expensive operations for significant reduction of computation cost of the proposed cryptosystem. This result in more than 65% of reduction in actual computation time required for modular exponents.

Figure 3 - True Positive Rates

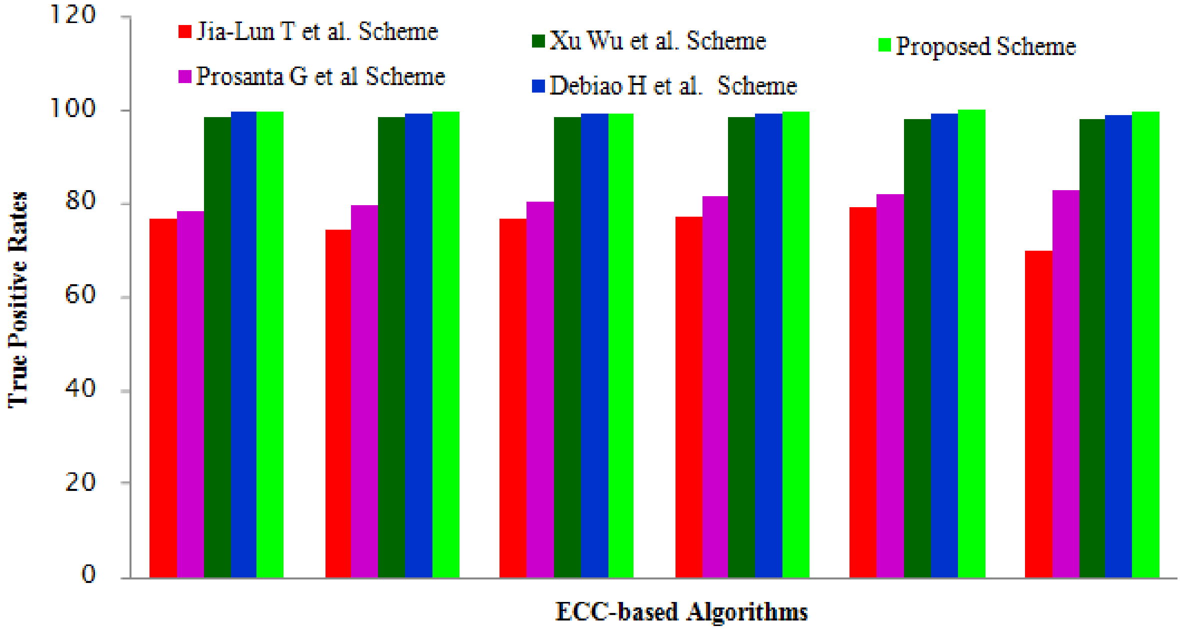


Figure 4 - True Negative Rates

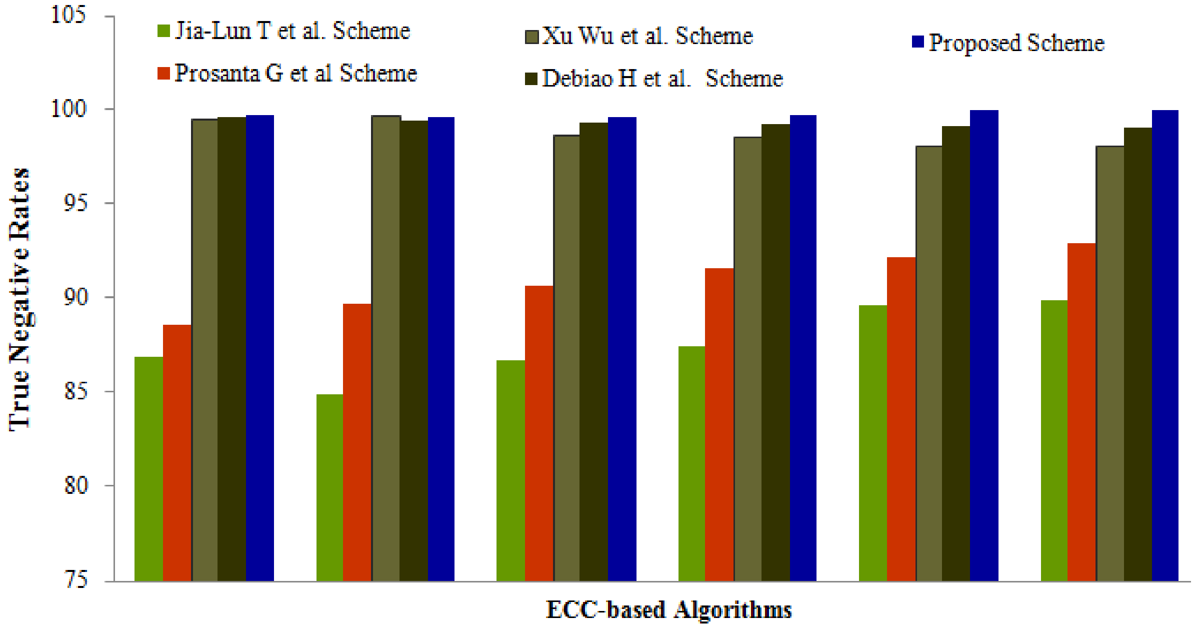


Figure 5 - False Negative Rates

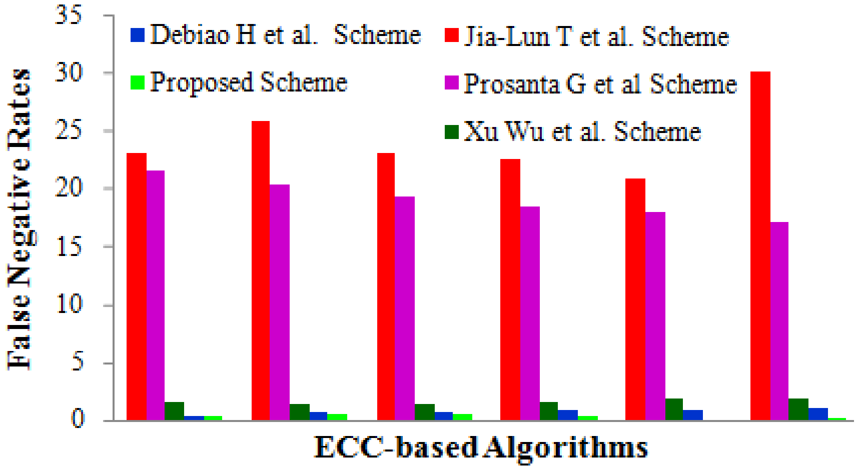
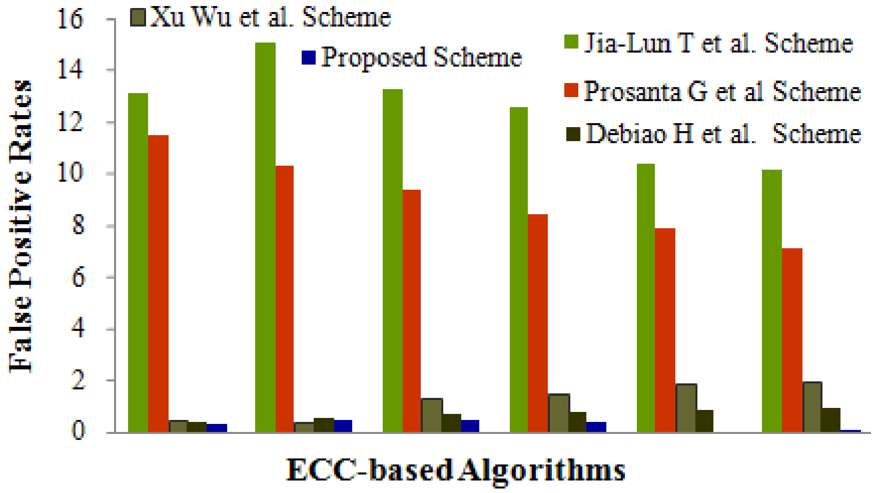


Figure 6 - False Positive Rates



We compared the accuracy parameters of our authentication n scheme (Sabout et al., 2021) with the adversary has no computationally feasible way to guess the login parameters, as well as a random nonce, which will reveal that the login message is replayed. Therefore, the proposed cryptosystem is able to support true mutual authentication and mitigates aforementioned authentication attacks.

5. Conclusion

In this article, a multi-linear key pairing cryptosystem is designed and developed for one-time unique session key generation and establishment. Adoption of this cryptosystem into cloud-based environments provides true mutual authentication among the communication entities. The proposed cryptosystem helps to improve authentication accuracy and withstand aforementioned authentication attacks. Compared to the existing works of literature, the proposed scheme consumes less computation cost and provides higher true positive and negative rates for variant ECC-based encryption algorithms. In the future, our proposed cryptosystem can be extended for IoT-Cloud based digital signatures and key agreements. Furthermore, deep learning analytics can be used to increase the authentication accuracy.

References

Dewni Weeraman (2018), *"Kerberos: The Computer Network Authentication Protocol,"* https://medium.com/@dewni.matheesha/kerberos-the-computer-network-authentication-protocol-a198309339b7.

Techotopia (2016). *"An overview of Public Key Infrastructures (PKI),"* https://www.techotopia.com/index.php/An_Overview_of_Public_Key_Infrastructures_(PKI).

C Neuman, T Yu, S Hartman, K Raeburn (2005), *"The Kerberos network authentication service (V5)",* https://www.hjp.at/doc/rfc/rfc4120.html.

R. Barnes, M. Thomson, A. Pironti, and A. Langley (2015). Deprecating Secure Sockets Layer Version 3.0. *In Internet Engineering Task Force (IETF),* 1-7. https://tools.ietf.org/pdf/rfc7568.pdf

L. Tung (2016), "Mozilla to China's WoSign: We'll kill Firefox trust in you after mis-issued GitHub certs," in ZDNet. [Online]. Available: https://www.zdnet.com/article/mozilla-to-chinas-wosign-well-kill-firefox-trust-in-you-after-mis-issued-github-certs/.

J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer (2007), "OpenPGP Message Format," in Network Working Group, RFC 4880, IETF. https://tools.ietf.org/pdf/rfc4880.pdf.

Open PGP (2019), "Open PGP Encryption," in GO ANYWHERE. https://www.goanywhere. com /managed-file-transfer/encryption/open-pgp

G. Hurlburt (2016), "Might the Blockchain Outlive Bitcoin?" *in IT Professional, 18*(2), 12-16.

Peter Pereira (2017), "Introducing AWS Directory Service for Microsoft Active Directory (Standard Edition)," in AWS Security Blog. https://aws.amazon.com /blogs/security/introducing-aws-directory-service-for-microsoft-active-directory-standard-edition/

Jason Wilson (2018), *"Secure your hybrid-cloud environments with Azure AD Identity Protection and Azure ATP,"* in Microsoft Blog. https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Secure-your-hybrid-cloud-environments-with-Azure-AD-Identity/ba-p/262400.

L. Lamport (1981), "Password authentication with insecure communication," *In Communications of the ACM,* 24(11), 770–772.

M.S Hwang, C.C Lee, and Y.L Tang (2002), "A Simple Remote User Authentication Scheme," *in Mathematical and Computer Modelling,* 36(12), 103-107.

E.J. Yoon, E.K. Ryu and K.Y. Yoo (2005), "An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication Scheme," *in Computers and Security,* 24(1), 50-56.

I.E Liao, C.C Lee, M.S Hwang (2006), "A Password Authentication Scheme over Insecure Network," *In Journal of Computer and System Sciences,* 72(4), 727-740.

M. Kumar, M.K Gupta, and S Kumari (2011), "An Improved Efficient Remote Password Authentication Scheme with Smart Card over Insecure Networks," *In International Journal of Network Security,* 13(3), 167-177.

Y Wang, X Peng (2015), "Cryptanalysis of Two Efficient Password-based Authentication Schemes Using Smart Cards," *In International Journal of Network Security,* 17(6), 728-735.

S.H. Islam and G. Biswas (2014), "Dynamic ID-based remote user mutual authentication scheme with smartcard using elliptic curve cryptography," *In Journal of Electronic Materials.,* 31(5), 473–488.

S Kumari, M.K Khan, and X Li (2014), "An Improved Remote User Authentication Scheme with Key Agreement," *Computers & Electrical Engineering, 40*(6), 1997-2012.

Y.J Shi, H Shen, Y.Y Zhang (2015), "An Improved Anonymous Remote User Authentication Scheme with Key Agreement based on Dynamic Identity," *In International Journal of Security and Its Applications, 9*(5), 255-268.

V. Odelu, A.K. Das, and A. Goswami (2015), "A secure biometrics-based multi-server authentication scheme using smart cards," *In IEEE Transactions on Information Forensics and Security,* 10(9), 1953–1966.

S.D Kaul, & A.K Awasthi (2016). Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement. *In Wireless Personal Communications, 89*(2), 621-637.

C.C. Lee, Y.M. Lai, C.T. Chen, S.D. Chen (2017), "Advanced Secure Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks," *In Wireless Personal Communications, 94*(3), 1281-1296.

Xu Wu, Jin Xu and Binxing Fang (2018), "Lightweight Mutual Authentication Scheme for Protecting Identity in Insecure Environment," *In IEEE China Communications Society,* 15(6), 158 - 168.

Jia-Lun Tsai and Nai-Wei Lo (2015), "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services," *In IEEE Systems Journal,* 9(3), 805-815.

Debiao He, Neeraj Kumar, Muhammad KK, Lina Wang, and Jian Shen (2018), "Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services," *In IEEE Systems Journal,* 12(2), 1621-31.

Prosanta G and Tzonelih Hwang (2016), "Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks," *In IEEE Systems Journal,* 10(4), 1370-1379.

Cai Li, Jiankun Hu, Josef Pieprzyk, and Willy Susilo (2016), "A New Bio-cryptosystem-Oriented Security Analysis Framework and Implementation of Multi-biometric Cryptosystems Based on Decision Level Fusion," *In IEEE Transactions on Information Forensics and Security,* 10(6).

Amioy Kumar, and Ajay Kumar (2016). A Cell-Array-Based Multi-biometric Cryptosystem. *In IEEE Access, 4,* 15-25.

Majid Alotaibi (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN. *In IEEE Access, 6,* 70072-70087.

Nima Karimian (2019). Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT, *In IEEE Access*, 7, 2019, 49135-49149.

Xiwei Shan, Lin You, & Gengran Hu (2021). Two Efficient Constructions for Biometric-Based Signature in Identity-Based Setting Using Bilinear Pairings. *In IEEE Access*, 9, 25973-25983.

Feng Wang (2020). Lightweight Certificate-Based Public/Private Auditing Scheme Based on Bilinear Pairing for Cloud Storage, *In IEEE Access*, 08, 2258- 2271.

Jorge Guajardo, Tim Giineysu, Sandeep S.Kumar, Christof Paar, and Jan Pelzl (2006), "Efficient hardware implementation of finite fields with applications to cryptography," *In Acta Applicandae Mathematica*, 93(1), 75-118.

Utsav Banerjee (2017), "Energy-efficient protocols and hardware architectures for transport layer security," *In Massachusetts Institute of Technology, PhD thesis.*

M. Brown, D. Hankerson, J. Lopez, & A. Menezes (2001). Software implementation of the NIST elliptic curves over prime fields. *In Topics in Cryptology—CT-RSA 2001 (LNCS 2020)*, 338, 250–265.

Sabout Nagaraju, S.K.V. Jayakumar, C Sweth Priya (2021). An Effective Mutual Authentication Scheme for Provisioning Reliable Cloud Computing Services. *In International Conference on Computing, Communication, and Intelligent Systems*, 1-6. 10.1109/ICCCIS51004.2021.9397113

Authors Profile

Dr. Sabout Nagaraju is currently working as an assistant professor at Pondicherry University. He is graduated from G. Pulla Reddy Engineering College, Kurnool, and did his post-graduation at the National Institute of Technology, Calicut. He has obtained his Ph.D. from Pondicherry University, India. His professional experience spans over 13 years in various Engineering colleges and the software industry. His areas of interest include Cloud Computing, the Internet of Things, and AI. He has published fourteen papers in international journals and 3. Eleven papers in national/ international conferences and principal investigator of an ongoing research project.

Dr.S.K.V. Jayakumar is currently working as associate professor in Pondicherry University. He obtained his B.E in Electrical and Electronics Engineering from Madurai Kamaraj University and did his M.E. in Computer Science and Engineering from Madras University. He has obtained his PhD from Pondicherry University. His teaching experience spans over 22 years and his research interest includes Web Services computing and cloud computing. He has published 32 research papers in International Journals and National and International Conferences.

C. Swetha Priya obtained her B.Tech in Computer Science and Engineering from JNTU, Anantapur, and did her M.Tech. in Information Security from Pondicherry University. She has qualified UGC-NET & APSET Assistant Professorships. She has published seven research papers in International Journals and National and International Conferences.