Innovative Digital Signature Paradigm and its Blockchain Applications

Chekkala Gayathri Sai Swarupa [1], Dr. B. S. N Murthy [2]
[1]M Tech Scholar, [2]Professor
[1,2] Department of Computer Science and Engineering
Bonam Venkata Chalamayya Engineering College(A), Odalarevu, Andhra Pradesh, India

Abstract: *This paper introduces an innovative digital signature method called the "expander signature" and explores its Blockchain technology applications. The key advantage of this approach is that a signer can create and manage multiple signatures using a powerful computer, storing expander keys securely. When needed, the signer can release specific expander keys for signature verification, even on resource-limited devices. The paper formally defines the syntax and the security of expander signatures, providing generic constructions from different signature schemes. Importantly, security of expander signatures relies on underlying public key signature schemes, ensuring the signer's secret key remains confidential. This innovation is showcased through an application in blockchain technology.*

Keywords: **Blockchain, Expander signature, public key, secret key, Signature verification**

1. Introduction

Digital signature is the robust cryptographic mechanism to ensure data integrity. In a conventional digital signature scheme, a signer uses their signing key (sk) to sign a message, producing a signature (σ) that can be verified with their public key (pk). Because the signer's signing key (sk) is kept secret, no one can forge a valid signature on their behalf as long as the key (sk) remains uncompromised. The public key (pk) is typically assumed to be publicly accessible, allowing anyone to verify the validity of a generated signature (σ). All digital signature schemes in the literature share a common feature that once the signer publishes a signature (σ), it can be immediately verified using the signer's public key (pk). As a result, these signature schemes fail to meet the requirement of producing a set S of signatures that can be divided into n subsets Si ($1 \leq i \leq n$), with $S1 \subset S2 \subset \cdots \subset Sn \subset S$, where only the signatures in each subset Si can be verified when specific conditions are met over time. This type of digital signature can be considered a fine-grained digital signature. Given that the verification scope of the signature gradually expands over time, we refer to this new signature primitive as an expander signature.

In an expander signature scheme, the signer publishes an expander key (ek) each time they want the related signatures to be verified. Using ek and the signer's public key (pk), these signatures can be verified. As the process evolves, the number of verifiable signatures increases, and the expansion stops once all signatures have been verified.

Expander signatures are specifically needed in certain scenarios. For instance, consider a signer who takes a one-year loan from bank B to purchase a car from company C. The signer signs a purchase contract (ConSC) with C and a 12-month repayment contract (ConSB) with B. ConSB outlines the monthly repayment amounts and the actions to be taken if the signer breaches the contract. Upon the validity of ConSC, bank B transfers the total car payment to company C. Signer generates 12 signatures for the 12 repayment plans in ConSB, but these signatures should only be verified once the signer makes each monthly repayment to bank B. Each month, the signer makes a repayment and releases an expander key (ek). With the signer's public key (pk) and the expander key (ek), anyone can verify the relevant signatures. If all 12 signatures are verified according to ConSB, the signer owns the car. Otherwise, bank B can repossess and auction the car.

Today, many people worldwide purchase items like cars or houses in installments. Recording personal repayments on the blockchain could be beneficial, as the blockchain's openness and unforgeability allow for public verification of individual honesty and trustworthiness. In conjunction with Blockchain, we utilize the InterPlanetary File System(IPFS) to establish a storage system where changes cannot be made by any party without authorization from all others, ensuring there is no single point of failure. IPFS guarantees that data within its network is unique, identified by a unique identifier, and is protected against modifications, thus ensuring immutability. If any data is altered, a new hash identifier is generated, which differs from the one stored in the blockchain for the original data.

Thus, Whenever a signature is validated as legitimate, the transaction is permanently recorded on the blockchain. In scenarios like purchasing a car as above, if the signer fails to transfer funds to bank B or cannot provide a verification token, they face potential financial loss. This underscores the need for a signature scheme that allows verification of only select signatures under specific conditions. Currently, there are no digital signature schemes meeting this requirement, prompting our efforts to address this scalability challenge within blockchain technology in this study. Our construction of the expander signature is versatile, as it seamlessly adapts any conventional signature scheme into an expander signature scheme without compromising security. Furthermore, our additional expander algorithm is efficient, requiring operations solely on a cryptographic collision resistant hash function (such as MD5, SHA256, etc).

2. Literature Review

2.1 Blockchain based Secure Multi signature Scheme for IoV

In the context of Internet of Vehicles (IoV), where real-time traffic data exchange enhances decision-making and reduces accidents, securing communications against passive and active threats is crucial. A Multivariate Multi-Signature Scheme (MV-MSS) is proposed, leveraging the efficiency and post-quantum security of multivariate public key cryptography. MV-MSS allows multiple entities to jointly sign messages with a compact signature, ensuring security against forgery under chosen message and chosen identity attacks, assuming the Multivariate-Quadratic (MQ) problem is NP-hard.

In IoV applications, MV-MSS is integrated where a dynamic cluster head aggregates and signs messages from member vehicles. These signed messages and their multi-signatures are transmitted through Road-Side Units (RSUs) to a blockchain-based cloud server maintained by a Peer-to-Peer (P2P) network. Comparative analysis confirms MV-MSS's efficiency and superior security compared to existing schemes, demonstrating its potential through simulated blockchain implementations for practical deployment in IoV environments.[3]

2.2 Multi security, privacy benchmarking framework

S. Qahtan presents a novel Multi-Criteria Decision Making (MCDM) framework for evaluating and analyzing IoT healthcare systems by integrating Blockchain in Industry 4.0 based on multiple security and privacy properties. It introduces the Spherical Fuzzy Weighted with Zero Inconsistency (S-FWZIC) method, which enhances the original FWZIC by utilizing spherical fuzzy sets to address vagueness, hesitancy, and uncertainty more effectively. The methodology involves creating a decision matrix intersecting IoT healthcare systems and key security/privacy properties, calculating weights through S-FWZIC, and benchmarking systems using a combination of Bald Eagle Search (BES) optimization along with Grey Relational Analysis Technique for Order of Preference by Similarity to Ideal Solution (GRA-TOPSIS). The study finds access control to have the highest significance weight and integrity the lowest. Sensitivity analysis confirms the robustness of the evaluation, providing valuable insights for medical administrators and developers in selecting and designing secure healthcare systems.[7]

2.3 BIoT for smart government and Industry

The price hike or price gouging is an issue all over the world which restricts access to nutritious food and proper treatment. The unauthorized VAT/tax charges and bribery in transportation as key contributors to price hikes. In the article[8] written by M K Hasan, he proposed a solution named blockchain-based Internet of Things (BIoT) model from the perspectives of Industry 4.0 and Blockchain 5.0. This model enables government monitoring of buying and selling activities between buyers and industrial companies to control price hikes and corruption. The system integrates blockchain with a relational database management system using remote database access protocol and cloud servers. The paper outlines the evolution of blockchain and industry generations, concluding with a next-generation blockchain model for an intelligent government to oversee price hikes and corruption.

2.4 Forward-secure PoS blockchain

Forward-secure public-key encryption (PKE) scheme was introduced which actually does not require key updates, making both public and private keys immutable. Unlike prior schemes, which achieve forward security through constant secret key updates, our approach leverages witness encryption (Garg et al., STOC 2013) and a proof-of-stake blockchain with the distinguishable forking property (Goyal et al., TCC 2017). This ensures that a ciphertext cannot be decrypted more than one time, rendering a compromised secret key ineffective for decrypting previously decrypted ciphertexts. We formalize the concept of blockchain-based forward-secure PKE, demonstrate the feasibility of constructing such a scheme without key updates, and explore its implications. The work highlights the potential for enhanced security in PKE systems by maintaining immutable keys and leveraging blockchain technology.[15]

2.5 Smart contract in blockchain

A smart contract is a code snippet that automates pre-agreed contracts between participants, automatically verifying and executing transactions when preset conditions are met. Despite its unique advantages, smart contract technology is still in early development stages and faces several unresolved problems. The article[16] by C. Wu, J. Xiong reviews the recent progress of smart contracts in blockchain technology, starting with a summary of blockchain development and focusing on blockchain 2.0 and smart contracts. Smart contracts are computer programs that automate pre-agreed contracts, executing automatically when preset conditions are met. They are used in financial transactions and various social applications. Despite their advantages, smart contract technology is still in early development stages and faces numerous challenges. The article explains the concepts, mechanisms, and difficulties of smart contracts, proposes solutions to these issues, and analyzes future challenges and development trends in the field.

3. Methodology

Blockchain has inbuilt support for data verification and data security which will not allow stored records to be tampered in any manner and Blockchain will store data at multiple nodes and if one node down then data can be accessed from any other working node in distributed manner.

Above advantage of Blockchain can save both user and bank data while giving EMI options for users. In the proposed work, the user or buyer will sign an EMI contract with required number of tenure for a particular Bank and then generate signatures for all EMI'S and once the user makes payment for a particular month EMI then that month signature from the user will get verified and payment will be marked in bank. If a user misses EMI or performs any fraud then the signature will not get verified and the bank can collect ITEM and go for an auction to recover the loan amount.

In the proposed work Identity Based Verification algorithm with Expander signatures is introduced which allow users to generate signatures prior and can perform verification using any device like laptop, computer or tablet.

Propose work consists of Secret Key Generation and then generating Public Key based on Secret Key and then signed message using secret key and then can perform verification using public key.

All key verification and generation can be performed using Blockchain Smart Contract which contains functions to UPLOAD and VERIFY signatures and this contract can be designed using solidity programming.

3.1 Advantages of Proposed System

1. Signature generation efficiency.
2. Personalized, controlled expander keys.

3. Flexible verification under varied conditions.
4. Resource-friendly verification process.
5. Enhanced security without key exposure.

3.2 System Architecture

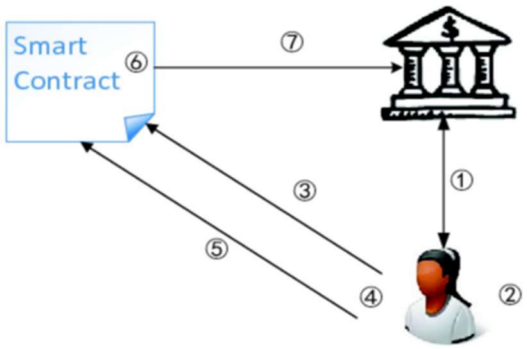


Figure 1. Architecture

1. User Registration: On the homepage, click on the "New User Signup" link to access the signup page. Users complete the signup process by providing necessary details.

2. User Authentication: After successful signup, users log in by clicking on the "User Login" link and entering their credentials. Upon login, users are directed to their dashboard.

3. Loan Application: Users navigate to the "Apply for Loan" section to initiate a loan application. They select the desired EMI tenure, understanding that longer tenures may require more time for signature generation.

4. Loan Details Entry: Users enter the necessary loan details in the provided form on the loan application page. After completing the form, they press the button to generate the signature and also upload them to the blockchain.

5. Signature Generation and Upload: Upon submission, the system generates the required signatures for the selected tenure. Users are informed about the successful generation of signatures and their upload to the blockchain.

6. Payment Verification: Users are provided with options to verify payments or perform other actions related to loan verification. They can access the "Payment Verification using Expander Signature" section to verify payments.

7. Verification Process: In the payment verification section, users can review all loan details retrieved from the blockchain. They initiate the verification process by clicking on the "Click Here to Verify" link.

- **Signature Verification:** The system verifies payment or user authentication using the displayed signature. Users receive confirmation regarding the success or failure of the verification process.
- **Extension:** In the existing system they have worked only on data verification and not concentrate on data security from internal Blockchain employees as they can see the data. So as extension work, we are applying AES encryption on all data so only data owners can decrypt and view the data and other users will not have proper keys to decrypt the data.

To implement this project, we have designed a dummy EMI where users can apply for loans and then generate verification signatures for a selected number of tenures and whenever users pay or click on verification then the system will verify signatures using Blockchain.

3.3 Activity Diagram

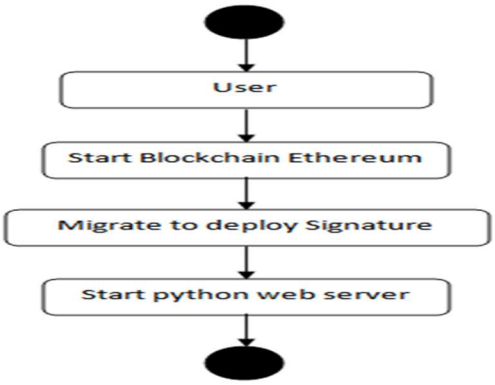
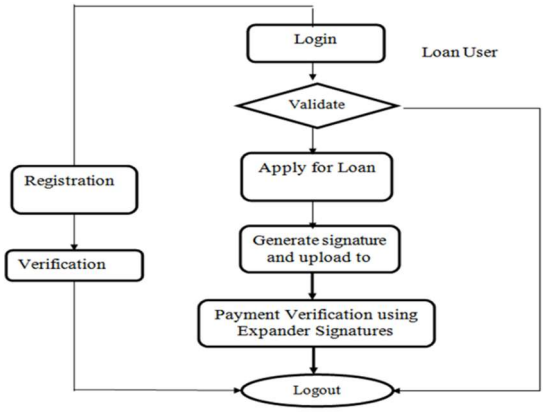


Figure 2. Activity diagram for Backend process

Figure 3. Activity Diagram

The Above Diagram describes the flow for the user. Initially user registration will be done. Once it is successful, the Loan user will login and verification of details is done. Then the loan user will



apply for a loan if he is eligible for it. There the signatures will be generated and during the payment verification is done using the expander signatures.

4. Results and Discussion

Loan users need to register in application and once the registration is successful, Loan users can login to the application.

If a User wants to apply for a loan, click on the “Apply for Loan” action. Fig.4 shows the Loan application page where users need to fill in the requested details like loan amount, EMI tenure time etc and do submit. Based on the number of EMI tenures selected the same number of signatures will be generated and uploaded to blockchain as shown in Figure 5.

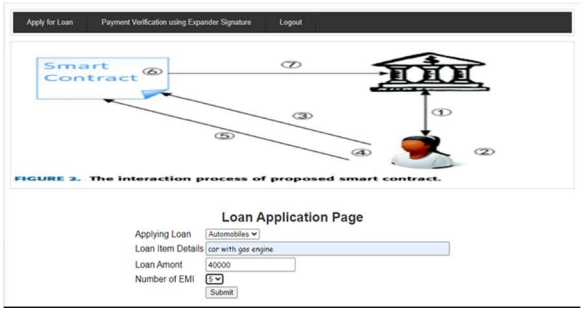


Figure 4. Loan Application Page

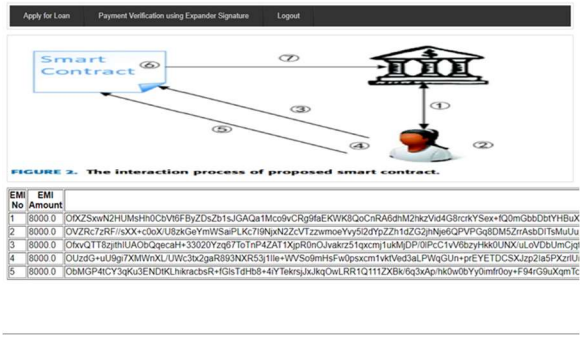


Figure 5. Signature Generation

If a user wants to make payment, they will click on the ‘Payment Verification using Expander Signature’. It contains all the loan details along with the link to verify as shown in Figure 6.

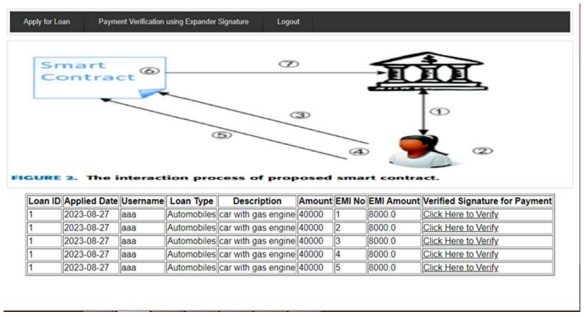


Figure 6. Loan details with signature verification

Click on the “Click Here to Verify” for the respective EMI period to perform verification.

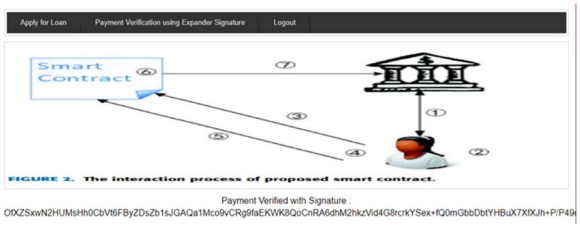


Figure 7. Payment verified with signature

Finally, User Verification and Payment is done successfully using the valid signature. Similarly, you can generate signatures for selected tenure and then can go for verification.

5. Conclusion

This work aim is to enhance the EMI payment system by migrating it to Blockchain with Digital Signatures, ensuring data security and verification integrity. Blockchain's inherent features prevent tampering with stored records, offering distributed data storage for resilience. The proposed Identity-Based Verification algorithm with Expander Signatures enables users to generate and verify signatures across various devices. By implementing AES encryption, the extension enhances data security, allowing only the data owner access. Through a comprehensive system of signature generation, upload to Blockchain, and payment verification, the project ensures authenticity and reliability in EMI transactions, promising a secure and efficient financial ecosystem.

REFERENCES

[1] D. Yu, R.-H. Hsu, J. Lee, and S. Lee, ''EC-SVC: Secure CAN bus in vehicle communications with fine-grained access control based on edge computing,'' IEEE Trans. Inf. Forensics Security, vol. 17, pp. 1388–1403, 2022, doi: 10.1109/TIFS.2022.3152405.

[2] H. N. Noura, O. Salman, R. Couturier, and A. Chehab, ''A single-pass and one-round message authentication encryption for limited IoT devices,'' IEEE Internet Things J., vol. 9, no. 18, pp. 17885–17900, Sep. 2022, doi: 10.1109/JIOT.2022.3161192.

[3] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, ''Blockchain-envisioned provably secure multivariate identity based multi-signature scheme for Internet of Vehicles environment,'' IEEE Trans. Veh. Technol., vol. 71, no. 9, pp. 9853–9867, Sep. 2022, doi: 10.1109/TVT.2022.3176755.

[4] M. Rasori, M. L. Manna, P. Perazzo, and G. Dini, ''A survey on attribute-based encryption schemes suitable for the Internet of Things,'' IEEE Internet Things J., vol. 9, no. 11, pp. 8269–8290, Jun. 2022, doi: 10.1109/JIOT.2022.3154039.

[5] S. Wiefling, P. R. Jørgensen, S. Thunem, and L. L. Iacono, ''Pump up password security! Evaluating and enhancing risk-based authentication on a real-world large-scale online service,'' ACM Trans. Privacy Secur., vol. 26, no. 1, pp. 1–36, Feb. 2023, doi: 10.1145/3546069.

[6] K. Qin, L. Zhou, and A. Gervais, ''Quantifying blockchain extractable value: How dark is the forest?'' in Proc. IEEE Symp. Secur. Privacy (SP), May 2022, pp. 198–214, doi: 10.1109/SP46214.2022.9833734.

[7] S. Qahtan, K. Y. Sharif, A. A. Zaidan, H. A. Alsattar, O. S. Albahri, B. B. Zaidan, H. Zulzalil, M. H. Osman, A. H. Alamoodi, and R. T. Mohammed, ''Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare Industry 4.0 systems,'' IEEE Trans. Ind. Informat., vol. 18, no. 9, pp. 6415–6423, Sep. 2022, doi: 10.1109/TII.2022.3143619.

[8] M. K. Hasan, M. D. Akhtaruzzaman, S. R. Kabir, T. R. Gadekallu, S. Islam, P. Magalingam, R. Hassan, M. Alazab, and M. A. Alazab, ''Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and Industry 4.0,'' IEEE Trans. Ind. Informat., vol. 18, no. 12, pp. 9153–9161, Dec. 2022, doi: 10.1109/TII.2022.3164066.

[9] S. Dziembowski, S. Faust, and K. Hostáková, ''General state channel networks,'' in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2018, pp. 949–966, doi: 10.1145/3243734.3243856.

[10] D. Boneh, B. Lynn, and H. Shacham, ''Short signatures from the Weil pairing,'' in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur., Dec. 2001, pp. 514–532, doi: 10.1007/3-540-45682-1_30.

[11] X. Boyen and B. Waters, ''Compact group signatures without random oracles,'' in Proc. 25th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., St. Petersburg, Russia, May 2006, pp. 427–444, doi: 10.1007/11761679_26.

[12] W. Diffie and M. Hellman, ''New directions in cryptography,'' IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.

[13] M. Bellare and S. K. Miner, ''A forward-secure digital signature scheme,'' in Proc. 19th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 1999, pp. 431–448, doi: 10.1007/3-540-48405-1_28.

[14] H. Jingxin, ''A new forward-secure digital signature scheme,'' in Proc. Int. Workshop Anti-Counterfeiting, Secur. Identificat. (ASID), Kyoto, Japan, Apr. 2007, pp. 116–129, doi: 10.1109/iwasid.2007.373738.

[15] S. Nuta, J. C. N. Schuldt, and T. Nishide, "PoS blockchain-based forward-secure public key encryption with immutable keys and post compromise security guarantees".

[16] C. Wu, J. Xiong, H. Xiong, Y. Zhao, and W. Yi, "A review on recent progress of smart contracts in blockchain".

[17] M. Abdalla, S. K. Miner, and C. Namprempre, ''Forward-secure threshold signature schemes,'' in Proc. Cryptographer's Track RSA Conf., San Francisco, CA, USA, Apr. 2001, pp. 441–456, doi: 10.1007/3-540- 45353-9_32.

[18] G. Itkis and L. Reyzin, ''Forward-secure signatures with optimal signing and verifying,'' in Proc. 21st Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, 2001, pp. 332–354, doi: 10.1007/3-540-44647-8_20.

[19] T. Malkin, D. Micciancio, and S. K. Miner, ''Efficient generic forward secure signatures with an unbounded number of time periods,'' in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., Amsterdam, The Netherlands, Apr. 2002, pp. 400–417, doi: 10.1007/3-540-46035-7_27.