ENHANCING COMMERCIAL BLOCKCHAIN SERVICES WITH IDENTITY-BASED NETWORK SECURITY

Mr. J. U. ARUN KUMAR [1], CH.VENKATA SRIHARI [2]

1 Assistant Professor of MCA, Dept of MCA, Audisankara Institute of Technology (AUTONOMOUS), Gudur (M), Tirupati (Dt), AP

[2]PG Scholar, Dept of MCA, Audisankara Technology (AUTONOMOUS) Gudur (M), Tirupati (Dt), AP

ABSTRACT_ Public IDs of entities are used for cryptographic purposes in Identity-Based Encryption (IBE) schemes. In contrast, we provide a brand-new encryption technique we term Private Identity-Based Encryption, which is based on private identities. A private IBE system ensures that the information used for encryption cannot be obtained by adversaries in order to decrypt data. Furthermore, a user-friendly system may be created to assist people in securing data without storing any secrets privately, all thanks to the usage of identities as secret keys. This makes it possible to maintain keys, which are frequently lengthy and challenging to remember, for decentralized apps.

1.INTRODUCTION

A collection of data that can be utilized to identify an entity is called an identity. There is only one such entity—that is, there aren't two distinct entities with the same identification—if an identity matches an entity. This suggests that each identity is distinct. Identity uniqueness can be utilized as cryptographic scheme keys. Adi Shamir created the Identity-Based Encryption (IBE) technique, which applies this principle to public-key encryption. In this technique, the sender can utilize the receiver's public key, which can be generated based on his identification, to encrypt and send messages to the recipient. To send something to someone, the sender must be aware of their identify, such as their name or email address. The identification in this instance, then. Another issue arises when using that characteristic in secret-key cryptography. Because the keys in secret key cryptography are secret, the identities are as well.

A cryptographically secure pseudorandom number generator is used to produce keys in order to protect the secret; however, since identification information is preset and unchanging, it cannot be employed in the same manner. Because of this, we devise a system that uses a questionnaire to randomly select information from the private identity rather than producing it ourselves. We also suggest security scenarios and demonstrate the security of our method under them, in order to guarantee the safety of the questionnaires. Ultimately, we use our key management strategy to build an application.

2.LITERATURE SURVEY

2.1 Title: "Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography"

Author: M. Abe and S. Fehr.

Description: We present the first distributed discrete-log key generation (DLKG) protocol that does not require interactive zero-knowledge proofs and is adaptively-secure in the non-erasure model. Consequently, in a universally-composable (UC) similar architecture that forbids rewinding, the protocol can be demonstrated to be secure. We establish the security in what we refer to as the single-inconsistent-player UC model, which ensures arbitrary composition under the condition that the same players execute all protocols. We suggest a fully UC threshold Schnorr signature method as an application. Our findings are predicated on a novel Feldman VSS scheme that is adaptively secure.

2.2 Title: "Certificateless Public Key Cryptography. In Advances in Cryptology"

Author: S. S. Al-Riyami and K. G. Paterson.

Description: In order to avoid the inherent escrow of identity-based cryptography and to ensure the authenticity of public keys without the need for certificates, this paper presents and clarifies the concept of certificateless public key cryptography (CL-PKC). A new security model must be carefully developed because there are no certificates and an enemy with access to a master key. Our research focuses on certificateless public key encryption (CL-PKE), and we demonstrate the security of a concrete pairing-based CL-PKE scheme under the condition that an underlying issue that is strongly linked to the Bilinear Diffie-Hellman Problem is hard.

2.3 Title: "Secure Spread: An Integrated Architecture for Secure Group Communication"

Author: Y. Amir, C. Nita-Rotaru, J. R. Stanton, . and G. Tsudik

Description: Group communication systems are high availability distributed systems that offer membership services and dependable, well-organized message delivery to applications that are focused on groups. A distributed client-server design, in which a comparatively small number of servers support a large number of clients, is used in the construction of many such systems. In this study, we demonstrate how security services can be added to group communication systems without compromising their resilience and performance. Specifically, we provide a number of integrated security architectures for group communication systems that are distributed client-server. Unlike a layered architecture, an integrated architecture implements security services in servers.

2.4 Title: "Safeguarding cryptographic keys. In the National Computer Conference"

Author: G. R. Blakley

Description: several cryptographic keys are so crucial that they create a problem. For example, the system master key and several other keys in a DES cryptosystem, 3; or a value that allows one to calculate the secret decoding exponent in an RSA public key cryptosystem, 1. A copy that is disseminated in excess could lead someone astray. Should insufficient copies be produced, they may all be destroyed. Several volatile copies of a crucial key are typically stored in secured memory regions in cryptosystems. If any tampering or probing takes place, these copies will most likely vanish. It is helpful to entrust one or more additional nonvolatile copies because

an adversary would be happy to disrupt the system by causing all of these copies to evaporate.

3.PROPOSED SYSTEM

The public key and private key for certified users in the suggested system will be generated using a private key generator. in order for the users to exchange public keys for identity purposes and for the data to be encrypted using a private key. We put forth security situations and demonstrate the security of our approach in each. Ultimately, we use our key management strategy to build an application. Only the data needed to remind users of the generating procedure is retained in the program; the keys themselves do not need to be kept there.

3.1 IMPLEMENTATION

 Dataset **Collection Module:**

The Private Identity-Based Encryption (PIBE) solution requires data collection from blockchain transactions and user information in order to be constructed and evaluated. Each transaction should have comprehensive information on the sender and recipient addresses, transaction amounts, and timestamps included in the blockchain transactions dataset. This information aids in creating a realistic blockchain testing environment for our encryption approach. Additionally, as they will be mapped to private identities in the PIBE scheme, we need the public IDs and pseudonyms used in transactions. Gathering pertinent metadata can also give the dataset important context, such as block numbers and transaction costs.

 Data **Preprocessing Module:**

Preprocessing is the next stage after data collection to make sure it is clean and prepared for model training. This entails eliminating any superfluous or unnecessary data and confirming the accuracy and coherence of each entry. For instance, we must guarantee that user IDs are appropriately anonymized and that all transaction records are complete. Another crucial stage in preprocessing is normalization. To do this, data formats must be standardized. For example, timestamps must all be converted to the same format. Scaling numerical data to a consistent range is another aspect of normalization that can enhance machine learning algorithm performance. We make sure that our model receives consistent and similar data inputs by normalizing our dataset.

 Training **and Model Building Module:**

Once the data has been preprocessed, we can start training our PIBE model. This involves feeding the blockchain transaction data and corresponding private identities into the model. The model learns to encrypt and decrypt data based on private identities through machine learning techniques. We will divide our dataset into training and validation sets to assess the model's performance. We may use techniques like cross-validation to improve the model's accuracy by training it on multiple subsets of the data to make sure it generalizes well to unseen data. Finally, we will adjust the model's parameters during the training process to maximize its performance.

 Predict **Output Module:**

We can use the model to predict encrypted outputs for fresh input data once it has been trained. This entails feeding fresh transaction data and matching private IDs into the model. After that, the model will provide encrypted outputs, guaranteeing that the data is safe and that only authorized parties will be able to decrypt it. To summarize, the PIBE system implementation process entails gathering extensive user and blockchain transaction data, preprocessing the data to guarantee its quality, training the model with machine learning methods, and utilizing the model to forecast encrypted outputs for new inputs. This method not only makes blockchain services more secure, but it also makes key management easier for users.

4.RESULTS AND DISCUSSION

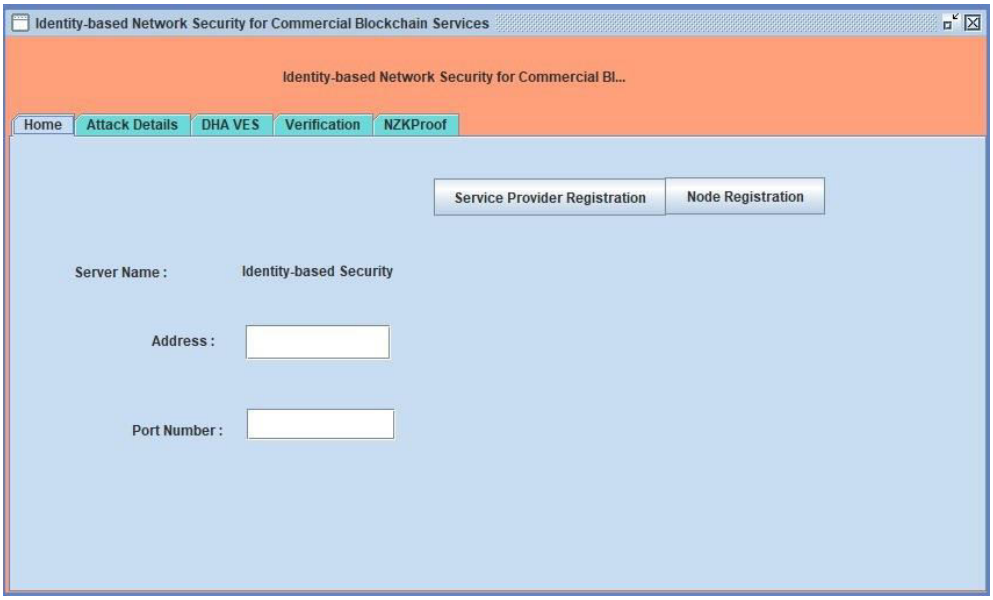

Figure 4.1: home page

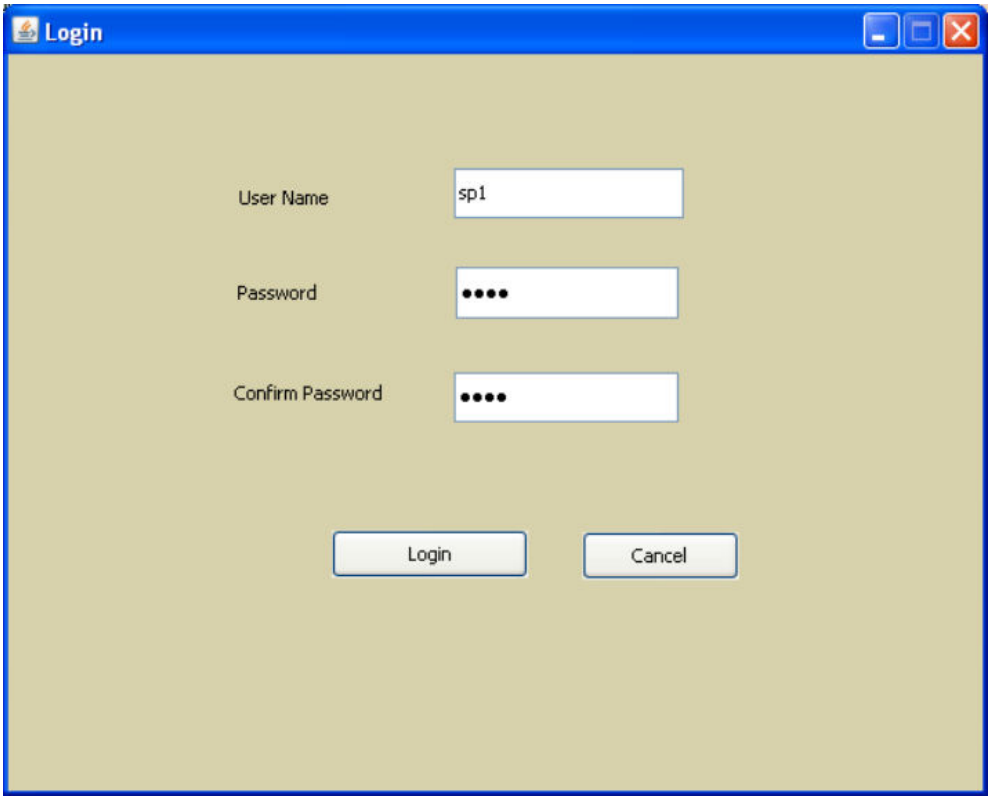

Figure 4.2: Login page

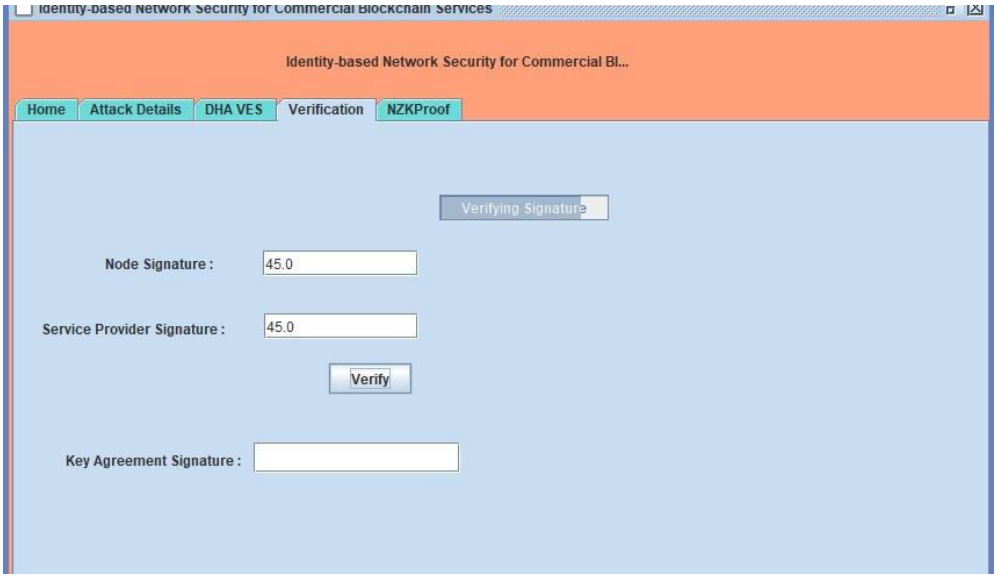

Figure 4.3: Verification

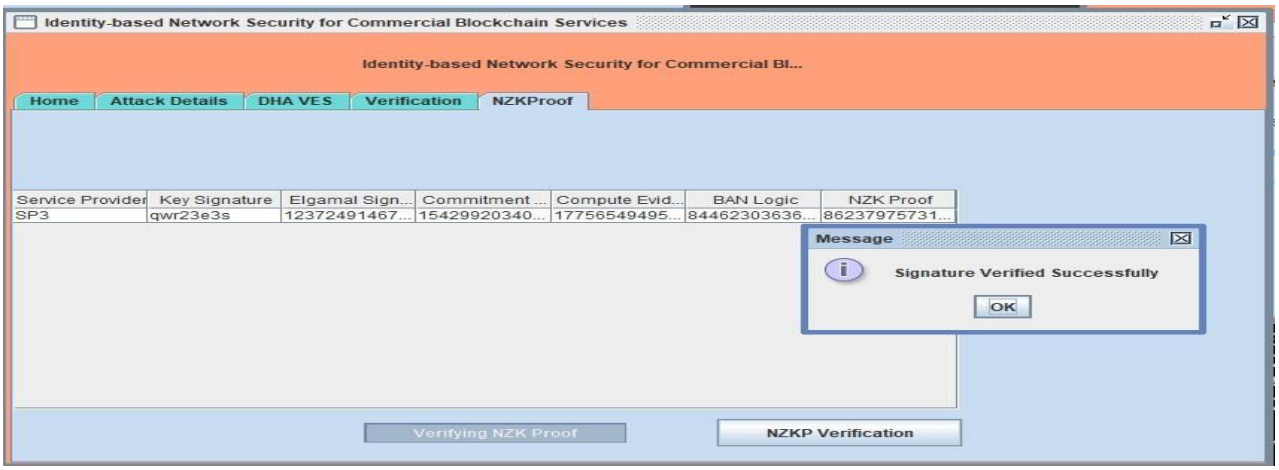

Figure 4.4: NZK Proof

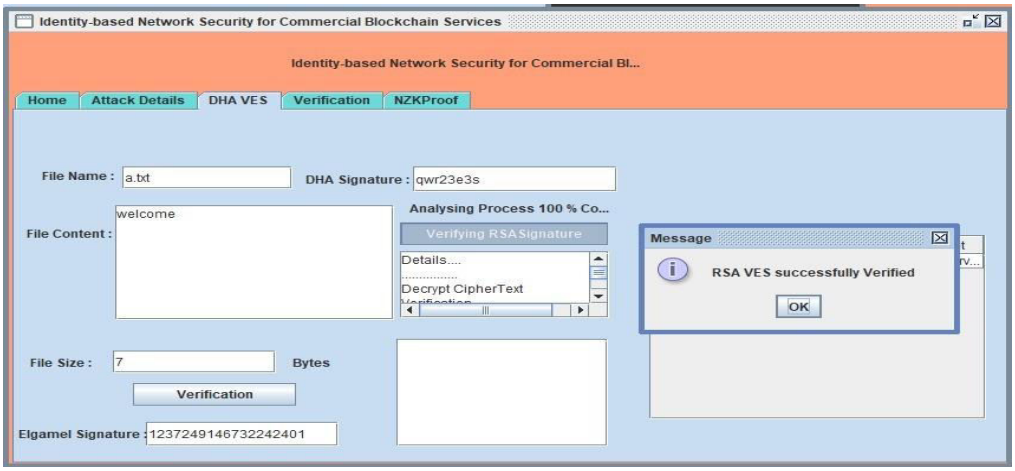

Figure 4.5: DHA VES

5.CONCLUSION

We have demonstrated how to create a secure and effective system for generating identification keys by integrating an individual's responses to a questionnaire with an XOR system of equations. We also developed a decentralized storage system application for secret storage and recovery based on this protocol. Additionally, we provide security scenarios in this study to assess the security of the schemes we develop using the questionnaire. But, we must hide go to each person's P when the questions include personal information about them, such When was the last time you had a cancer test or How often do you get a lung exam annually.

REFERENCES

1. M. Abe and S. Fehr. Adaptively Secure Feldman VSS and Ap- plications to Universally- Composable Threshold Cryptography.In Advances in Cryptology—CRYPTO'04, pages 317–334, 2004.

2. S. S. Al-Riyami and K. G. Paterson. Certificateless Public Key Cryp- tography. In Advances in Cryptology—ASIACRYPT'03, pages 452–473, 2003.

3. Y. Amir, C. Nita-Rotaru, J. R. Stanton, and G. Tsudik. Secure Spread: An Integrated Architecture for Secure Group Communi- cation. IEEE Transactions on Dependable and Secure Comput- ing, 2(3):248–261, 2005.

4. G. R. Blakley. Safeguarding cryptographic keys. In the National Computer Conference, pages 313–317, 1979.

5. D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based en- cryption with constant size ciphertext. In Advances in Cryptol- ogy—EUROCRYPT'05, pages 440–45 6, 2005.

Author Profiles

Mr. J. U. ARUN KUMAR Received M.Tech(CSE) form JNTUH & PG-DAC from CDAC New Delhi. He has around 2 years of teaching experience working as an Assistant Professor in the department of MCA & CSE at Audisankara Institute of Technology, Gudur, Tirupati(Dt), AP

CH. VENKATA SRIHARI is pursuing MCA from Audisankara institute of Technology (AUTONOMOUS), Gudur, Affiliated to JNTUA in 2024. Andhra Pradesh, India.